モニタリングおよびトラブルシューティング

- Cisco ISE のモニタリングとトラブルシューティング サービス，2 ページ
- モニタリングのためのデバイス設定，7 ページ
- プロファイラ フィードのトラブルシューティング，7 ページ
- ポスチャ コンプライアンス，7 ページ
- Cisco ISE プロセスをモニタする SNMP トラップ，8 ページ
- Cisco ISE アラーム，10 ページ
- ログ収集（Log Collection），34 ページ
- ライブ認証，34 ページ
- エンドポイントのグローバル検索，36 ページ
- エンドポイントのセッションのトレース，38 ページ
- 認証概要レポート，40 ページ
- 診断トラブルシューティング ツール，40 ページ
- セッション トレース テスト ケース，43 ページ
- 高度なトラブルシューティングのテクニカル サポートのトンネル，45 ページ
- 着信トラフィックを検証する TCP ダンプ ユーティリティ，46 ページ
- モニタリング ノードからのエンドポイント統計データのダウンロード，51 ページ
- その他のトラブルシューティング情報の入手，51 ページ
- モニタリング データベース，57 ページ

Cisco ISE のモニタ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 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。このメニューはプライマリ 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 ノードには表示されません。

- 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し、作用することができます。
- 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。次のフィールド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：[ID（Identity）]、[エンドポイントID（Endpoint ID）]、および [ISEノード（ISE Node）]（健全性の概要レポートは除く）。

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。

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 ([ホーム（Home）]>[概要（Summary）]）は、Cisco ISE 管理コンソールにログインすると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。デフォルトのダッシュボードは、[概要（Summary）]、[エンドポイント（Endpoints）]、[ゲスト（Guests）]、[脆弱性（Vulnerability）]、[脅威（Threat）] です。詳しくは、ISE ホーム ダッシュボード を参照してください。

（注） ダッシュボード データはプライマリ PAN にのみ表示されます。

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） ダッシュレットと対応するすべてのドリル ダウン ページを適切に表示するには、ブラウザに Adobe Flash Player がインストールされている必要があります。

[ダッシュボード設定（Dashboard Settings）] では次のオプションを使用できます。

オプション	説明
新しいダッシュボードの追加（Add New Dashboard）	プラス記号をクリックするか、ページの右上にある [ダッシュボード設定（Dashboard Settings）] をクリックすることで新しいダッシュボードを追加できます。 （注） 5 つのデフォルトのダッシュボードを含めて、最大で 20 個のダッシュボードを追加できます。
ダッシュボードの名前の変更	ダッシュボードの名前を変更するには、次の手順を実行します（カスタム ダッシュボードに対してのみ使用可能）。 1 [ダッシュボード設定（Dashboard Settings）] > [ダッシュボードの名前の変更（Rename Dashboard）] の順に選択します。 2 新しい名前を指定します。 3 [適用（Apply）] をクリックします。
ダッシュレットの追加（Add Dashlet）	ダッシュレットを追加するには、次の手順を実行します。 1 [ダッシュボード設定（Dashboard Settings）] > [ダッシュレットの追加（Add Dashlet(s)）] の順に選択します。 2 [ダッシュレットの追加（Add Dashlets）] ウィンドウで、追加するダッシュレットに対して [追加（Add）] をクリックします。 3 [保存（Save）] をクリックします。 （注） ダッシュボードごとに最大で 9 個のダッシュレットを追加できます。

オプション	説明
エクスポート（Export）	ダッシュレット データを PDF または CSV ファイルとしてエクスポートできます。 手順は次のとおりです。 **1** Cisco ISE ホーム ページから必要なダッシュボード（[概要（Summary）] など）を選択します。 **2** [ダッシュボード設定（Dashboard Settings）] > [エクスポート（Export）] の順に選択します。 **3** [エクスポート（Export）] ダイアログボックスで、次のいずれかのファイル形式を選択します。 • 選択したダッシュレットのスナップショットを表示するには、 PDF 形式を選択します。 • 選択したダッシュボード データを ZIP ファイルとしてダウンロードするには、CSV 形式を選択します。 **4** [ダッシュレット（Dashlets）] セクションで必要なダッシュレットを選択します。 **5** [エクスポート（Export）] をクリックします。 ZIP ファイルの名前は、選択したダッシュボードに基づいて指定されます（例：Summary.zip）。ZIP ファイルには、選択したダッシュボードの個々のダッシュレット CSV ファイルが含まれています。ダッシュレットの各タブに関連するデータは、対応するダッシュレット CSV ファイルで個別のセクションとして示されます。 カスタムダッシュボードをエクスポートする場合、ファイルは同じ名前でエクスポートされます。たとえば、MyDashboard という名前のカスタムダッシュボードをエクスポートすると、エクスポートされたファイルの名前は MyDashboard となります。

オプション	説明
レイアウト テンプレート（Layout Template）	ダッシュレットが表示されるテンプレートのレイアウトを変更できます。 レイアウトを変更するには、次の手順を実行します。 1 [ダッシュボード設定（Dashboard Settings）] > [レイアウト テンプレート（Layout Template）] の順に選択します。 2 使用可能なオプションから目的のレイアウトを選択します。
ダッシュボードの管理	[ダッシュボードの管理（Manage Dashboards）] では次のオプションを使用できます。 • デフォルトのダッシュボードにする（Mark as Default Dashboard）：ダッシュボードをデフォルト ダッシュボード（ホーム ページ）として設定するには、このオプションを使用します • すべてのダッシュボードのリセット（Reset all Dashboards）：すべてのダッシュボードを元の設定にリセットするには、このオプションを使用します

カスタム ダッシュボードの横にある閉じる（x）アイコンをクリックすることで作成したダッシュボードを削除できます。

（注） デフォルト ダッシュボードの名前を変更したり、削除することはできません。

すべてのダッシュレットには右上にツールバーがあり、次のオプションが含まれています。

1 分離（Detach）：別のウィンドウにダッシュレットを表示します。

2 更新（Refresh）：ダッシュレットを更新します。

3 削除（Remove）：ダッシュボードからダッシュレットを削除します。

ダッシュレットの左上隅にあるグリッパアイコンを使用して、ダッシュレットをドラッグアンドドロップできます。

[アラーム（Alarms）]ダッシュレットのクイック フィルタ：[重大（Critical）]、[警告（Warning）]、[情報（Info）]などの重大度に基づいてアラームをフィルタリングできます。[アラーム（Alarms）]

ダッシュレットはホーム ページに表示されます。このダッシュレットの [フィルタ（Filter）] ドロップダウンには、重大度に基づいてアラームを検索するためのクイック フィルタが含まれています。

NPF イベント フロー プロセス

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	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 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 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。

モニタリング 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。

モニタリングのためのデバイス設定

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 デバイスの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。

プロファイラ フィードのトラブルシューティング

テストがCiscoフィードサーバに接続できた場合は、テスト接続が成功したことを示すポップアップが表示されます。

接続に失敗した場合は、テスト ボタンの領域に、次の例のようなサーバからの応答が表示されます。メッセージの太字部分はメッセージの重要な部分を示します。

Test result: Failure: FeedService test connection failed : Feed Service unavailable : SocketTimeoutException invoking https://ise.cisco.com:8443/feedserver/feed/serverinfo: sun.security.validator.ValidatorException:PKIX path building failed: Sun.security.provider.certpath.SunCertPathBuilderException **Unable to find valid certification path to requested target**

考えられるエラー メッセージと実行すべきアクションを次に示します。

- 要求されたターゲットへの有効な認証パスを見つけることができません（Unable to find valid certification path to requested target）：フィード サーバが使用した証明書が無効です。Verisign 証明書がイネーブルになっていることを確認します。
- ホストへのルートがありません（No route to host）：ISE サーバから外部ネットワークへのアクティブな接続があるかを確認します。
- UnknownHostException（エラー メッセージの先頭）：ISE サーバから外部ネットワークへのアクティブな接続があるかを確認します。

ポスチャ コンプライアンス

ポスチャ コンプライアンス 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とそのユーザがポスチャ コンプライアンスに適合するかどうかに関する情報を示します。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。

ポスチャ コンプライアンスのチェック

ステップ 1 Cisco ISE ダッシュボードに進みます。

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、カーソルを積み上げ棒またはスパークラインに合わせます。
ツール チップに詳細情報が示されます。

ステップ 3 データ カテゴリを展開すると、詳細を参照できます。

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

（注） [コンテキストの可視性（Context Visibility ）] ページにポスチャ コンプライアンス レポートを表示できます。[コンテキストの可視性（Context Visibility）] ページ（[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]）には、コンプライアンス ステータス、場所、エンドポイントのタイプ、およびステータス トレンドに基づいてさまざまなチャートが表示されます。

Cisco ISE プロセスをモニタする SNMP トラップ

SNMP トラップは、Cisco ISE プロセスの状態を監視できます。Cisco ISE サーバにアクセスせずに、Cisco ISE プロセスをモニタする場合、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 プロセスのステータスを監視することもできます。

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。CLI から SNMP ホスト 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 プロセスを監視します。最初の SNMP ホストの設定時に、Cisco ISE で実行されている各プロセスに対し、そのステータスとは関係なく、SNMP サーバでトラップを個別に受信していることがわかります。

設定済みの SNMP サーバが Cisco ISE から送信されたトラップを受信できることを確認できます。その後、トラップは Cisco ISE プロセス ステータスが変化した場合にのみ、Cisco ISE から送信されます。MIB ブラウザのトラップ レシーバを使用して SNMP トラップを表示できます。

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。

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とき

- Linkup：イーサネット インターフェイスを起動するとき
- Linkdown：イーサネット インターフェイスをダウンするとき
- Authentication failure：コミュニティ ストリングが一致しないとき

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。
- Disk utilization：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たとき（設定された空きディスク領域の量に達するとトラップが送信されます）。

SNMP サーバで、すべてのオブジェクトについて一意のオブジェクト ID が生成され、値が OID に割り当てられます。SNMP サーバの 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 が SNMP トラップを SNMP サーバ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。

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 Reference Guide』を参照してください。

（注） ISE には、プロセス ステータスまたはディスク使用状況の MIB はありません。Cisco ISE は SNMP トラップの送信に OID HOST-RESOURCES-MIB::hrSWRunName を使用します。プロセス ステータスまたはディスク使用状況の照会には snmp walk または snmp get コマンドは使用できません。

OID	SNMP トラップ（SNMP Trap）
ディスク使用率の SNMP トラップ イベント	
1.3.6.1.4.1.2021.9.1.9	UCD_SNMP_OID:dskPercent
1.3.6.1.4.1.2021.9.1.2	UCD_SNMP_OID:dskPath
プロセス ステータスの SNMP トラップ通知	
1.3.6.1.2.1.25.4.2.1.2	HOST-RESOURCES-MIB:hrSWRunName

OID	SNMP トラップ（SNMP Trap）
通知イベントがデフォルトで通信されるその他の SNMP トラップ。詳細については、http://oidref.com/1.3.6.1.6.3.1.1.5 を参照してください。	
1.3.6.1.6.3.1.1.5.1	ColdStart
1.3.6.1.6.3.1.1.5.5	AuthenticationFailure
ネットワークから Cisco ISE に送信される SNMP トラップ イベント	
1.3.6.1.6.3.1.1.5.3	linkUp イベント
1.3.6.1.6.3.1.1.5.4	linkDown イベント
1.3.6.1.2.1.11.0.3	Cisco Link Up イベント
1.3.6.1.2.1.11.0.2	Cisco Link Down イベント
1.3.6.1.4.1.9.9.215.2.0.1	Cisco Mac 変更通知
1.3.6.1.4.1.9.9.215.2.0.2	Cisco Mac 移動通知

Cisco Mac 変更通知 SNMP トラップ OID を使用して、MAC-Address、Timestamp、MacStatus、Vlan、および dot1dBasePort の各属性は、エンドポイントの作成に使用されます。

SNMP トラップ イベント CommandResponderEvent を使用して、ネットワーク デバイスのアドレスである peerAddress を読み取ることができます。CommandResponderEvent PDU コマンド変数から IfIndex、Vlan、および MAC-Address 属性を読み取り、これらを使用してネットワーク上で SNMP クエリを実行して CDP 属性を取得し、エンドポイントに追加することができます。

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 アクティビティについてどのように通知するかを設定したり、それら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した場合、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は、トリガーに応じて、アラームが再び表示されるのに約 1 時間かかる場合があります。

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 *1*：*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措置について、失敗したノードの ADE.ログを確認します。
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措置について、失敗したノードの ADE.ログを確認します。
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 Redirect 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。ISE 2.0 へのアップグレードにより、デフォルトのシスコ ネットワーク デバイス プロファイルがすべてのネットワークデバイスに適用されました。	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。
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 サーバにインストールします。

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 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 が非推奨の URL を検出しました。	要求された URL が非推奨であるため、使用しないでください。
ERS が古い URL を検出（ERS identified out-dated URL）	ERS が古い URL を検出しました。	要求された URL が古いため、新しいものを使用してください。この URL は今後のリリースで削除されません。
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。

アラーム名	アラームの説明	アラームの解決方法
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。 • リポジトリに使用するクレデンシャルが正しいこと。 • 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 ユーザが書き込み特権を持っていること。
CA サーバがダウン（CA Server is down）	CA サーバがダウンしています。	CA サービスが CA サーバで稼働中であることを確認します。
CA サーバが稼働中（CA Server is Up）	CA サーバは稼働中です。	CA サーバが稼働中であることを管理者に通知します。
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。
証明書が失効（Certificate Revoked）	管理者は、内部 CA がエンドポイントに発行した証明書を取り消しました。	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。

アラーム名	アラームの説明	アラームの解決方法
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おり、証明書チェーンを構築できません。SCEPサーバからそれらを含むシステム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。見つかった場合、セカンダリ ノードに存在するその証明書を削除し、プライマリの新しい証明書をエクスポートしてから削除し、その後インポートすることによっ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条件によりセカンダリ 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から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。	コマンド **ip name-server** で設定した DNS サーバが到達可能であることを確認してください。 「CNAME <hostname of the node> に対する DNS 解決が失敗しました（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 を作成でき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。	Cisco Technical Assistance Center に問い合わせてファームウェア アップデートを入手してください。
仮想マシン リソースが不十分（Insufficient Virtual Machine Resources）	このホストでは、CPU、RAM、ディスク容量、IOPS などの仮想マシン（VM）リソースが不十分です。	Cisco ISE Hardware Installation Guide 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 サーバと Cisco ISE ノードとの間に大きな時間差（1000 秒を超える）があるために発生することがあります。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て、時間を同期します。

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を行います。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。このことは、M&T ノードがビジー状態である場合に発生する可能性があります。	[データ消去の監査（Data Purging Audit）] レポートをチェックし、used_space が threshold_space を下回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。
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、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 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、展開ページ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を確認します。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 プロセスがサーバで失敗しました。	サーバにパッチ プロセスを再インストールします。

アラーム名	アラームの説明	アラームの解決方法
パッチに成功（Patch Success）	パッチプロセスがサーバで成功しました。	-
外部 MDM サーバ API バージョンが不一致（External MDM Server API Version Mismatch）	外部 MDM サーバ 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 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 サーバ設定を更新します（必要な場合）。
外部 MDM サーバ接続に失敗（External MDM Server Connection Failure）	外部 MDM サーバへの接続に失敗しました。	MDM サーバが稼働し、Cisco ISE-MDM API サービスが MDM サーバで稼働していることを確認します。
外部 MDM サーバ応答エラー（External MDM Server Response Error）	外部 MDM サーバ応答エラーです。	Cisco ISE-MDM API サービスが MDM サーバ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 にログインして展開ページ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で再登録します。
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てください。
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。	アクションは必要ありません。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（Endpoints Purge Activities）	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（Endpoints and Users）] > [エンドポイントのアクティビティ消去（Endpoints Purge Activities）] で消去アクティビティを確認します。
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
複製低速情報（Slow Replication Info）	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てください。
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 を起動してください。
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 ノードがダウンまたは同期していないかどうかを確認し、必要な場合は手動で同期してください。
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してください。
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）	プライマリ管理ノード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 を起動して、フェールオーバーが発生するまで待機します。

アラーム名	アラームの説明	アラームの解決方法
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 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。
EST サービスの停止	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たことを確認します。
EST サービスの稼働	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管理者に通知します。
Smart Call Home の通信障害	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	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、送信元のサーバに接続できません。	送信元のサーバ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。

アラーム名	アラームの説明	アラームの解決方法
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。
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/NAD 設定を確認します。
MSE ロケーション サーバへのアクセス回復（MSE Location Server accessible again）	MSE ロケーション サーバへのアクセスが回復しました。	なし。
MSE ロケーション サーバにアクセス不能（MSE Location Server not accessible.）	MSE ロケーション サーバはアクセス不能でダウンしています。	MSE ロケーション サーバが稼働中で、ISE ノードからアクセスできるかどうかを確認します。
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。	この問題が連続して発生する場合は、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 GC（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。	ISE/NAD 設定を確認します。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。

アラーム名	アラームの説明	アラームの解決方法
IDマッピングの認証非アクティビティ（ID Map. Authentication Inactivity）	ユーザ認証イベントが過去 15 分に ID マッピング サービスによって収集されませんでした。	これがユーザ認証が想定される時間（たとえば、勤務時間）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。
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許可変更（CoA）要求を拒否しました。	Cisco ISE から許可変更（CoA）を受け入れるようにネットワーク デバイスが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どうかを確認します。
設定されたネームサーバがダウン（Configured nameserver is down）	設定されたネームサーバ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）] カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。

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/NAD 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）] カラムの横に表示される数値は、過去 15 分間で Cisco ISE に対して認証されたか失敗した認証の合計数です。
AD：マシン TGT のリフレッシュに失敗（AD: Machine TGT refresh failed）	ISE サーバ TGT（チケット認可チケット）のリフレッシュに失敗しました。これは AD 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、Kerberos 設定やネットワーク エラーも確認します。
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 は、NAS から多すぎる 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 からの認証とアカウンティング要求がサイレントに廃棄されています。これは、NAD が不明であるか、共有秘密鍵が不一致であるか、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 の共有秘密鍵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 グループを取得する権限があるかどうかを確認します。
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。
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。
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。
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。

アラーム名	アラームの説明	アラームの解決方法
操作 DB の使用率が高い（High Operations DB Usage）	ノードをモニタする 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。
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 ノードが稼働中であ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。
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 サービスが大量のトラフィック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てください。
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 [ライセンシング（Licensing）] ページ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 ノードは、許可されたライセンス数を超過しているか、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。

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）] ページを参照して、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。
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）] ページを参照し、[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、手動で認証を更新します。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 の認証の更新が完了したことを通知します。
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通知します。
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）] ページ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。

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通知します。
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）] ページを参照してください。Cisco ISE のスマート ライセンスの使用の詳細については、管理ガイドを参照するか、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）] ページ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 でのハイ アベイラビリティの役割が変化したことを通知します。
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）] ページ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）] ページ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通知します。

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）]ページ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）]ページ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）]ページ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 の登録が成功したことを通知します。
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保持できません。	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。その他の解決のために TAC に連絡してください。
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。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。
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 接続の失敗（TrustSec SSH connection failed）	TrustSec SSH 接続に失敗しました。	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）] ページでネットワーク デバイスの SSH クレデンシャルがネットワーク デバイス上のクレデンシャル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 は 1.0 以外の TLS バージョンで動作するよう設定されました（TrustSec identified ISE was set to work with TLS versions other then 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。

アラーム名	アラームの説明	アラームの解決方法
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）] ページとデバイスの CLI で、Trustsec デバイス クレデンシャルを確認します。デバイスが ISE サーバ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。
TrustSec 環境データのダウンロードの失敗	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 メッセージは無視されました	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。	TrustSec のデフォルトの出力ポリシーのセルが変更されました。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。

アラームは、Cisco ISE にユーザ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

次の表に、[アラーム設定（Alarm Settings）] ページのフィールドの説明を示します。（[管理（Administration）]>[システム（System）]>[設定（Settings）]>[アラーム設定（Alarm Settings）]）

フィールド	説明
アラーム タイプ（Alarm Type）	ドロップダウンリストからアラーム タイプを選択します。
アラーム名	アラームの名前を入力します。
説明	アラームの説明を入力します。
推奨されるアクション（Suggested Actions）	アラームがトリガーされるときに実行する推奨アクションを入力します。
ステータス	ステータスとして、アラーム ルールの [有効化（Enable）] または [無効化（Disable）] を選択します。
重大度（Severity）	ドロップダウン リスト ボックスを使用して、アラームの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（Warningi）]：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 メッセージを送信する場合に、このチェックボックスをオンにします。
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 Emails 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カンマ区切りリストを入力します。
電子メールのカスタムテキスト（Custom Text in Email）	システム アラームに関連付けるカスタム テキスト メッセージを入力します。

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。Cisco によって定義されるシステム アラームは [アラーム設定（Alarms Settings）] ページに表示されます（[管理（(Administration）] > [システム（System）] > [設定（Settings）] > [アラーム設定（Alarms Settings）]）。システム アラームだけを編集できます。

既存のシステム アラームの他に、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。

各アラーム タイプで最大 5 つのアラームを作成でき、アラームの合計数は 200 に制限されます。

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）] ページに表示されます。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 [送信（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。

アラームごとに通知設定を設定できます。各アラームに対し通知する必要があるユーザの電子メール ID を入力できます（システム定義およびユーザ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）] を選択します。

ステップ 2 デフォルト アラームのリストからアラームを選択して [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 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 [送信（Submit）] をクリックします。

モニタリング用の Cisco ISE アラーム

Cisco ISE は、重大なシステム状態が発生するたびに通知するシステム 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 ダッシュレットに表示されます。

アラーム 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。

モニタリング 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 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クリック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、データは表示されません。

ログ収集（Log Collection）

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。

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必要があります。

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（Live Authentications）] ページには、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。認証エントリに加えて、このページには、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、目的の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することもできます。

[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には、サーバ日付、時刻、およびタイムゾーンが示されます。

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し、もう 1 つは（セッション ライブ ビューからプルされた）セッション 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）] ページ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。

「最近の RADIUS 認証」の項で説明されている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。

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

ステップ 1 [操作（Operations）] > [RADIUSライブログ（RADIUS Livelog）] の順に選択します。

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 ドロップダウン リストの下部にある [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 セッションの動的な許可変更（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リング

[ライブ認証（Live Authentications）] ページのフィルタを使用して、必要な情報をフィルタリングし、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)）] ページのレコードをフィルタして、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、特定のユーザまたはロケーションから認証をフィルタリングすると、データをすばやくスキャンするために役立ちます。[ライブ認証（Live Authentications）] ページの各種フィールドで使用できる複数の演算子を使用して、検索基準に基づいてレコードをフィルタリングできます。

- 「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 を持つユーザの認証レコードを確認する場合は、ID フィルタ テキスト ボックスに "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リングできます。緑色のチェック マークは以前発生したすべての成功した認証をフィルタリングします。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リングします。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（RADIUS Livelog）] の順に選択します。

ステップ 2 [ライブ認証の表示（Show Live Authentications）] ページのいずれかのフィールドに基づいてデータをフィルタリングします。
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。

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して、エンドポイントを検索できます。次の条件を使用してエンドポイントを検索できます。

- ユーザ名（User name）
- MAC アドレス
- [IPアドレス（IP Address）]
- 許可プロファイル
- エンドポイント プロファイル
- 失敗の理由
- 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 タイプ
- オペレーティング システム（Operating System）
- ポスチャ ステータス

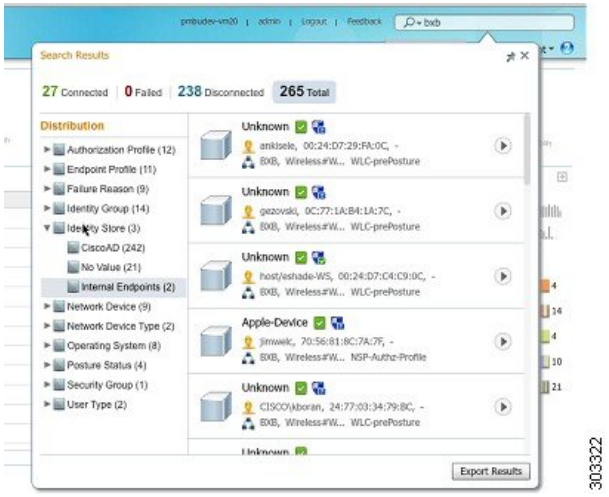
- 参照先
- セキュリティ グループ
- ユーザ タイプ（User Type）

データを表示するには、[検索（Search）]フィールドに任意の検索条件の少なくとも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概要の情報が表示され、これをトラブルシューティングに使用することができます。検索結果には、上位25のエントリのみが表示されます。結果を絞り込むためにフィルタを使用することを推奨します。

次の図は、検索結果の例を示しています。

図 *1*：エンドポイントの検索結果



左パネルの任意のプロパティを使用して、結果をフィルタリングします。エンドポイントをクリックして、エンドポイントに関する次のような詳細情報を表示することもできます。

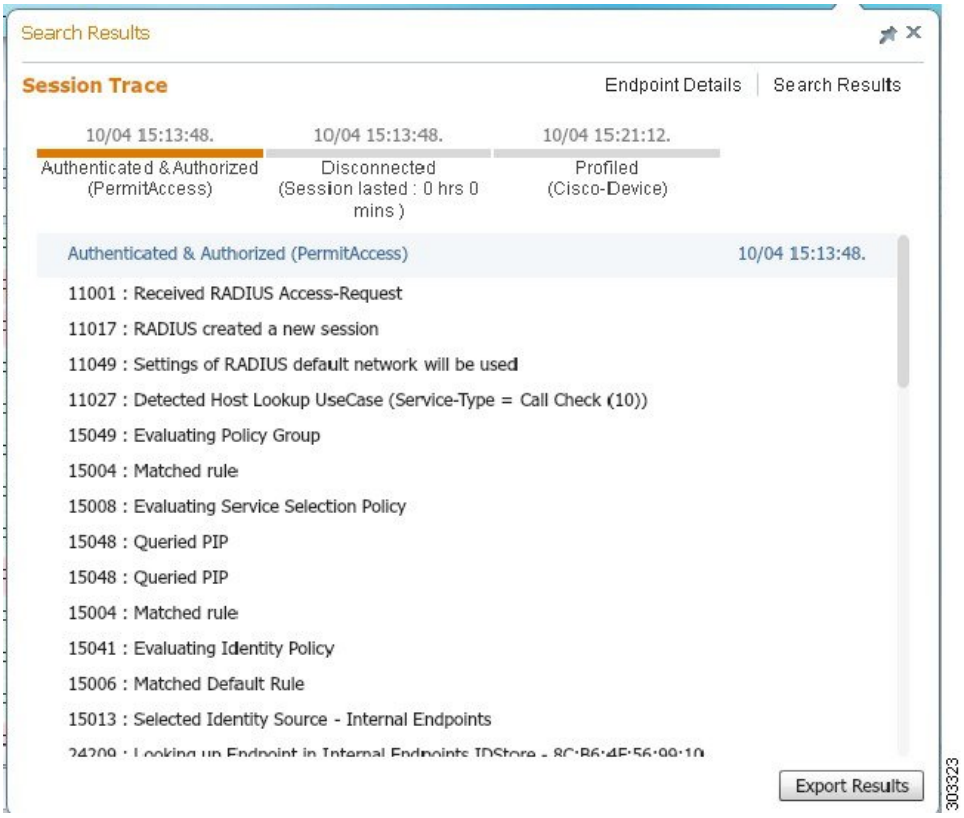
- セッションのトレース
- 認証の詳細
- アカウンティングの詳細
- ポスチャの詳細
- プロファイラの詳細
- クライアント プロビジョニングの詳細
- ゲスト アカウンティングおよびアクティビティ

エンドポイントのセッションのトレース

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して、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。基準に基づいて検索する場合は、エンドポイントのリストを取得します。エンドポイントのセッション トレース情報を表示するには、そのエンドポイントをクリックします。次の図に、エンドポイントに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、認証が行われる場合、検索結果セットにそれらを含めるには、認証にエンドポイントのエンドポイント ID が必要です。

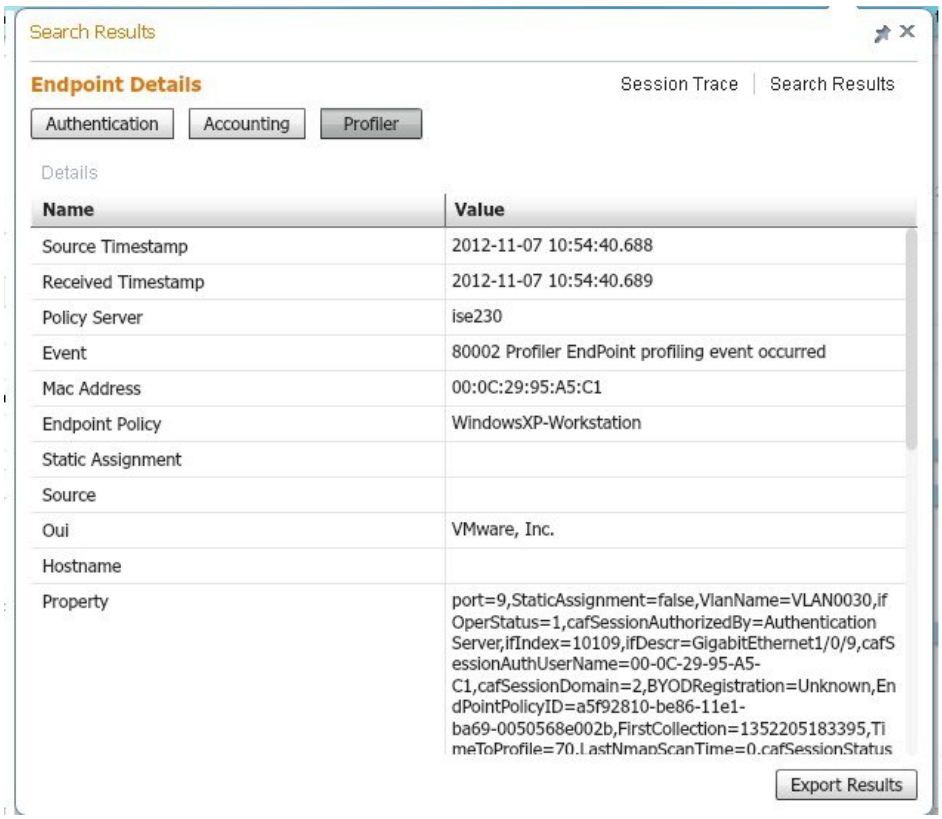
図 *2*：エンドポイントのセッションのトレース



上部にあるクリック可能なタイムラインを使用すると、主な許可の遷移を確認できます。[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。レポートは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）]リンクをクリックします。次の図に、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 *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、終了後 15 分で削除されます。
- 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 セッションは、7 日後に削除されます。

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、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。このことは、認証概要レポートを実行して行います。

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）] > [認証概要レポート（Authentication Summary Report）] を選択します。

ステップ 2 失敗の理由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） 認証概要レポートが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。

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、TrustSec 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。

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することができます。認証が成功すると予想していたのに失敗した場合、またはユーザやマシンが特定の特権レベルを持っていると予想したのにユーザやマシンがこれらの特権を持っていなかった場合は、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）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、その後設定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。
AD 関連の認証を検索する際に、展開に Active Directory サーバ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。
AD 関連の認証をトラブルシューティングする必要がある場合は、[管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] > [AD ノード（AD node）] で、診断ツールに移動します。

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、問題を解決するための手順、およびトラブルシューティング概要を表示するには、[完了（Done）] をクリックします。

ネットワーク デバイス 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。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思われる場合や、設定を検証したい場合、または単にどのように設定されているか関心がある場合に、使用することができます。

設定を確認する 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 該当する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）] 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。

設定バリデータ ツールの評価

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。

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）] > [一般的なツール（General Tools）] > [設定バリデータの評価（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）] 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。

ポスチャのトラブルシューティング ツール

[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。

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

このツールでは、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、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。この詳細情報を使用して、ポリシー システムとのやりとりが行われ、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

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）] > [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 [追加（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 事前定義テストケースを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目的の値を選択することができます。また、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）] ページの下部に、すべての属性の概要が表示されます。

ステップ 5 [送信（Submit）] をクリックして、テスト ケースを作成します。
Cisco ISE はテストの詳細を保存する前に、属性とそ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。[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 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は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を表形式で表示します。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 [以前のテスト実行（Previous Test Executions）] タブをクリックし、以前のテスト実行結果を表示します。また、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。

[RADIUS ライブ ログ（RADIUS Live Logs）] ページから [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）] ページ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。必要に応じてこ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。

高度なトラブルシューティングのテクニカルサポートのトンネル

Cisco ISE は、Cisco IronPort トンネル インフラストラクチャを使用して、ISE サーバに接続してシステムの問題をトラブルシューティングするための、シスコ テクニカル サポート エンジニア用のセキュア トンネルを作成します。Cisco ISE は SSH を使用して、トンネル経由のセキュアな接続を作成します。

管理者として、トンネルアクセスを制御できます。サポートエンジニアにアクセス権を付与する時期と期間を選択できます。シスコ カスタマーサポートは、ユーザの介入なしにトンネルを確立できません。サービス ログインに関する通知を受信します。任意の時点でトンネル接続をディセーブルにできます。デフォルトでは、テクニカル サポート トンネルは 72 時間開いたままになりますが、すべてのトラブルシューティング作業が完了したら、ご自身またはサポート エンジニアがトンネルを閉じることを推奨します。必要に応じて、72 時間を超えてトンネルを延長することもできます。

tech support-tunnel enable コマンドを使用して、トンネル接続を開始できます。

tech support-tunnel status コマンドでは、接続のステータスが表示されます。このコマンドでは、接続が確立されたかどうか、または認証エラーがあるかどうか、あるいはサーバが到達不能であるかどうかに関する情報が提示されます。トンネル サーバは到達可能であるが ISE が認証できない場合、ISE は 30 分にわたり 5 分ごとに再認証を試行し、その後トンネルは無効になります。

tech support-tunnel disable コマンドを使用してトンネル接続を無効にできます。このコマンドでは、サポート エンジニアが現在ログインしている場合も既存のトンネルが切断されます。

ISE サーバからのトンネル接続をすでに確立している場合は、生成される SSH キーを ISE サーバで使用できます。後でサポート トンネルをイネーブルにしようとすると、システムによって、以前に生成された SSH キーを再使用するよう指示されます。同じキーを使用するか、または新しいキーを生成するかを選択できます。また、**tech support-tunnel resetkey** コマンドを使用してキーを

手動でリセットすることもできます。トンネル接続が有効な場合にこのコマンドを実行すると、先に接続をディセーブルにするよう求めるプロンプトが表示されます。既存の接続を続け、無効にしないことを選択した場合、キーは既存の接続が無効になった後でリセットされます。接続を無効にすることを選択した場合、トンネル接続はドロップされ、キーは即座にリセットされます。

トンネル接続の確立後に、**tech support-tunnel extend** コマンドを使用して拡張することができます。

tech support-tunnel コマンドの使用上のガイドラインについては、『Cisco Identity Services Engine CLI Reference Guide』を参照してください。

テクニカル サポート トンネルの確立

Cisco ISE コマンドライン インターフェイス（CLI）からセキュア トンネルを確立できます。

ステップ 1 Cisco ISE CLI から、次のコマンドを入力します。
tech support-tunnel enable

トンネルのパスワードとニックネームの入力が求められます。

ステップ 2 パスワードを入力します。

ステップ 3 （任意）トンネルのニックネームを入力します。
システムによって SSH キーが生成され、パスワード、デバイスのシリアル番号および SSH キーが表示されます。サポート エンジニアがシステムに接続できるように、この情報をシスコ カスタマー サポートに渡す必要があります。

ステップ 4 パスワード、デバイスのシリアル番号および SSH キーをコピーし、シスコ カスタマー サポートに送信します。
これで、サポート エンジニアが ISE サーバに安全に接続できるようになります。サービス ログに関する定期的な通知を受信します。

着信トラフィックを検証する TCP ダンプ ユーティリティ

これは、予想されたパケットが実際にノードに到達したことを調査する場合に、パケットをスニッフィングするツールです。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。

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することができます。

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リングでの TCP ダンプの使用

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）のみが表示されます。デフォルトでは、すべての NIC は VMware に接続されるため、NIC は、IPv6 アドレスを使用して設定され、[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。

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、オンかオフにして、無差別モードを設定します。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。[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。

（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

はじめる前に

「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 TCPdump 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 [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。

エンドポイントまたはユーザの予期しない 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 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 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。

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を使用して比較が行われます。

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 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。

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 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。

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。

モニタリングノードからのエンドポイント統計データのダウンロード

モニタリング ノードからネットワークに接続するエンドポイントの統計データをダウンロードできます。ロード、CPU 使用率、認証トラフィック データを含む主要パフォーマンス メトリック（KPM）が使用可能で、ネットワークの問題の監視およびトラブルシューティングに使用できます。日次 KPM 統計情報または過去 8 週間の KPM 統計情報をそれぞれダウンロードするには、Cisco ISE コマンドライン インターフェイス（CLI）から、**application configure ise** コマンドを使用し、オプション 12 または 13 を使用します。

このコマンドの出力では、エンドポイントに関する次のデータが提供されます。

- ネットワーク上のエンドポイントの総数
- 正常な接続を確立したエンドポイントの数
- 認証に失敗したエンドポイントの数。
- 毎日の接続済みの新しいエンドポイントの総数
- 毎日のオンボーディングしたエンドポイントの総数

出力には、タイムスタンプの詳細、展開内の各ポリシー サービス ノード（PSN）を介して接続したエンドポイントの総数、エンドポイントの総数、アクティブ エンドポイント、負荷、および認証トラフィックの詳細も含まれています。

このコマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide*』を参照してください。

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、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）情報、およびモニタリングとレポートが取得されます。

  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、第 11 章「ログ」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。詳細については、Cisco ISE デバッグ ログ, （54 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、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*』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。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, （53 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 および他のログ 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には、暗号化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ように選択できるようになりました。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。

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 レベルを設定します。

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と終了日を入力します。

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）：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選択します。
- 共有キー暗号化（Shared Key Encryption）：このオプションは、オンプレミスでローカルで問題をトラブルシューティングする場合に選択します。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。

次の作業

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警告アラームと、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。

デバッグ ログの入手

ステップ 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。

ステップ 2 デバッグ ログをダウンロードします。

Cisco ISE コンポーネントおよび対応するデバッグ ログ

表 *2*：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
ライセンス	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
クライアント	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
ゲスト アクセス管理	guest.log
ゲスト アクセス	guest.log

コンポーネント	デバッグ ログ
MyDevices	guest.log
ポータル（Portal）	guest.log
ポータル セッション マネージャ	guest.log
ポータル Web アクション	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-alarm	alarms.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
ポスチャ	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

デバッグ ログのダウンロード

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 [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

モニタリング データベース

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と復元

モニタリング データベースは、大量のデータを処理します。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） 消去操作の実行中には、バックアップを実行しないでください。消去操作の実行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 ノードを登録する場合は、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、新しいセカンダリ モニタリング ノードにデータを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ため、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 ノードと同期状態となります。

モニタリング データベースの消去

消去プロセスでは、消去時にデータを保持する月数を指定することで、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）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 日で構成されます。デフォルトの 3 ヵ月は 90 日間です。

モニタリング データベースの消去に関するガイドライン

次に、モニタリング データベースのディスク使用に関連して従うべきガイドラインをいくつか示します。

- モニタリング データベースのディスク使用量がしきい値設定の 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。ディスク使用量が 90% より大きい場合は、別のアラームが生成されます。

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

- 消去は、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も基づきます。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%）以上になると、消去プロセスが開始されます。このプロセスは、管理者ポータルの設定に関係なく、過去 7 日間のモニタリング データのみを削除します。ディスク領域が 80% 未満になるまで繰り返

しプロセスを続行します。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。

運用データの消去

[運用データの消去（Operational Data Purging）] ページ（[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [運用データの消去（Operational Data Purging）]）には、[データベースの使用状況（Database Utilization）] 領域と [データを今すぐ消去（Purge Data Now）] 領域があります。[データベースの使用状況（Database Utilization）] 領域には、使用可能なデータベース容量の合計と、保存されている RADIUS および TACACS データが表示されます。ステータスバーをマウスオーバーすると、利用可能なディスク容量と、データベースに既存データが保存されている日数が表示されます。RADIUS データと TACACS データを保持できる期間を [データ保存期間（Data Retention Period）] 領域に指定できます。データは毎朝午前 4 時に消去されます。また、保存日数を指定して、消去前にデータをリポジトリにエクスポートするように設定できます。[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにして、リポジトリを選択して作成し、暗号キーを指定できます。

[データを今すぐ消去（Purge Data Now）] 領域では、すべての RADIUS および TACACS データを消去するか、またはデータ消去までに保存できる日数を指定できます。

（注） 消去前にリポジトリにエクスポートできるテーブルは、RADIUS 認証およびアカウンティング、TACACS 認証およびアカウンティング、RADIUS エラー、および設定が誤っているサプリカントの各テーブルです。

関連トピック

古い運用データの消去, （59 ページ）

古い運用データの消去

運用データはサーバに一定期間集められています。すぐに削除することも、定期的に削除することもできます。データ消去の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）] > [運用データの消去（Operational Data Purging）] を選択します。

ステップ 2 次のいずれかを実行します。

- [データ保持期間（Data Retention Period ）] 領域で次の操作を行います。

1. RADIUS または TACACS データを保持する期間を日単位で指定します。指定した期間より前のデータはすべてリポジトリにエクスポートされます。
2. [リポジトリ（Repository）] 領域で、[リポジトリのエクスポートを有効にする（Enable Export Repository）] チェックボックスをオンにし、データを保存するリポジトリを選択します。詳細については、「リポジトリの作成」の項を参照してください。
3. [暗号キー（Encryption Key）] テキスト ボックスに必要なパスワードを入力します。
4. [保存（Save）] をクリックします。

（注） 設定し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日に設定し、この値が診断テーブルの既存のしきい値（たとえば、5 日のデフォルト）未満の場合、データはこのページで設定した値（3 日）に従って消去されます。

- [データを今すぐ消去（Purge Data Now）] 領域で、次の操作を行います。

1. すべてのデータを消去するか、または指定された日数よりも古いデータを消去します。データはリポジトリに保存されません。
2. [消去（Purge）] をクリックします。