メンテナンスとモニター

適応型ネットワーク制御

適応型ネットワーク制御（ANC）は、管理ノードで実行されるサービスです。このサービスは、エンドポイントのネットワークアクセスをモニターおよび制御します。ANCは、ISE管理者が管理 GUI で呼び出すことも、サードパーティ製システムから pxGrid を介して呼び出すこともできます。 ANC は有線展開とワイヤレス展開をサポートしており、Plus ライセンスと ライセンスが必要です。

ANC を使用すると、システムの許可ポリシー全体を変更することなく許可状態を変更できます。ANC を使用すると、エンドポイントを隔離するときに認証状態を設定できます。その結果、ANCPolicyを確認してネットワークアクセスを制限または拒否するように認証ポリシーが定義されている認証ポリシーが確立されます。エンドポイントを隔離解除して、フル ネットワーク アクセスを可能にできます。ネットワークからエンドポイントを接続解除する Network Attached System（NAS）上のポートをシャットダウンすることもできます。

一度に隔離できるユーザーの数に制限はありません。また、隔離期間の長さに時間的な制約はありません。

ANC によってネットワーク アクセスをモニターおよび制御するには、次の操作を実行できます。

- [隔離（Quarantine）]：例外ポリシー（認証ポリシー）を使用して、ネットワークへのエンドポイントアクセスを制限または拒否することができます。 ANCPolicy に応じて異なる許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエン

ドポイントが移動します。エンドポイントと同じ NAS でサポートされる隔離 VLAN を事前に定義する必要があります。

- [隔離解除（Unquarantine）] : 隔離ステータスを元に戻し、エンドポイントのネットワークへのフルアクセスを許可します。これは、エンドポイントを元の VLAN に戻すことで発生します。
- [シャットダウン（Shutdown）] : NAS 上のポートを非アクティブ化して、ネットワークからエンドポイントの接続を解除できます。エンドポイントが接続されている NAS でポートがシャットダウンされたら、NASのポートを再度手動でリセットします。これにより、エンドポイントがネットワークに接続できるようになります。これはワイヤレス展開には使用できません。

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからトリガーできます。

（注） 隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

Cisco ISE での適応型ネットワーク制御の有効化

ANC は、デフォルトで無効になっています。ANC は pxGrid が有効にされた場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

ネットワーク アクセスの設定

ANC によってエンドポイントのネットワークアクセスのステータスをポートの隔離、隔離解除、またはシャットダウンにリセットできます。これらは、ネットワーク内のエンドポイントの許可の程度を定義します。

エンドポイントの隔離や隔離解除、またはエンドポイントが接続されているネットワーク アクセス サーバー（NAS）ポートのシャットダウンを行うには、エンドポイントの IP アドレスまたは MAC アドレスを使用します。同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、 ANC を使用してそのエンドポイントのアクセスをシャットダウンし、NAS ポートを閉じることができます。

ANC ポリシーをエンドポイントに割り当てるには、次の手順を実行します。

始める前に

- ANC を有効にします。
- ANC の認証プロファイルと例外タイプの認証ポリシーを作成します。

ステップ 1 **[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [ポリシーリスト（Policy List）]** 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 ANC ポリシーの名前を入力し、ANC アクションを指定します。次のオプションを使用できます。

- 検疫（Quarantine）
- シャットダウン（Shut_Down）
- ポートバウンス（Port_Bounce）

1 つまたは複数のアクションを選択できますが、[Shut_Down] および [Port_Bounce] を他の ANC アクションと組み合わせることはできません。

[Quarantine] と [Re_Authenticate] は、組み合わせることができる唯一の 2 つのアクションです。

[Quarantine]、[Port_Bounce]、または [Re_Authenticate] を含む ANC ポリシーがアクティブなエンドポイントに割り当てられるか、割り当て解除されると、そのエンドポイントに対して CoA がトリガーされます。

[Shut_Down] アクションを含む ANC ポリシーがアクティブなエンドポイントに割り当てられると、CoA がトリガーされてスイッチインターフェイスがシャットダウンされます。ただし、[Shut_Down] アクションを含む ANC ポリシーが割り当て解除されるときは、CoA はトリガーされません。

ステップ 4 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択して、ポリシー セットを展開します。

ステップ 5 ANCPolicy 属性を使用して ANC ポリシーを対応する許可ポリシーに関連付けます。

ステップ 6 [操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [エンドポイント割り当て（Endpoint Assignment）] の順に選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 エンドポイントの IP アドレスまたは MAC アドレスを入力し、[ポリシー割り当て（Policy Assignment）] ドロップダウン リストからポリシーを選択します。

ステップ 9 [Submit] をクリックします。

ANC によるネットワーク アクセスの許可プロファイルの作成

ANC と使用する認証プロファイルを作成する必要があります。認証プロファイルは、標準認証プロファイルのリストに表示できます。エンドポイントはネットワークで認証および許可されますが、ネットワークへのアクセスが制限されています。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]** 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 認証プロファイルの一意の名前と説明を入力し、**[アクセス タイプ（Access Type）]** は **[ACCESS_ACCEPT]** に更新します。

ステップ 4 [DACL名（DACL Name）]チェックボックスをオンにし、ドロップダウンリストから[DENY_ALL_TRAFFIC]を選択します。

ステップ 5 [送信（Submit）] をクリックします。

例外許可ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。ANC 許可用に、すべての標準認証ポリシーの前に処理される隔離例外ポリシーを作成する必要があります。次の条件で例外ルールを作成する必要があります。

セッション：ANCPolicy EQUALS Quarantine。

ANC NAS ポートのシャットダウン フロー

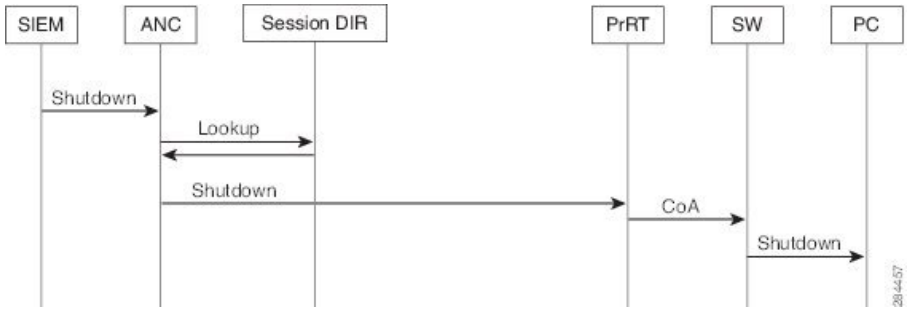
エンドポイントのIPアドレスまたはMACアドレスを使用して、エンドポイントの接続先NASポートをシャット ダウンできます。

シャットダウンを使用すると、MAC アドレスに指定された IP アドレスに基づいて NAS ポートを閉じることができます。手動でポートを復元して、エンドポイントをネットワークに戻す必要があります。これは、有線メディアで接続されたエンドポイントのみに有効です。

シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

この図は、 ANC のシャットダウンのフローを示しています。クライアントデバイスでは、このクライアントデバイスがネットワークにアクセスするために使用する NAS でシャットダウン操作が実行されます。

図 *1 : ANC* のシャットダウン フロー



エンドポイントの消去の設定

ID グループとその他の条件に基づいた設定ルールで、エンドポイントの消去ポリシーを定義できます。**[管理（Administration）]**>**[ID の管理（Identity Management）]**>**[設定（Settings）]**>**[エンドポイントの消去（Endpoint Purge）]** の順に選択します。指定したエンドポイントを消

去しないことや、選択したプロファイリング条件に基づいてエンドポイントを消去することを選択できます。

エンドポイント消去ジョブをスケジュールできます。このエンドポイント消去スケジュールはデフォルトで有効です。Cisco ISE はデフォルトで、30 日よりも古い登録デバイスとエンドポイントを削除します。消去ジョブは、プライマリ管理ノード（PAN）で設定されたタイムゾーンに基づいて毎日午前 1 時（深夜）に実行されます。

エンドポイントの消去では、3 分ごとに 5000 以上のエンドポイントが削除されます。

次に、エンドポイントの消去に使用できる条件と例の一部を示します。

- InactivityDays：エンドポイントでの最後のプロファイリングアクティビティまたは更新からの日数。
  - この条件によって、時間の経過に伴って蓄積した古いデバイス（一般的には一時的なゲストやパーソナルデバイス）、または廃止されたデバイスが消去されます。これらのエンドポイントは、ネットワーク上でアクティブでないか、近い将来に使用される可能性が低いため、展開でノイズとなる傾向があります。それらが再度接続した場合は、必要に応じて再検出、プロファイリング、登録などが行われます。
  - エンドポイントから更新が発生すると、InactivityDays はプロファイリングが有効である場合にのみ 0 にリセットされます。
- ElapsedDays：オブジェクトが作成されてからの日数。
  - この条件は、ゲストまたは請負業者のエンドポイント、ネットワーク アクセス WebAuth を利用する従業員などの、未認証アクセスまたは条件付きアクセスが一定期間認められたエンドポイントに使用できます。許可された接続猶予期間が経過した後、それらは完全に再認証および登録される必要があります。
- PurgeDate：エンドポイントを消去する日付。
  - このオプションは、作成または開始時間に関係なく一定期間のアクセスを許可する、特別なイベントやグループに使用できます。このオプションでは、すべてのエンドポイントを同時に消去できます。たとえば、展示会、会議、または毎週メンバーが入れ替わる週ごとのトレーニングクラスでは、絶対的な日や週や月ではなく、特定の週や月にアクセスを許可する場合に使用します。

（注） 消去するエンドポイント数が 10,000 を超える場合、初回の消去時に最初の 10,000 エンドポイントのみが消去されます。1 時間後に、次の 10000 エンドポイントのセットを削除するために別のパージが開始されます。この消去サイクルは、一致する消去条件に基づいてすべてのエンドポイントが消去されるまで続きます。この動作により、システムパフォーマンスが最適化されます。

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

問題

ポリシー変更またはIDの追加後に認証が失敗し、再認証が行われません。認証が失敗するか、問題のエンドポイントがネットワークに接続できなくなります。この問題は、ユーザーロールに割り当てられるポスチャポリシーごとのポスチャ評価に失敗するクライアントマシンで頻繁に発生します。

考えられる原因

クライアントマシンで認証タイマーが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。

ソリューション

この問題には、解決策がいくつか考えられます。

1. Cisco ISE で、指定された NAD またはスイッチの **[セッションステータス概要（Session Status Summary）]** レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。
2. NAD/スイッチ上で "show running configuration" と入力し、適切な「authentication timer restart」設定でインターフェイスが設定されていることを確認します（たとえば、「authentication timer restart 15」および「authentication timer reauthenticate 15」）。
3. NAD/スイッチ上で「interface shutdown」および「no shutdown」と入力してポートをバウンスし、Cisco ISE で構成変更があったと考えられる場合には再認証を適用します。

Note CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する

エンドポイントで実行する ANC 操作は、そのエンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。

（注） ANC を介してエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。エンドポイントのアクティブなセッションで IP アドレスまたは MAC アドレスが見つからない場合は、次のエラーメッセージが表示されます。

```
この MAC アドレス、IP アドレス、またはセッション ID のアクティブなセッションが見つかりません（No active session found for this MAC address, IP Address or Session ID）
```

.

外部認証された管理者が ANC 操作を実行できない

外部認証された管理者がライブ セッションから CoA 隔離を発行しようとすると、Cisco ISE は次のエラー メッセージを返します。

```
「xx: xx: xx: xx: xx: xx に対する隔離の CoA アクションを開始できません。（CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated.）原因：内部でユーザーが見つかりません。（Cause:User not found internally.）サポートされていない外部認証されたユーザーを使用している可能性があります（Possible use of unsupported externally authenticated user）」
```

外部認証された管理者が、エンドポイントの IP アドレスまたは MAC アドレスを使用して、Cisco ISE の **[操作（Operations）]** から ANC 操作を実行すると、Cisco ISE は次のエラーメッセージを返します。

```
「サーバー障害：内部でユーザーが見つかりません。（Server failure: User not found internally.）サポートされていない外部認証されたユーザーを使用している可能性があります（Possible use of unsupported externally authenticated user）」
```

Cisco ISE ソフトウェアパッチ

Cisco ISE ソフトウェアのパッチは常に累積されます。Cisco ISE では、パッチのインストールおよびロールバックを CLI または GUI から実行できます。

展開内の Cisco ISE サーバーにパッチをインストールする作業は、プライマリ PAN から行うことができます。プライマリ PAN からパッチをインストールするには、Cisco.com からクライアントブラウザを実行しているシステムにパッチをダウンロードします。

GUI からパッチをインストールする場合、パッチは最初にプライマリ PAN に自動的にインストールされます。その後、システムは、GUI にリストされている順序で、展開内の他のノードにパッチをインストールします。ノードが更新される順序を制御することはできません。パッ

チバージョンを手動でインストール、ロールバック、および表示することもできます。これを行うには、GUI で [管理者（Administrator）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch management）] ウィンドウを選択します。

CLI からパッチをインストールする場合は、ノードの更新順序を制御できます。ただし、最初にプライマリ PAN にパッチをインストールすることを推奨します。残りのノードでのインストールの順序は関係ありません。プロセスを高速化するために、パッチを複数のノードに同時にインストールできます。

展開全体をアップグレードする前にいくつかのノードでパッチを検証する場合、CLI を使用すると、選択したノードでパッチをインストールできます。パッチをインストールするには、次の CLI コマンドを使用します。

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

詳細については、『Cisco Identity Services Engine CLI リファレンスガイド』の「EXEC モードの Cisco ISE CLI コマンド」の章にある「patch install」の項を参照してください。

必要なパッチバージョンを直接インストールすることができます。たとえば、Cisco ISE 2.x を使用していて、Cisco ISE 2.x パッチ 5 をインストールする場合、以前のパッチ（Cisco ISE 2.x パッチ 1 ～ 4 など）をインストールしなくても、Cisco ISE 2.x パッチ 5 を直接インストールできます。CLI でパッチバージョンを表示するには、次の CLI コマンドを使用します。

```
show version
```

関連トピック

ソフトウェア パッチ インストールのガイドライン （9 ページ）
ソフトウェア パッチ ロールバックのガイドライン （11 ページ）
ソフトウェアパッチのインストール （10 ページ）
ソフトウェアパッチのロールバック （11 ページ）

ソフトウェア パッチ インストールのガイドライン

ISE ノードにパッチをインストールすると、インストールの完了後にノードが再起動されます。再びログインできる状態になるまで、数分かかることがあります。メンテナンスウィンドウ中にパッチをインストールするようにスケジュール設定し、一時的な機能停止を回避することができます。

インストールするパッチが、ネットワーク内に展開されている Cisco ISE のバージョンに適用されるものであることを確認してください。Cisco ISE はパッチファイルのバージョンの不一致とあらゆるエラーをレポートします。

Cisco ISE に現在インストールされているパッチよりも低いバージョンのパッチをインストールできません。同様に、あるバージョンのパッチの変更をロールバックしようとしたときに、それよりも高いバージョンのパッチがその時点で Cisco ISE にインストール済みの場合は、ロールバックはできません。たとえば、パッチ 3 が Cisco ISE サーバーにインストール済みの場合に、パッチ 1 または 2 をインストールしたり、パッチ 1 または 2 にロールバックすることはできません。

分散展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco ISEによってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco ISE はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。ただし、何らかの理由でセカンダリノードのいずれかでインストールに失敗した場合は、処理が続行され、展開内の次のセカンダリノードでインストールが実行されます。

2 ノード展開の一部であるプライマリ PAN からパッチのインストールを実行するときは、Cisco によってそのパッチが展開内のプライマリノードとセカンダリノードにインストールされます。パッチのインストールがプライマリ PAN で成功すると、Cisco はセカンダリノードでパッチのインストールを続行します。プライマリ PAN で失敗した場合は、インストールはセカンダリノードに進みません。

ソフトウェアパッチのインストール

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。
- **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** > **[PANのフェールオーバー（PAN Failover）]** に移動し、[PANの自動フェールオーバーを有効にする（Enable PAN Auto Failover）] チェックボックスがオフになっていることを確認します。このタスクの期間中は、PAN の自動フェールオーバー設定を無効にする必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[メンテナンス（Maintenance）]** > **[パッチ管理（Patch Management）]** > **[インストール（Install）]** を選択します。

ステップ 2 [参照（Browse）] をクリックし、Cisco.com からダウンロードしたパッチを選択します。

ステップ 3 [インストール（Install）] をクリックしてパッチをインストールします。

PAN でのパッチのインストールが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

（注） パッチインストールの進行中は、[パッチ管理（Patch Management）] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

ステップ 4 インストールしたパッチの横のオプションボタンをクリックし、[ノードステータスを表示（Show Node Status）] をクリックしてインストールが完了したことを確認します。

ソフトウェアパッチのロールバック

複数のノードの展開の一部である PAN からパッチのロールバックを実行するときは、Cisco ISEによってそのパッチが展開内のプライマリノードとすべてのセカンダリノードにロールバックされます。

始める前に

- スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）]** を選択します。

ステップ 2 変更をロールバックするパッチバージョンのオプションボタンをクリックしてから、[ロールバック（Rollback）] をクリックします。

（注） パッチのロールバックの進行中は、[パッチ管理（Patch Management）] ページ上の機能のうち、アクセスできるのは **Show Node Status** のみです。

PAN からのパッチのロールバックが完了すると、Cisco ISE から自動的にログアウトされます。再びログインできるようになるまで数分間待つ必要があります。

ステップ 3 ログイン後に、ページの一番下にある [アラーム（Alarms）] リンクをクリックしてロールバック操作のステータスを表示します。

ステップ 4 パッチのロールバックの進行状況を表示するには、[パッチ管理（Patch Management）] ページでパッチを選択し、[ノードステータスを表示（Show Node Status）] をクリックします。

ステップ 5 パッチのオプションボタンをクリックし、セカンダリノード上で [ノードステータスを表示（Show Node Status）] をクリックして、そのパッチが展開内のすべてのノードからロールバックされたことを確認します。

そのパッチがロールバックされていないセカンダリノードがある場合は、そのノードが稼働中であることを確認してから、プロセスをもう一度実行して残りのノードから変更をロールバックしてください。Cisco ISE は、このバージョンのパッチがインストールされているノードからのみパッチをロールバックします。

ソフトウェア パッチ ロールバックのガイドライン

展開の Cisco ISE ノードからパッチをロールバックするには、最初に PAN から変更をロールバックします。これに成功すると、セカンダリノードからパッチがロールバックされます。PAN でロールバックプロセスが失敗した場合は、セカンダリノードからのパッチロールバックは行われません。ただし、いずれかのセカンダリノードでパッチのロールバックが失敗しても、展開内の次のセカンダリノードからのパッチのロールバックは継続されます。

Cisco ISE によるセカンダリノードからのパッチロールバックが進行中のときも、引き続き PAN GUI から他のタスクを実行できます。セカンダリノードは、ロールバック後に再起動されます。

パッチのインストールおよびロールバックの変更の表示

インストールされているパッチに関連するレポートを表示するには、次の手順を実行します。

始める前に

スーパー管理者またはシステム管理者の管理者ロールが割り当てられている必要があります。パッチをインストールまたはロールバックするには、[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] > [パッチ管理（Patch Management）] ページを選択します。展開内の各ノードで特定のパッチのステータス（[インストール済み（installed）]、[処理中（in-progress）]、[未インストール（not installed）]）を確認できます。このためには、特定のパッチを選択し、[ノードステータスを表示（Show Node Status）] ボタンをクリックします。

ステップ 1 **[操作（Operations）] > [レポート（Reports）] > [監査（Audit）] > [操作監査（Operations Audit）]** を選択します。デフォルトでは、過去 7 日間のレコードが表示されます。

ステップ 2 [フィルタ（Filter）] ドロップダウンをクリックして [クイックフィルタ（Quick Filter）] または [高度なフィルタ（Advanced Filter）] を選択し、必要なキーワード（例：patch install iniated）を使用して、インストール済みのパッチを示すレポートを生成します。

バックアップ データのタイプ

Cisco ISE では、プライマリ PAN とモニタリングノードからデータをバックアップできます。バックアップは CLI またはユーザー インターフェイスから実行できます。

Cisco ISE では次のタイプのデータのバックアップが可能です。

- 設定データ：アプリケーション固有および Cisco ADE オペレーティング システム両方の設定データが含まれます。バックアップは、GUI または CLI を使用してプライマリ PAN を介して実行できます。
- 運用データ：モニタリングおよびトラブルシューティング データが含まれます。バックアップは、プライマリ PAN GUI を介して、またはモニタリングノードの場合は CLI を使用して実行できます。

Cisco ISE が VMware で実行されている場合、ISE データをバックアップするのに、VMware スナップショットはサポートされていません。

（注） Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータが現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。シスコは、データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットまたはサードパーティのバックアップサービスを使用して Cisco ISE データをバックアップすると、Cisco ISE サービスが割り込まれることがあります。バックアップが VMware または CommVault SAN レベルのバックアップのようなサードパーティのバックアップサービスによって開始された場合、ファイルシステムを休止してクラッシュ整合を維持するために、Cisco ISE 機能がフリーズする可能性があります。Cisco ISE 展開でサービスを再開するには再起動が必要です。

復元操作は、以前のバージョンの Cisco ISE のバックアップファイルを使用して実行でき、以前のバージョンが以降のバージョンでサポートされている直接アップグレードパスにある場合、以降のバージョンで復元できます。。

Cisco ISE リリース 2.7 は、リリース 2.2 以降から取得したバックアップからの復元をサポートしています。

（注） データをバックアップおよび復元した後に展開を再作成するときに、両方のノードのデータが同期されるようにするには、プライマリ PAN とセカンダリ PAN の両方の **[コンテキストの可視性リセット（Context Visibility Reset）]** が必要です。

バックアップ/復元リポジトリ

Cisco ISE では管理者ポータルを使用してリポジトリを作成および削除できます。次のタイプのリポジトリを作成できます。

- ディスク（DISK）
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

（注） リポジトリは、各デバイスに対してローカルです。

どのタイプの展開（小規模、中規模、大規模）であっても、最低でも 100 GB のリポジトリ サイズを用意することを推奨します。

次の表に、Cisco ISE の操作と外部リポジトリのタイプ間でのサポート情報を示します。

表 *1:* 外部リポジトリのサポート マトリックス

リポジトリ タイプ（**Repository Type**）	バックアップの設定	復元の設定	のアップグレード	操作バックアップ	復元操作	サポート バンドル	ユーザー インターフェイスからの検証	ユーザー インターフェイスからのレポートのエクスポート	ユーザー インターフェイスからのポリシーのエクスポート
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	X	X	X	X	X	X	X	X	X
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

リポジトリの作成

リポジトリを作成するには、CLI と GUI を使用できます。次の理由により、GUI を使用することを推奨します。

- CLI で作成されたリポジトリはローカルに保存され、他の展開ノードに複製されません。これらのリポジトリは、GUI のリポジトリ ページに表示されません。
- プライマリ PAN で作成されたリポジトリが他の展開ノードに複製されます。

キーはプライマリ PAN でのみ GUI で生成されます。このため、アップグレード時に新しいプライマリ管理ノードの GUI でキーを再生成して、SFTP サーバーにエクスポートする必要があります。展開からノードを除去する場合、管理対象以外のノードの GUI でキーを生成し、SFTP サーバーにエクスポートする必要があります。

RSA 公開キー認証を使用する Cisco ISE の SFTP リポジトリを設定できます。データベースとログを暗号化するために管理者が作成したパスワードを使用する代わりに、セキュア キーを使用する RSA 公開キー認証を選択できます。RSA 公開キーを使用して作成された SFTP リポジトリの場合、GUI から作成されたリポジトリは CLI では複製されず、CLI から作成されたリポジトリは GUI では複製されません。CLI と GUI で同じリポジトリを設定するには、CLI と GUI の両方で RSA 公開キーを生成し、この両方のキーを SFTP サーバーにエクスポートします。

（注） Cisco ISE は、FIPS モードが ISE で有効になっていない場合でも、FIPS モードで発信 SSH または SFTP 接続を開始します。ISE と通信するリモート SSH または SFTP サーバーが FIPS 140 承認暗号化アルゴリズムを許可していることを確認します。

Cisco ISE では、組み込みの FIPS 140 の検証済み暗号化モジュールが使用されています。FIPS コンプライアンスの要求の詳細については、『FIPS Compliance Letter』を参照してください。

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。
- RSA 公開キー認証を使用して SFTP リポジトリを作成する場合は、次の手順を実行します。
  - SFTP リポジトリの RSA 公開キー認証を有効にします。
  - 管理 CLI ユーザーとしてログインする必要があります。**crypto host_key add** コマンドを使用して Cisco ISE CLI から SFTP サーバーのホスト キーを入力します。ホストキー文字列は、リポジトリの設定ページで、[パス（Path）] フィールドに入力したホスト名と一致する必要があります。
  - GUI でキーペアを生成し、ローカル システムに公開キーをエクスポートします。Cisco ISE CLI から **crypto key generate rsa passphrase** *test123* コマンドを使用してキーペアを生成し（この場合パスフレーズは 5 文字以上でなければなりません）、キーを任意のリポジトリ（ローカルディスクまたは設定されているその他のリポジトリ）にエクスポートします。
  - エクスポートした RSA 公開キーを PKI 対応の SFTP サーバーにコピーし、「authorized_keys」ファイルに追加します。

ステップ 1 [管理（Administration）]>[システム（System）]>[メンテナンス（Maintenance）]>[リポジトリ（Repository）] を選択します。

ステップ 2 [追加（Add）] をクリックして、新しいリポジトリを追加します。

ステップ 3 新しいリポジトリのセットアップの必要に応じて値を入力します。フィールドの説明については、リポジトリの設定 （16 ページ）を参照してください。

ステップ 4 [送信（Submit）] をクリックしてリポジトリを作成します。

ステップ 5 左側の [操作（Operations）] ナビゲーションペインで [リポジトリ（Repository）] をクリックするか、または [リポジトリ（Repository）] ウィンドウ上部の [リポジトリリスト（Repository List）] リンクをクリックして、リポジトリのリスト ページに移動して、リポジトリが正常に作成されていることを確認します。

次のタスク

- 作成したリポジトリが有効であることを確認します。これは、[リポジトリのリスト（Repository Listing）] ウィンドウから行います。対応するリポジトリを選択し、[検証（Validate）] をクリックします。また、Cisco ISE コマンドライン インターフェイスから次のコマンドを実行することもできます。

  show repository *repository_name*

  ここで、*repository_name* は作成したリポジトリの名前です。

（注） リポジトリの作成時に指定したパスが存在しない場合、次のエラーが表示されます。

```
%Invalid Directory
```

- オンデマンド バックアップを実行するかバックアップのスケジュールを設定します。

リポジトリの設定

表 *2:* リポジトリの設定

フィールド	使用上のガイドライン
リポジトリ（**Repository**）	リポジトリの名前を入力します。最大 80 文字の英数字を使用できます。
[Protocol]	使用する使用可能なプロトコルの 1 つを選択します。

フィールド	使用上のガイドライン
サーバー名（Server Name）	（TFTP、HTTP、HTTPS、FTP、SFTP、およびNFS で必須）リポジトリの作成先サーバーのホスト名または IP アドレス（IPv4 または IPv6）を入力します。 （注） IPv6 アドレスを使用してリポジトリを追加する場合は、IPv6 アドレスを使用して ISE eth0 インターフェイスが設定されていることを確認します。
Path	リポジトリへのパスを入力します。このパスは、リポジトリの作成時に有効であり、存在している必要があります。 この値は、サーバーのルート ディレクトリを示す 2 つのスラッシュ（//）または単一のスラッシュ（/）で開始できます。ただし、FTP プロトコルの場合は、単一のスラッシュ（/）はルートディレクトリではなく、ローカル デバイス ホーム ディレクトリの FTP を示します。
PKI 認証を有効にします。	（オプション：SFTP リポジトリにのみ適用）SFTP リポジトリで RSA 公開キー認証を有効にするには、このチェック ボックスをオンにします。
[User Name]	（FTP、SFTP で必須）指定されたサーバーに対する書き込み権限を持つユーザー名を入力します。ユーザー名には、英数字と _-. /@\$ 文字を含めることができます。
[Password]	（FTP、SFTP で必須）指定されたサーバーへのアクセスに使用するパスワードを入力します。パスワードに使用できる文字は、0 ～ 9、a ～ z、A ～ Z、-、.、|、@、#、$、^、&、*、,、+、および = です。

関連トピック

バックアップ/復元リポジトリ （13 ページ）
リポジトリの作成 （14 ページ）

SFTP リポジトリでの RSA 公開キー認証の有効化

SFTP サーバーでは、各ノードに 2 つの RSA 公開キー（CLI 用と GUI 用にそれぞれ 1 つずつ）が必要です。SFTP リポジトリで RSA 公開キー認証を有効にするには、次の手順を実行します。

（注） SFTP リポジトリで RSA 公開キー認証を有効にすると、SFTP ログイン情報を使用してログインできなくなります。PKI ベースの認証またはログイン情報ベースの認証を使用できます。ログイン情報ベースの認証を再度使用する場合は、SFTP サーバーから公開キーペアを削除する必要があります。

ステップ 1 */Etc/ssh/sshd_config.file* を編集する権限を持つアカウントで SFTP サーバーにログインします。

（注） *sshd_config* ファイルのロケーションは、インストールされているオペレーティング システムによって異なる可能性があります。

ステップ 2 **vi etc/ssh/sshd_config** コマンドを入力します。

Sshd_config ファイルの内容がリストされます。

ステップ 3 RSA 公開キー認証を有効にするには、以下の行の「#」記号を削除します。

- RSAAuthentication yes
- PubkeyAuthentication yes

（注） Public Auth Key が no の場合は yes に変更してください。

- AuthorizedKeysFile ~/.ssh/authorized_keys

オンデマンドおよびスケジュール バックアップ

プライマリ PAN とプライマリ モニタリング ノードのオンデマンドバックアップを設定できます。バックアップデータがすぐに必要な場合にオンデマンドバックアップを実行します。

システムレベルのバックアップは、1 回のみ、毎日、毎週、または毎月実行するようにスケジュールできます。バックアップ操作は長時間かかる場合がありますが、スケジュールできるため中断が発生することはありません。管理者ポータルからバックアップをスケジュールできます。

（注） 内部 CA を使用している場合は、CLI を使用して証明書とキーをエクスポートする必要があります。管理ポータルでのバックアップでは、CA チェーンはバックアップされません。

詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Basic Setup」の章にある「Export Cisco ISE CA Certificates and Keys」の項を参照してください。

Cisco ISE の設定バックアップおよび運用バックアップは、短時間でシステムがオーバーロードになる可能性があります。この一時的なシステムオーバーロードで予想される動作は、システムの設定とモニタリングデータベースのサイズによって異なります。

関連トピック

メンテナンスの設定

オンデマンド バックアップの実行

オンデマンドバックアップを実行して、設定データまたはモニタリング（運用）データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書も元のターゲットの証明書も使用されません。元のソースシステムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- オンデマンドバックアップを実行する前に、Cisco ISE 内のバックアップデータタイプの基本を理解しておく必要があります。
- バックアップファイルを保存するためのリポジトリが作成されていることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- バックアップを取得する前に、すべての証明書関連の変更を実行します。

- 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。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、またはTFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。バックアップを復元するには、リポジトリを選択し、[復元（Restore）] をクリックします。

関連トピック

Cisco ISE 復元操作 （25 ページ）
認証および許可ポリシー設定のエクスポート （32 ページ）

オンデマンド バックアップの設定

次の表では、バックアップを任意の時点で取得するために使用できる**[オンデマンドバックアップ（On-Demand Backup）]** ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[管理（Administration）]** > **[システム（System）]** > **[バックアップ/復元（Backup & Restore）]** です。

表 *3:* オンデマンド バックアップの設定

フィールド名	使用上のガイドライン
タイプ	次のいずれかを選択します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
バックアップ名（Backup Name）	バックアップ ファイルの名前を入力します。
リポジトリ名（Repository Name）	バックアップ ファイルを保存するリポジトリ。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
Encryption Key	このキーは、バックアップ ファイルの暗号化および解読に使用されます。

関連トピック

バックアップ データのタイプ （12 ページ）
オンデマンドおよびスケジュール バックアップ （18 ページ）
バックアップ履歴 （24 ページ）
バックアップの失敗 （24 ページ）
Cisco ISE 復元操作 （25 ページ）
認証および許可ポリシー設定のエクスポート （32 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （33 ページ）
オンデマンド バックアップの実行 （19 ページ）

バックアップのスケジュール

オンデマンドバックアップを実行して、設定データまたはモニタリング（運用）データを即座にバックアップすることができます。復元操作では、バックアップ取得時の設定状態に Cisco ISE が復元されます。

重要 バックアップと復元を行う場合、復元によってターゲットシステム上の信頼できる証明書のリストがソースシステムの証明書のリストによって上書きされます。バックアップおよび復元機能に内部認証局（CA）の証明書に関連付けられた秘密キーが含まれないことに注意することが非常に重要です。

1 つのシステムから別のシステムにバックアップと復元を行う場合は、エラーを回避するために、次のオプションのいずれかを選択する必要があります。

- **オプション 1**：

  CA 証明書をソース ISE ノードから CLI を使用してエクスポートし、ターゲット システムに CLI を使用してインポートします。

  長所：ソースシステムからエンドポイントに発行されたすべての証明書が引き続き信頼されます。ターゲット システムによって発行された新しい証明書は、同じキーによって署名されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

- **オプション 2**：

  復元処理の後、内部 CA のすべての新しい証明書を生成します。

  長所：このオプションは推奨される適切な方法です。元のソースの証明書または元のターゲットの証明書が使用されます。元のソース システムによって発行された証明書は引き続き信頼されます。

  短所：復元機能を使用する前にターゲットシステムによって発行された証明書は信頼されないため、再発行する必要があります。

始める前に

- バックアップをスケジュールする前に、Cisco ISE 内のバックアップデータタイプの基本を理解しておく必要があります。
- リポジトリを設定していることを確認します。
- ローカルリポジトリを使用してバックアップしないでください。リモート モニタリング ノードのローカル リポジトリで、モニタリング データをバックアップすることはできません。
- 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。

（注） バックアップ/復元操作では、次のリポジトリ タイプはサポートされていません。CD-ROM、HTTP、HTTPS、または TFTP。これは、これらのリポジトリ タイプが読み取り専用であるか、またはプロトコルでファイルのリストがサポートされないためです。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 [作成（Create）][スケジュール（Schedule）]をクリックして、設定または操作バックアップをスケジュールします。

ステップ 3 必要に応じてバックアップをスケジュールするための値を入力します。

ステップ 4 [保存（Save）] をクリックして、バックアップをスケジュールします。

ステップ 5 次のいずれかの操作を実行します。

- [リポジトリの選択（Select Repository）] ドロップダウンリストから、必要なリポジトリを選択します。
- [リポジトリの追加（Add Repository）] リンクをクリックして新しいリポジトリを追加します。

ステップ 6 [更新（Refresh）] リンクをクリックして、スケジュール バックアップのリストを表示します。

作成できる設定または操作バックアップのスケジュールは 1 回に 1 つだけです。スケジュール バックアップは有効化または無効化できますが、削除はできません。

スケジュール バックアップの設定

次の表では、フルバックアップまたは増分バックアップの復元に使用できる [スケジュールバックアップ（Scheduled Backup）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** です。

Table 4: スケジュール バックアップの設定

フィールド名	使用上のガイドライン
タイプ	次のいずれかを選択します。 • **[設定データのバックアップ（Configuration Data Backup）]**：アプリケーション固有およびCisco ADE オペレーティングシステム両方の構成データが含まれます。 • **[運用データのバックアップ（Operational Data Backup）]**：モニタリングおよびトラブルシューティング データが含まれます。
[Name]	バックアップ ファイルの名前を入力します。任意のわかりやすい名前を入力できます。Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加して、ファイルをリポジトリに格納します。複数のバックアップを作成するように設定しても、一意なバックアップ ファイル名を得ることができます。[スケジュールバックアップ（Scheduled Backup）] リストウィンドウで、ファイル名の先頭に「backup_occur」が追加され、このファイルが **kron** ジョブであることを示します。
説明	バックアップの説明を入力します。
リポジトリ名（**Repository Name**）	バックアップ ファイルを保存するリポジトリを選択します。ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。
Encryption Key	バックアップ ファイルを暗号化および復号化するためのキーを入力します。
スケジューリング オプション（**Schedule Options**）	スケジュール バックアップの頻度を選択し、適宜他のオプションに入力します。

Related Topics

バックアップ データのタイプ （12 ページ）
オンデマンドおよびスケジュール バックアップ （18 ページ）
バックアップ履歴 （24 ページ）
バックアップの失敗 （24 ページ）
Cisco ISE 復元操作 （25 ページ）
認証および許可ポリシー設定のエクスポート （32 ページ）
分散環境でのプライマリ ノードとセカンダリ ノードの同期 （33 ページ）
CLI を使用したバックアップ （24 ページ）
バックアップのスケジュール （21 ページ）

CLI を使用したバックアップ

CLI と GUI の両方からバックアップのスケジュールを設定できますが、GUI の使用を推奨します。ただし、セカンダリ モニタリング ノードの操作バックアップは、CLI からのみ実行できます。

バックアップ履歴

バックアップ履歴は、スケジュールまたはオンデマンドバックアップに関する基本情報です。バックアップ履歴には、バックアップ名、バックアップ ファイルのサイズ、バックアップが保存されているリポジトリ、バックアップが取られたタイム スタンプを表示します。この情報は、操作監査レポートまたは、履歴テーブルの [バックアップ/復元（Backup and Restore）] ページから入手できます。

バックアップが失敗すると、Cisco ISE がアラームをトリガーします。バックアップ履歴ページに失敗の原因が表示されます。障害の原因は操作監査レポートにも記載されます。障害の原因が欠落しているか明確でない場合は、Cisco ISE CLI から **backup-logs** コマンドを実行し、ADE.log でより詳細な情報を確認できます。

バックアップ操作の実行中は、**show backup status** CLI コマンドを使用して、バックアップ操作の進行状況を確認することができます。

バックアップ履歴は、Cisco ADE オペレーティング システムの設定データとともに保存されています。つまり、アプリケーションのアップグレード後もそこに残っており、PAN のイメージを再作成した場合にのみ削除されます。

バックアップの失敗

バックアップが失敗した場合は、次を確認してください。

- NTP 同期またはサービス障害の問題があるかどうかを確認します。Cisco ISE の NTP サービスが動作していない場合、Cisco ISE では、[NTPサービスの障害（NTP Service Failure）] のアラームが発生します。Cisco ISE が、設定されているすべての NTP サーバーと同期できない場合、Cisco ISE では、[NTP同期に失敗（NTP Sync Failure）] のアラームが発生します。NTP サービスがダウンしている場合、または同期の問題がある場合は、Cisco ISE のバックアップが失敗する可能性があります。バックアップ操作を再試行する前に、[アラーム（Alarm）] ダッシュレットを確認し、NTP 同期またはサービスの問題を修正してください。
- 他のバックアップが同時に実行されていないことを確認します。
- 設定したリポジトリの使用可能なディスク領域を確認します。
  - （操作）バックアップのモニタリングは、モニタリング データがモニタリング データベースに割り当てられたサイズの 75% を超えると失敗します。たとえばモニタリング ノードに 600 GB 割り当てられており、モニタリング データがストレージの 450 GB を超える領域を消費すると、モニタリングのバックアップは失敗します。

- データベースのディスク使用量が 90% を超える場合、消去が発生してデータベースを割り当てられたサイズの 75% 以下のサイズにします。

- 消去が進行中かどうかを確認します。消去の進行中はバックアップ/復元操作は動作しません。
- リポジトリが正しく設定されていることを確認します。

Cisco ISE 復元操作

プライマリまたはスタンドアロン 管理ノードで設定データを復元できます。プライマリ PAN にデータを復元したら、手動でセカンダリ ノードをプライマリ PAN と同期する必要があります。

運用データを復元するプロセスは、展開のタイプによって異なります。

（注） Cisco ISE の新しいバックアップ/復元ユーザー インターフェイスでは、バックアップ ファイル名にメタデータが使用されます。したがって、バックアップが完了後に、バックアップ ファイル名を手動で変更しないでください。バックアップ ファイルの名前を手動で変更すると、Cisco ISE バックアップ/復元ユーザー インターフェイスがそのバックアップ ファイルを認識できなくなります。バックアップ ファイル名を変更しなければならない場合は、バックアップの復元に Cisco ISE CLI を使用する必要があります。

データの復元に関するガイドライン

次は、Cisco ISE バックアップ データを復元する場合に従うべきガイドラインです。

- Cisco ISE では、ある ISE ノード（A）からバックアップを取得して、別の ISE ノード（B）に復元することができます。両方のノードは同じホスト名（IP アドレスは異なる）です。ただし、ノード B 上のバックアップを復元した後は、証明書とポータル グループ タグの問題が生じる可能性があるため、ノード B のホスト名を変更することはできません。
- あるタイムゾーン内のプライマリ PAN からバックアップを取得して、別のタイムゾーン内の別の Cisco ISE ノードに復元する場合、復元プロセスが失敗することがあります。この問題は、バックアップ ファイルのタイムスタンプが、バックアップが復元される Cisco ISE ノードのシステム時刻より新しい場合に発生します。同じバックアップを、取得後 1 日経過してから復元すると、バックアップ ファイルのタイムスタンプが過去のものになり、復元プロセスは成功します。
- バックアップを取得したホスト名と別のホスト名を持つプライマリ PAN にバックアップを復元すると、プライマリ PAN はスタンドアロン ノードになります。展開が切断し、セカンダリ ノードは機能しなくなります。スタンドアロン ノードをプライマリ ノードにし、セカンダリ ノードの設定をリセットしてプライマリ ノードに再登録する必要があります。

Cisco ISE ノードの設定をリセットするには、Cisco ISE CLI から次のコマンドを入力してください。

- **application reset-config ise**

- システムのタイムゾーンは、最初の Cisco ISE インストールおよびセットアップ後に変更しないことを推奨します。
- 展開の 1 つ以上のノードの証明書設定を変更した場合は、データを復元するための別のバックアップをスタンドアロン Cisco ISE ノードまたはプライマリ PAN から取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。
- プライマリ PAN 上で設定バックアップを復元した後に、以前にエクスポートした Cisco ISE CA 証明書およびキーをインポートできます。

Note Cisco ISE CA 証明書およびキーをエクスポートしなかった場合は、プライマリ PAN 上で設定バックアップを復元した後に、プライマリ PAN およびポリシー サービス ノード（PSN）でルート CA および下位 CA を生成します。

- 適切な FQDN（プラチナ データベースの FQDN）を使用せずにプラチナ データベースを復元する場合は、CA 証明書を再生成する必要があります。（[管理（Administration）]>[証明書（Certificates）]>[証明書署名要求（Certificate Signing Requests）]>[ISE ルート CA 証明書チェーンの置き換え（Replace ISE Root CA certificate chain）] を選択します）。ただし、適切な FQDN でプラチナ データベースを復元する場合は、CA 証明書が自動的に再生成されます。
- Cisco ISE がバックアップ ファイルを格納するデータ リポジトリが必要です。オンデマンドまたはスケジュール設定されたバックアップを実行する前に、リポジトリを作成する必要があります。
- スタンドアロン管理ノードに障害が発生した場合、設定バックアップを実行して復元する必要があります。プライマリ PAN で障害が発生した場合、分散セットアップを使用してセカンダリ管理ノードをプライマリに昇格できます。その後、新しいプライマリ PAN にデータを復元できます。

Note Cisco ISE では、**backup-logs** CLI コマンドも使用できます。このコマンドを使用して、ログやコンフィギュレーション ファイルの収集を行い、これらをトラブルシューティングに利用できます。

CLI からの設定またはモニターリング（操作）バックアップの復元

Cisco ISE CLI から設定データを復元するには、EXEC モードで **restore** コマンドを使用します。設定または操作バックアップからデータを復元するには、次のコマンドを使用します。

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

構文の説明

restore	設定または操作バックアップからデータを復元するには、このコマンドを入力します。
filename	リポジトリに存在するバックアップ ファイルのファイル名。120 文字までの英数字で指定します。 **Note** ファイル名の後に、tar.gpg という拡張子を付ける必要があります（myfile.tar.gpg など）。
repository	バックアップを含むリポジトリを指定します。
repository-name	バックアップを復元するリポジトリの名前。
encryption-key	（オプション）バックアップを復元するユーザー定義の暗号キーを指定します。
hash	バックアップを復元するためのハッシュされた暗号キー。使用する暗号化された（ハッシュ化された）暗号化キーを指定します。40 文字までで指定します。
plain	バックアップを復元するためのプレーンテキストの暗号キー。使用する暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。
encryption-key name	暗号キーを入力します。
include-adeos	（オプション、設定バックアップのみに該当）設定バックアップから ADE-OS 設定を復元する場合に、このコマンド オペレータ パラメータを入力します。設定バックアップを復元する場合にこのパラメータを含めないと、Cisco ISE は Cisco ISE アプリケーション設定データのみを復元します。

デフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

使用上のガイドライン

Cisco ISE で restore コマンドを使用すると、Cisco ISE サーバーが自動的に再起動します。

データの復元処理で、暗号キーはオプションです。暗号キーを指定しなかった以前のバックアップの復元をサポートするために、暗号キーなしで **restore** コマンドを使用できます。

例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

関連コマンド

	説明
backup	バックアップ（Cisco ISE と Cisco ADE OS）を実行して、そのバックアップをリポジトリに保存します。
backup-logs	システム ログをバックアップします。
repository	バックアップを設定するためにリポジトリ サブモードに入ります。
show repository	特定のリポジトリにある使用可能なバックアップ ファイルを表示します。
show backup history	システムのバックアップ履歴を表示します。
show backup status	バックアップ操作のステータスを表示します。
show restore status	復元操作のステータスを表示します。

いずれかのセカンダリ ノードでアプリケーション復元後の同期ステータスおよび複製ステータスが [非同期（Out of Sync）] になっている場合、該当セカンダリ ノードの証明書をプライマリ PAN に再インポートして、手動同期を実行する必要があります。

GUI からの設定バックアップの復元

管理者ポータルで設定バックアップを復元できます。

始める前に

プライマリ PAN の自動フェールオーバー構成が展開で有効になっている場合はオフにします。設定バックアップを復元すると、アプリケーション サーバー プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ PAN の自動フェールオーバーが開始される場合があります。

構成のバックアップ時に展開がデュアルノード展開の場合は、次のことを確認します。

- 復元のソースノードとターゲットノードは、構成のバックアップに使用されたものと同じで、ターゲットノードはスタンドアロンまたはプライマリのいずれかです。
- 復元のソースノードとターゲットノードは、構成のバックアップで使用されたものとは異なり、ターゲットノードはスタンドアロンである必要があります。

（注） 構成データベースのバックアップを復元し、プライマリ PAN でのみルート CA を再生成することができます。ただし、登録済みの PAN でコンフィギュレーション データベースのバックアップは復元できません。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を設定バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

次のタスク

Cisco ISE CA サービスを使用する場合は、次のことを実行する必要があります。

1. Cisco ISE CA ルート チェーン全体を再生成します。
2. Cisco ISE CA 証明書およびキーのバックアップをプライマリ PAN から取得し、セカンダリ PAN で復元します。これにより、プライマリ PAN の障害が発生した場合に、セカンダリ PAN が外部 PKI のルート CA または下位 CA として機能するようになり、セカンダリ PAN をプライマリ PAN に昇格させることができます。

モニターリング データベースの復元

モニタリングデータベースを復元するプロセスは、展開のタイプによって異なります。次の項では、スタンドアロンおよび分散展開でモニタリングデータベースを復元する方法について説明します。

Cisco ISE の以前のリリースからのオンデマンド モニタリング データベースのバックアップを復元するには、CLI を使用する必要があります。Cisco ISE リリース間でのスケジュール バックアップの復元はサポートされていません。

（注） データが取得されたノードとは別のノードにデータを復元しようとする場合、新しいノードを指すロギング ターゲット設定を設定する必要があります。これにより、モニタリング syslog が正しいノードに送信されるようになります。

スタンドアロン環境でのモニターリング（運用）バックアップの復元

GUIには現在のリリースから取得されたバックアップのみが表示されます。前のリリースから取得されたバックアップを復元するには、CLI から restore コマンドを使用します。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup and Restore）]** を選択します。

ステップ 2 バックアップの名前を操作バックアップのリストから選択し、[復元（Restore）] をクリックします。

ステップ 3 バックアップ時に使用した暗号キーを入力します。

ステップ 4 [復元（Restore）] をクリックします。

管理およびモニタリングペルソナによるモニタリング バックアップの復元

管理およびモニタリングペルソナを使用して、分散環境でのモニタリングバックアップを復元することができます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 プライマリとセカンダリ PAN を使用している場合は、PAN と同期します。

PAN と同期する場合、PAN を選択し、それをアクティブなプライマリに昇格させる必要があります。

ステップ 2 モニタリング ノードを登録解除する前に、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開ごとに、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 3 バックアップするモニタリングノードを登録解除します。

ステップ 4 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 5 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 6 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

モニタリング ペルソナによるモニタリング バックアップの復元

分散環境のモニタリング バックアップは、モニタリング ペルソナによってのみ復元できます。

始める前に

- 古いモニタリング データを消去します。
- バックアップをスケジュールするか、オンデマンド バックアップを実行します。

ステップ 1 復元されるノードの登録を解除する準備をします。これを行うには、モニタリング ペルソナを展開内の別のノードに割り当てます。

展開内に、機能中のモニタリング ノードが少なくとも 1 つ必要です。

ステップ 2 復元されるノードを登録解除します。

（注） 登録解除が完了するのを待機してから、復元に進みます。復元を続行する前に、ノードがスタンドアロン状態になっている必要があります。

ステップ 3 新しく登録解除されたノードにモニタリング バックアップを復元します。

ステップ 4 現在の管理ノードにより新たに復元されたノードを登録します。

ステップ 5 新たに復元されて登録されたノードをアクティブなモニタリング ノードに昇格します。

復元履歴

[操作監査レポート（Operations Audit Report）] ウィンドウから、すべての復元操作、ログイベント、ステータスに関する情報を取得できます。

（注） ただし [操作監査レポート（Operations Audit Report）] には、前回の復元操作に対応する開始時間に関する情報はありません。

トラブルシューティング情報を入手するには、Cisco ISE CLI から **backup-logs** コマンドを実行して、ADE.log ファイルを調べる必要があります。

復元操作の進行中は、すべての Cisco ISE サービスは停止します。**show restore status** CLI コマンドを使用して、復元操作の進行状況を確認できます。

認証および許可ポリシー設定のエクスポート

認証および許可ポリシー設定を XML ファイルの形式でエクスポートし、これをオフラインで読み取って設定エラーを特定し、トラブルシューティングのために使用できます。この XML ファイルには認証および認可ポリシールール、単純および複合ポリシー条件、任意アクセス制御リスト（DACL）、および認証プロファイルが含まれます。XML ファイルを電子メールで送信するか、ローカル システムに保存することを選択できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [バックアップと復元（Backup & Restore）]** を選択します。

ステップ 2 [ポリシーのエクスポート（Policy Export）] をクリックします。

ステップ 3 必要に応じて値を入力します。

ステップ 4 [エクスポート（Export）] をクリックします。

XML ファイルの内容を表示するには、ワードパッドなどのテキスト エディタを使用します。

ポリシーのエクスポート設定のスケジュール

次の表では、[ポリシーのエクスポートのスケジュール（Schedule Policy Export）] ウィンドウのフィールドについて説明します。このウィンドウへのナビゲーションパスは、**[管理（Administration）] > [システム（System）] > [バックアップ/復元（Backup and Restore）] > [ポリシーのエクスポート（Policy Export）]** です。

表 *5:* ポリシーのエクスポート設定のスケジュール

分散環境でのプライマリノードとセカンダリノードの同期

分散環境では、PANのバックアップファイルの復元後に、プライマリおよびセカンダリノードの Cisco ISE データベースが自動的に同期されないことがあります。この場合には、PAN からセカンダリ ISE ノードへの完全複製を手動で強制実行できます。強制同期は、PANからセカンダリ ノードにのみ可能です。同期操作中は、設定を変更することはできません。Cisco ISE では、同期が完全に完了した後にのみ、他の Cisco ISE 管理者ポータル ページに移動して設定変更を行うことができます。

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である必要があります。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択します。

ステップ 2 非同期レプリケーション ステータスのセカンダリ ISE ノードの横にあるチェックボックスをオンにします。

ステップ 3 [同期を更新（Syncup）] をクリックし、ノードが PAN と同期されるまで待ちます。Cisco ISE 管理者ポータルへのアクセスは、このプロセスが完了するのを待たなければなりません。

スタンドアロンおよび分散展開での失われたノードの復元

この項では、スタンドアロンおよび分散展開での失われたノードの復元に使用できるトラブルシューティング情報を提供します。次の使用例の一部では、失われたデータの復旧にバックアップと復元機能を使用し、その他の使用例では、複製機能を使用しています。

分散展開での既存IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。復元後に、既存 IP アドレスとホストネームを使用します。

たとえば、2 つのノード、N1（プライマリ ポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリ ポリシー管理ノードすなわちセカンダリ PAN）があります。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。

前提

展開内のすべての Cisco ISE ノードが破壊されました同じホスト名と IP アドレスを使用して、新しいハードウェアのイメージが作成されました。

解決手順（Resolution Steps）

1. N1 および N2 ノードの両方を置き換える必要があります。N1 および N2 ノードはスタンドアロン構成になりました。
2. N1 と N2 のノードの UDI を使用してライセンスを取得し、N1 ノードにインストールします。
3. 置き換えた N1 ノードでバックアップを復元する必要があります。復元スクリプトは N2 にデータを同期しようとしますが、N2 はスタンドアロン ノードであるため同期は失敗します。N1 のデータは時刻 T1 にリセットされます。
4. N1 の管理者ポータルにログインして、N2 ノードを削除して再登録する必要があります。これで、N1 および N2 ノードのデータが時刻 T1 にリセットされます。

分散展開の新IPアドレスとホスト名を使用しての失われたノードの復元

シナリオ

分散展開では、自然災害が全ノードの損失につながります。新しいハードウェアのイメージが新しい場所で再作成され、新しい IP アドレスとホスト名が必要です。

たとえば、2 つの ISE、ノード N1（プライマリポリシー管理ノード（プライマリ PAN））と N2（セカンダリ ポリシー サービス ノード）があるとします。時刻 T1 に取得された N1 ノードのバックアップが利用可能です。自然災害のために、N1 と N2 両方のノードに障害が発生しました。Cisco ISE ノードが新しいロケーションで置き換えられ、新しいホスト名は N1A（プライマリ PAN）および N2A（セカンダリ ポリシー サービス ノード）です。N1A および N2A はこの時点ではスタンドアロン ノードです。

前提条件

展開内のすべての Cisco ISE ノードが破壊されました新しいハードウェアのイメージが、異なるホスト名と IP アドレスを使用して異なる場所で作成されました。

解決手順（Resolution Steps）

1. N1 のバックアップを入手し、これを N1A 上で復元します。復元スクリプトは、ホスト名とドメイン名の変更を認識し、現在のホスト名に基づいて展開設定内のホスト名とドメイン名を更新します。
2. 新しい自己署名証明書を生成する必要があります。
3. N1A で Cisco ISE 管理者ポータルにログインし、**[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択して、次の操作を行う必要があります。

   古い N2 ノードを削除します。

   新しい N2A ノードをセカンダリ ノードとして登録します。N1A ノードのデータが N2A ノードに複製されます。

スタンドアロン展開の既存IPアドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノードN1があったとします。N1データベースのバックアップは、時刻 T1 に取得されました。物理的な障害により N1 ノードがダウンし、イメージの再作成または新しいハードウェアが必要です。N1 ノードを、同じ IP アドレスとホスト名を使用して回復させる必要があります。

前提条件

この展開はスタンドアロン展開であり、新規またはイメージを再作成したハードウェアは、同じ IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

イメージの再作成後、または同一 IP アドレスとホスト名で新しい Cisco ISE ノードを導入した後に N1 ノードが起動したら、古い N1 ノードから取得したバックアップを復元する必要があります。ロールを変更する必要はありません。

スタンドアロン展開の新 IP アドレスとホスト名によるノードの復元

シナリオ

スタンドアロン管理ノードがダウンします。

たとえば、スタンドアロン管理ノード N1 があったとします。時刻 T1 に取得された N1 データベースのバックアップが利用可能です。物理的な障害により N1 ノードがダウンし、異なる IP アドレスとホスト名を使用した新しいハードウェアに別のロケーションで置き換えられます。

前提条件

これはスタンドアロン展開であり、置き換えられたハードウェアは、異なる IP アドレスとホスト名を持ちます。

解決手順（Resolution Steps）

1. 新しいハードウェアで N1 ノードを置き換えます。このノードはスタンドアロン状態となり、ホスト名は N1B です。
2. バックアップを N1B ノード上で復元できます。ロールを変更する必要はありません。

コンフィギュレーション ロールバック

問題

意図せずに設定を変更してしまい、後でそれが正しくないことがわかる場合があります。たとえば、いくつかの NAD を削除したり、一部の RADIUS 属性を誤って修正したりして、数時間後にこの問題に気付く場合があります。この場合、変更を行う前に取得したバックアップを復元することにより、元の構成に戻すことができます。

考えられる原因

N1（プライマリポリシー管理ノードすなわちプライマリ PAN）と N2（セカンダリポリシー管理ノードすなわちセカンダリ PAN）の 2 つのノードがあり、N1 ノードのバックアップを使用できます。N1 上で誤った変更をいくつか行い、変更を元に戻す必要があります。

ソリューション

誤った設定変更を行う前に取得したN1ノードのバックアップを入手します。N1 ノード上でこのバックアップを復元します。復元スクリプトにより、N1 のデータで N2 が同期されます。

分散展開での障害発生時のプライマリ ノードの復元

シナリオ

マルチノード展開内で、PAN に障害が発生しました。

たとえば、2 つの Cisco ISE ノード、N1（PAN）と N2（セカンダリ管理ノード）があります。ハードウェアの問題で N1 に障害が発生します。

前提条件

分散展開内のプライマリ ノードのみに障害が発生します。

解決手順（Resolution Steps）

1. N2 管理者ポータルにログインします。**[管理（Administration）]**>**[システム（System）]**>**[展開（Deployment）]** を選択して、N2 をプライマリノードとして設定します。

   N1 ノードが新しいハードウェアで置き換えられ、イメージが再作成され、スタンドアロン状態となります。

2. N2 管理者ポータルで、セカンダリノードとして新しい N1 ノードを登録します。

   これで、N2 ノードがプライマリ ノードになり、N1 ノードがセカンダリ ノードになります。

N1 ノードを再びプライマリノードにするには、N1 の管理者ポータルにログインして、このノードをプライマリノードに設定します。N2 は、自動的にセカンダリ サーバーとなります。データが失われることはありません。

分散展開での障害発生時のセカンダリ ノードの復元

シナリオ

マルチノード展開で、1 台のセカンダリ ノードに障害が発生しました。復元の必要はありません。

たとえば、N1（プライマリ PAN）、N2（セカンダリ PAN）、N3（セカンダリ ポリシー サービス ノード）、N4（セカンダリ ポリシー サービス ノード）の複数のノードが存在します。セカンダリ ノードの 1 つである N3 に障害が発生しました。

解決手順（Resolution Steps）

1. 新しい N3A ノードのイメージを再作成して、デフォルトのスタンドアロン状態にします。
2. N1 の管理者ポータルにログインし、N3 ノードを削除します。
3. N3A ノードを登録します。

   N1 から N3A へ、データが複製されます。復元の必要はありません。

Cisco ISE ロギング メカニズム

Cisco ISE には、監査、障害管理、およびトラブルシューティングに使用されるロギング メカニズムが備わっています。このロギング メカニズムは、展開されたサービスの障害状態を識別したり、問題のトラブルシューティングを効率的に行う場合に役立ちます。また、プライマリ ノードのモニタリングおよびトラブルシューティングのロギング出力が一貫した形式で生成されます。

仮想ループバック アドレスを使用してローカル システムにログを収集するように Cisco ISE ノードを設定できます。ログを外部に収集するには、ターゲットと呼ばれる外部 syslog サー

バーを設定します。ログは事前定義された各種のカテゴリに分類されます。ターゲット、シビラティ（重大度）レベルなどに応じてカテゴリを編集することにより、ロギング出力をカスタマイズできます。

ベストプラクティスとして、Cisco ISE のモニタリングおよびトラブルシューティング（MnT）ノードに syslog を送信するようにネットワーク デバイスを設定しないでください。これは、一部のネットワーク アクセス デバイス（NAD）の syslog が失われる可能性があるほか、MnT サーバーが過負荷になりロードの問題が発生するためです。NAD syslog が MnT に直接送信されるように設定されている場合、セッション管理機能が停止します。NAD syslog は、トラブルシューティングのために外部 syslog サーバーに送信できますが、MnT には送信できません。

ノードで ISE メッセージング サービスに障害が発生した場合、プロセス ダウン アラームがトリガーされなくなりました。ノードで ISE メッセージング サービスに障害が発生すると、そのノードでメッセージング サービスが再開されるまで、すべての syslog およびプロセス ダウン アラームが失われます。

この場合、管理者は、Cisco ISE のホーム ウィンドウの [アラーム（Alarm）] ダッシュレットにリストされるキュー リンク エラー アラームを検索する必要があります。アラームをクリックすると、[推奨されるアクション（Suggested Actions）] セクションが含まれた新しいウィンドウが開きます。問題を解決するには、次の手順に従ってください。

Note モニタリング ノードがネットワーク デバイスの syslog サーバーとして設定されている場合、ロギング ソースが次の形式で正しいネットワーク アクセス サーバー（NAS）の IP アドレスを送信することを確認してください。

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

そうしないと、これは NAS の IP アドレスに依存する機能に影響を及ぼすことがあります。

syslog の消去の設定

このプロセスを使用して、ローカル ログ格納期間を設定し、特定の期間後にローカル ログを削除します。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ローカルログ設定（Local Log Settings）]** を選択します。

ステップ 2 [ローカル ログ格納期間（Local Log Storage Period）] フィールドに、設定ソースでログ エントリを保持する最大日数を入力します。

localStore フォルダのサイズが 97 GB に達した場合、ログは設定された [ローカルログの保存期間（Local Log Storage Period）] よりも前に削除されることがあります。

ステップ 3 格納期間が経過する前に既存のログ ファイルを削除するには、[今すぐログを削除（Delete Logs Now）] をクリックします。

ステップ 4 [Save] をクリックします。

Cisco ISE システム ログ

Cisco ISE では、システム ログはロギング ターゲットと呼ばれる場所で収集されます。ターゲットは、ログを収集して格納するサーバーの IP アドレスを参照します。ログをローカルで生成して格納することも、FTP ファシリティを使用して外部サーバーに転送することもできます。Cisco ISE には、次のデフォルト ターゲットがあり、これらはローカル システムのループバック アドレスに動的に設定されます。

- LogCollector：ログ コレクタのデフォルトの syslog ターゲット。
- ProfilerRadiusProbe：プロファイラ Radius プローブのデフォルトの syslog ターゲット。

デフォルトでは、AAA 診断サブカテゴリとシステム診断サブカテゴリのロギング ターゲットは、ディスク領域を減らすために、新規 Cisco ISE インストールまたはアップグレード時に無効になります。これらのサブカテゴリのロギング ターゲットを手動で設定できますが、これらのサブカテゴリのローカル ロギングは常に有効です。

Cisco ISE インストールの最後にローカルに設定されるデフォルトのロギング ターゲットを使用するか、またはログを保存する外部ターゲットを作成することができます。

（注） syslog サーバーが分散展開で設定されている場合、syslog メッセージは MnT ノードではなく認証 PSN から syslog サーバーへ直接送信されます。

関連トピック

Cisco ISE メッセージ コード （41 ページ）

リモート syslog 収集場所の設定

Web インターフェイスを使用して、システム ログ メッセージの送信先になるリモート syslog サーバー ターゲットを作成できます。ログ メッセージは、syslog プロトコル標準（RFC-3164 を参照）に従ってリモート syslog サーバー ターゲットに送信されます。syslog プロトコルはセキュアでない UDP です。

メッセージは、イベントが発生したときに生成されます。イベントは、プログラムの終了時に表示されるメッセージやアラームなどのステータスを表示するものである場合があります。カーネル、メール、ユーザーレベルなど、異なるファシリティから生成されたさまざまなタイプのイベントメッセージがあります。イベントメッセージはシビラティ（重大度）レベルに関連付けられており、管理者はメッセージをフィルタリングし、優先度付けできます。数値コードはファシリティおよびシビラティ（重大度）レベルに割り当てられます。syslog サーバーはイベント メッセージ コレクタで、これらのファシリティからイベント メッセージを収集しま

す。管理者は、シビラティ（重大度）レベルに基づいてメッセージを転送するイベントメッセージコレクタを選択できます。

UDP syslog（ログ コレクタ）はデフォルトのリモート ロギング ターゲットです。このロギングターゲットを無効にした場合、ログコレクタとして動作しなくなり、[ロギングカテゴリ（Logging Categories）] ウィンドウから削除されます。このロギングターゲットを有効にした場合は、[ロギングカテゴリ（Logging Categories）] ウィンドウのログコレクタになります。

（注） デフォルトのリモートロギングターゲット **SecureSyslogCollector** を変更すると、Cisco ISE モニタリングおよびトラブルシューティング ログ プロセッサ サービスが再起動されます。

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 次の必須詳細情報を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [リモート ロギング ターゲット（Remote Logging Targets）] ページに移動し、新しいターゲットが作成されたことを確認します。

その後、ロギングターゲットを、以下のそれぞれのロギング カテゴリにマッピングできます。PSN ノードは、それらのノードで有効になっているサービスに応じて、該当するログをリモートロギング ターゲットに送信します。

- AAA 監査
- AAA の診断
- アカウンティング（Accounting）
- 外部 MDM
- パッシブ ID
- ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
- ポスチャおよびクライアント プロビジョニングの診断（Posture and Client Provisioning Diagnostics）
- プロファイラ

展開内のすべてのノードによって、次のカテゴリのログがロギング ターゲットに送信されます。

- 管理および操作の監査（Administrative and Operational Audit）
- システム診断
- システム統計

Cisco ISE メッセージ コード

ロギング カテゴリは、ACS の機能、フロー、または使用例を説明するメッセージ コードのバンドルです。Cisco ISE では、各ログにはログ メッセージの内容に従ってロギング カテゴリにバンドルされているメッセージ コードが関連付けられています。ロギング カテゴリは、含まれているメッセージの内容を説明する場合に役立ちます。

ロギングカテゴリはロギング設定で役立ちます。各カテゴリには、アプリケーションの要件に応じて設定可能な名前、ターゲット、およびシビラティ（重大度）レベルがあります。

Cisco ISE では、サービスに対して事前定義されたロギング カテゴリ（[ポスチャ（Posture）]、[プロファイラ（Profiler）]、[ゲスト（Guest）]、[AAA（認証、許可、アカウンティング）（AAA (authentication, authorization, and accounting)）] など）が提供されており、これらにログ ターゲットを割り当てることができます。

ロギングカテゴリが [成功した認証（Passed Authentications）] の場合、ローカルロギングを許可するオプションは、デフォルトでは無効になっています。このカテゴリのローカルロギングを有効にすると、運用スペースの使用率が高くなり、iseLocalStore.log とともに prrt-server.log がいっぱいになります。

[成功した認証（Passed Authentications）] のローカルロギングを有効にする場合は、**[管理（Administration）] > [システム（System）] > [ロギング（logging）] > [ロギングカテゴリ（logging Categories）]** に移動し、[カテゴリ（category）] セクションから [成功した認証（Passed Authentications）] をクリックして、[ローカルロギング（Local Logging）] のチェックボックスをオンにします。

関連トピック

メッセージ コードの重大度レベルの設定 （41 ページ）

メッセージ コードの重大度レベルの設定

ログのシビラティ（重大度）レベルを設定し、選択したカテゴリのログが格納されるロギング ターゲットを選択できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択します。

ステップ 2 編集するカテゴリの隣のオプション ボタンをクリックにして、[編集（Edit）] をクリックします。

ステップ 3 必須フィールドの値を変更します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [ロギング カテゴリ（Logging Categories）] ページに移動し、特定のカテゴリに対して行われた設定の変更内容を確認します。

Cisco ISE メッセージ カタログ

可能性があるすべてのログ メッセージと説明を表示するために、[メッセージカタログ（Message Catalog）] ページを使用できます。**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [メッセージカタログ（Message Catalog）]** を選択します。 を選択します。

[ログ メッセージ カタログ（Log Message Catalog）] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。すべての Syslog メッセージを CSV ファイル形式でエクスポートするには、[エクスポート（Export）] を選択します。

Cisco ISE から送信される syslog メッセージの包括的なリスト、syslog メッセージの意味、ローカルおよびリモートターゲットでの syslog メッセージの記録方法については、『Cisco ISE Syslogs』ドキュメントを参照してください。

デバッグ ログ

デバッグ ログにより、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、モニタリングとレポート、および公開キーインフラストラクチャ（PKI）に関する情報が取得されます。過去 30 日間の重大アラームと警告アラーム、および過去 7 日間の情報アラームがデバッグ ログに含まれます。

個々のコンポーネントのデバッグ ログシビラティ（重大度）レベルを設定できます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ローカル サーバーにデバッグ ログを保存できます。

（注） デバッグ ログの設定は、システムをバックアップから復元した場合やアップグレードした場合には保存されません。

関連トピック

デバッグ ログの重大度レベルの設定 （43 ページ）

ノードのロギング コンポーネントの表示

ステップ 1 [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [デバッグ ログ設定（Debug Log Configuration）] を選択します。

ステップ 2 ロギング コンポーネントを表示するノードを選択し、[編集（Edit）] をクリックします。

[デバッグ レベルの設定（Debug Level Configuration）] ページが表示されます。次の詳細情報を表示できます。

- 選択したノードで実行中のサービスに基づくロギング コンポーネントのリスト
- 各コンポーネントの説明
- 個々のコンポーネントに設定されている現在のログ レベル

関連トピック

デバッグ ログの重大度レベルの設定 （43 ページ）

デバッグ ログの重大度レベルの設定

デバッグ ログのシビラティ（重大度）レベルを設定できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[デバッグログの設定（Debug Log Configuration）]** を選択します。

ステップ 2 ノードを選択して、[編集（Edit）] をクリックします。

[デバッグログの設定（Debug Log Configuration）] ページには、選択したノードで実行されているサービス、および個別のコンポーネントに対して設定されている現在のログ レベルに基づいたコンポーネントのリストが表示されます。

ノードまたはコンポーネントで [デフォルトにリセット（Reset to Default）] オプションを使用して、ログ レベルを出荷時のデフォルト値に戻すことができます。

ステップ 3 ログシビラティ（重大度）レベルを設定するコンポーネントを選択し、[編集（Edit）] をクリックします。[ログレベル（Log Level）] ドロップダウン リストから目的のログシビラティ（重大度）レベルを選択し、[保存（Save）] をクリックします。

（注） runtime-AAA コンポーネントのログシビラティ（重大度）レベルを変更すると、サブコンポーネント prrt-JNI のログ レベルも変更されます。サブコンポーネントのログ レベルを変更しても、その親コンポーネントには影響はありません。

関連トピック

デバッグ ログの重大度レベルの設定 （43 ページ）
Cisco ISE デバッグ ログ

エンドポイントのデバッグ ログ コレクタ

特定のエンドポイントの問題をトラブルシューティングするために、IP アドレスまたは MAC アドレスに基づいて、特定のエンドポイントのデバッグ ログをダウンロードできます。その特定のエンドポイント固有のログが、展開内のさまざまなノードから 1 つのファイルに収集されるため、迅速かつ効率的に問題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 ツールは、一度に 1 つのエンドポイントに対してのみ実行できます。ログ ファイルが GUI

に表示されます。1 つのノードまたは展開内のすべてのノードからエンドポイントのログをダウンロードできます。

特定のエンドポイントのデバッグ ログのダウンロード

ネットワーク内の特定のエンドポイントの問題をトラブルシューティングするには、管理者ポータルからデバッグ エンドポイント ツールを使用できます。または、このツールを [認証（Authentications）] ページから実行できます。[認証（Authentications）] ページの [エンドポイント ID（Endpoint ID）] を右クリックして、[エンドポイント デバッグ（Endpoint Debug）] をクリックします。このツールでは、単一ファイルの特定のエンドポイントに関連するすべてのサービスに関するすべてのデバッグ情報が提供されます。

始める前に

デバッグ ログを収集するエンドポイントの IP アドレスまたは MAC アドレスが必要です。

ステップ 1 **[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [エンドポイントデバッグ（Endpoint Debug）]** を選択します。

ステップ 2 [MAC アドレス（MAC Address）] または [IP] オプション ボタンをクリックし、エンドポイントの MAC または IP アドレスを入力します。

ステップ 3 一定の時間が経過した後にログ収集を停止する場合は、[*n* 分後に自動的に無効化（Automatic disable after n Minutes）] チェックボックスをオンにします。このチェックボックスをオンにする場合は、1 ～ 60 分の時間を入力する必要があります。

次のメッセージが表示されます。「エンドポイントデバッグによって、展開のパフォーマンスが低下します。続行しますか?（Endpoint Debug degrades the deployment performance. Would you like to continue?）」

ステップ 4 ログを収集するには、[続行（Continue）] をクリックします。

ステップ 5 手動でログの収集を中止する場合は、[停止（Stop）] をクリックします。

関連トピック

エンドポイントのデバッグ ログ コレクタ （43 ページ）

収集フィルタ

収集フィルタを設定して、モニタリング サーバーおよび外部サーバーに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

モニタリング ノードまたは外部サーバーに syslog メッセージを送信する前に、Cisco ISE は送信する syslog メッセージのフィールドとそれらの値を比較します。一致が見つかった場合、対応するメッセージは送信されません。

（注） 任意の [Attribute] および [Filter Type] に対して収集フィルタ（**[Administration]** > **[System]** > **[Logging]** > **[Collection Filter]**）を設定していて、[Disable account after n days of inactivity] チェックボックス（**[Administration]** > **[Identity Management]** > **[User Authentication Settings]** > **[Disable Account Policy]**）をオンにしている場合、認証成功の syslog メッセージがモニタリングノードにリレーされない結果、アカウントが無効になる可能性があります。

収集フィルタの設定

さまざまな属性のタイプに基づいて複数の収集フィルタを設定できます。フィルタ数を 20 に制限することを推奨します。収集フィルタを追加、編集、または削除できます。

ステップ 1 **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[収集フィルタ（Collection Filters）]** 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 次のリストから**フィルタ タイプ**を選択します。

- ユーザー名（User Name）
- MAC アドレス（MAC Address）
- ポリシー セット名
- NAS IP アドレス
- Device IP Address（デバイス IP アドレス）

ステップ 4 選択したフィルタ タイプの対応する**値**を入力します。

ステップ 5 ドロップダウン リストから**結果**を選択します。結果は、[すべて（All）]、[成功（Passed）]、または [失敗（Failed）] になります。

ステップ 6 [送信（Submit）] をクリックします。

関連トピック

収集フィルタ （44 ページ）
イベント抑制バイパス フィルタ （45 ページ）

イベント抑制バイパス フィルタ

Cisco ISE では、フィルタを設定し、収集フィルタを使用して、一部の syslog メッセージがモニタリング ノードおよび他の外部サーバーに送信されることを抑制できます。場合によっては、これらの抑制されたログ メッセージにアクセスすることが必要になります。Cisco ISE は、設定可能な時間について、ユーザー名などの属性に基づいてイベント抑制をバイパスするオプションを提供します。デフォルトは 50 分ですが、5 分から 480 分（8 時間）の期間を設定でき

ます。イベント抑制バイパスは、設定した後すぐに有効になります。設定した期間が経過すると、バイパス抑制フィルタは失効します。

抑制バイパス フィルタは、Cisco ISE ユーザー インターフェイスの [収集フィルタ（Collection Filters）] ページから設定できます。この機能を使用して、特定の ID（ユーザー）のすべてのログを表示し、その ID の問題をリアルタイムでトラブルシューティングできます。

フィルタは有効または無効にできます。バイパス イベント フィルタで設定した期間が経過すると、フィルタは再度有効にするまで自動的に無効になります。Cisco ISE は設定変更監査レポートでこれらの設定変更を取得します。このレポートは、イベント抑制またはバイパス抑制を設定したユーザー、およびイベントが抑制された期間または抑制がバイパスされた期間に関する情報を提供します。

Cisco ISE レポート

モニターリング機能およびトラブルシューティング機能とともに Cisco Identity Services Engine（ISE）レポートを使用して、集中管理する場所からのトレンドの分析、システム パフォーマンスおよびネットワーク アクティビティのモニターリングを行います。

Cisco ISE はネットワークからログおよび設定データを収集します。その後、表示と分析のために、データがレポートに集約されます。Cisco ISE には、使用可能な事前定義されたレポートが用意されており、必要に応じてカスタマイズできます。

Cisco ISE レポートは事前設定されており、認証、セッショントラフィック、デバイス管理、設定、管理、およびトラブルシューティングに関する情報のカテゴリにグループ化されます。

関連トピック

レポートの実行および表示 （48 ページ）
レポートのエクスポート （49 ページ）
使用可能なレポート （55 ページ）

レポート フィルタ

レポートには、シングルセクション レポートとマルチセクション レポートの 2 種類があります。シングルセクション レポートには 1 つのグリッドが含まれており（RADIUS 認証レポート）、マルチセクション レポートには複数のグリッドが含まれており（認証概要レポート）、データがグラフと表の形式で示されます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

マルチセクション レポートには、入力が必要な必須拡張フィルタが 1 つ以上含まれていることがあります。たとえば、健全性の概要レポート（[操作（Operations）] > [レポート（Reports）] > [診断（Diagnostics）] ページ）をクリックすると、2 つの必須拡張フィルタ（[サーバー（Server）] と [時間範囲（Time Range）]）が表示されます。レポートを生成するには、この両方のフィルタで演算子コマンド、サーバー名、必要な値を指定し、[実行（Go）] をクリックする必要があります。プラス記号（+）をクリックして新しい拡張フィルタを追加できます。マ

ルチセクション レポートは PDF 形式でのみエクスポートできます。特定の時刻または時間間隔で Cisco ISE マルチセクション レポートを実行または再実行するようにスケジュールすることはできません。

（注） レポートをクリックすると、デフォルトでは最新のデータが生成されます。ただし一部のマルチセクション レポートでは、時間範囲以外にもユーザーが入力する必要のある項目があります。

シングルセクション レポートでは、デフォルトでクイック フィルタが 1 番目の行として表示されます。フィールドには、検索基準を選択できるドロップダウン リストまたはテキスト ボックスが含まれています。

拡張フィルタには、1 つ以上の内部条件を含む外部条件が含まれています。外部条件では、検索で指定された内部条件すべてに一致する必要があるか、またはいずれかに一致する必要があるかを指定します。内部条件には、カテゴリ（[エンドポイント ID（Endpoint ID）]、[ID グループ（Identity Group）]）、メソッド（Contains、Does Not Contain などの演算子コマンド）、および時間範囲を条件として指定するために使用される 1 つ以上の条件が含まれています。

[クイックフィルタ（Quick Filter）] を使用すると、[記録日時（Logged At）] ドロップダウン リストから日付または時刻を選択し、過去 30 日以内にログインしたデータ セットのレポートを生成できます。30 日より前の日付または時刻のレポートを生成する場合は、[高度なフィルタ（Advanced Filters）] を使用して、ドロップダウン リストの [カスタム（Custom）] オプションの [開始日（From）] と [終了日（To）] のフィールドに必要な時間枠を設定します。

クイック フィルタ条件の作成

ここでは、クイック フィルタ条件の作成方法を説明します。クイック フィルタ条件はシングルセクション レポートでのみ作成できます。

ステップ 1 **[操作（Operations）]** > **[レポート（Reports）]** を選択し、必要なレポートをクリックします。

ステップ 2 [設定（Settings）] ドロップダウンリストから必須フィールドを選択します。

ステップ 3 データをフィルタリングするため、必須フィールドでドロップダウンリストから選択するか、または特定の文字を入力できます。検索では Contains 演算子コマンドが使用されます。たとえば、「K」で始まるテキストをフィルタリングするには K と入力し、テキスト内の任意の位置に「geo」が含まれているテキストをフィルタリングするには geo と入力します。また、アスタリスク（*）を使用することもできます。たとえば、*abc で始まり *def で終わる正規表現などです。

クイック フィルタで使用される条件には、contains、starts with、ends with、starts with or ends with、および OR 演算子で結合する複数の値があります。

ステップ 4 **Enter** を押します。

拡張フィルタ条件の作成

ここでは、拡張フィルタ条件の作成方法を説明します。拡張フィルタは、シングルセクション レポートとマルチセクション レポートで作成できます。シングルセクション レポートの [フィルタ（Filter）] ドロップダウン メニューには、[クイック フィルタ（Quick Filter）] と [拡張フィルタ（Advanced Filter）] があります。マルチセクション レポートでは、拡張フィルタだけを指定できます。

ステップ 1 **[操作（Operations）]** > **[レポート（Reports）]** を選択し、必要なレポートをクリックします。

ステップ 2 [フィルタ（Filters）] セクションで [一致（Match）] ドロップダウン リストから次のいずれかのオプションを選択します。

a) 指定したすべての条件に一致する必要がある場合は、[すべて（All）] を選択します。

b) 指定したいずれか 1 つの条件に一致すればよい場合は、[いずれか（Any）] を選択します。

ステップ 3 [時間範囲（Time Range）] ドロップダウンリストから必要なカテゴリを選択します。

ステップ 4 [演算子コマンド（Operator Commands）] ドロップダウンリストから、必要なコマンドを選択します。たとえば、特定の文字で始まるテキストや（[次の文字で始まる（Begin With）] を使用）、テキスト内の任意の位置に特定の文字が含まれているテキスト（[次の文字を含む（Contains）] を使用）をフィルタリングできます。あるいは、[ログに記録された時刻（Logged Time）] と対応する [カスタム（Custom）] オプションを選択し、カレンダーからデータをフィルタリングする期間の開始日時と終了日時を指定します。

ステップ 5 [時間範囲（Time Range）] ドロップダウンリストから必要なオプションを選択します。

ステップ 6 [移動（Go）] をクリックします。

今後の参照のために、フィルタリングされたレポートを保存し、[フィルタ（Filter）] ドロップダウンリストから取得することができます。

レポートの実行および表示

ここでは、Reports View を使用してレポートを実行、表示、およびナビゲートする方法について説明します。デフォルトでは、レポートをクリックすると過去 7 日間のデータが生成されます。各レポートでは、ページごとに 500 行のデータが表示されます。レポートにデータを表示する時間の増分を指定できます。

ステップ 1 **[操作（Operations）]** > **[レポート（Reports）]** > **[ISE レポート（ISE Reports）]** を選択します。

また、各ワーク センターの [レポート（Reports）] リンクに移動して、ワーク センター固有の一連のレポートを確認することもできます。

ステップ 2 使用可能な**レポート** カテゴリからレポートをクリックします。

ステップ 3 レポートを実行する 1 つ以上のフィルタを選択します。各レポートに、異なるフィルタを使用できます。フィルタの一部は必須で一部は任意選択です。

ステップ 4 フィルタに適切な値を入力します。

ステップ 5 [移動（Go）] をクリックします。

関連トピック

レポートのエクスポート （49 ページ）
使用可能なレポート （55 ページ）

レポートのナビゲーション

レポート出力から詳細情報を取得できます。たとえば、5 ヵ月間のレポートを生成した場合、5 ヵ月分の集約データがグラフと表で表示されます。

表の特定の値をクリックすると、その特定のフィールドに関連する別のレポートが表示できます。たとえば、[authentication summary] レポートでは、該当するユーザーやユーザー グループの失敗回数が表示されます。失敗したカウントをクリックすると、その特定の失敗したカウントについての認証概要レポートが開きます。

レポートのエクスポート

次のレポートは PDF ファイル形式でののみエクスポートできます。

- 認証概要（Authentication Summary）
- 健全性の概要
- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

ステップ 1 「レポートの実行と表示」の項の説明に従ってレポートを実行します。

ステップ 2 レポートの要約ページの右上隅にある **[エクスポート先（Export To）]** をクリックします。

ステップ 3 次のいずれかのオプションを選択します。

- [リポジトリ（CSV）（Repository (CSV)）]：レポートを CSV ファイル形式でリポジトリにエクスポートします。
- [ローカル（CSV）（Local (CSV)）]：レポートを CSV ファイル形式でローカルディスクにエクスポートします。
- [ローカル（PDF）（Local (PDF)）]：レポートを PDF ファイル形式でローカルディスクにエクスポートします。

（注）
- ローカル CSV または PDF オプションを選択すると、最初の 500 個のレコードのみがエクスポートされます。[リポジトリ（CSV）（Repository CSV）] オプションを使用すると、すべてのレコードをエクスポートできます。
- ローカル PDF オプションを使用してマルチセクションレポートをエクスポートすると、各セクションの最初の 100 行のみがエクスポートされます。

マイレポート

事前設定されたシステムレポートと個人的にフィルタリングされたレポートを [マイレポート（My Reports）] セクションに追加できます。[マイレポート（My Reports）] セクションに保存されたレポートには、適用されたフィルタが保持されます。

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]**>**[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから必要なレポートをクリックします。

ステップ 2 （オプション）選択したレポートが開いたら、必要なフィルタを追加してレポートをカスタマイズします。

ステップ 3 ウィンドウの右上隅にある [マイレポートに追加（Add to My Reports）] ボタンをクリックします。

ステップ 4 [マイレポートに保存（Save to My Reports）] ダイアログボックスが開きます。レポートの名前と説明は自動的に入力されます。必要に応じて、これらのフィールドを編集できます。

ステップ 5 （オプション）選択したレポートは、適用可能なフィルタとともに保存されるため、カスタマイズが保持されます。

ステップ 6 [保存（Save）] をクリックして、レポートを保存します。レポートが正常に保存されたことを示すダイアログボックスが表示されます。

ステップ 7 選択したレポートは、簡単にアクセスできるように [マイレポート（My Reports）] ドロップダウンリストに表示されます。

[マイレポート（My Reports）] セクションに追加されたレポートを削除するには、ウィンドウの右上隅にある [マイレポートから削除（Remove From My Reports）] ボタンをクリックします。表示される [アラート（Alert）] ダイアログボックスで [OK] をクリックすると、レポートが [マイレポート（My Reports）] セクションから削除されます。

Cisco ISE レポートのスケジュール

Cisco ISE レポートをスケジュールして、特定の時間または時間間隔で実行および再実行することができます。選択したレポートに適切なフィルタを適用することもできます。毎時、日次、週次、月次、年次の頻度でCisco ISEで実行するようにレポートをスケジュールできます。1回限りのレポートスケジューリングジョブにすることもできます。レポートの開始日と終了日を選択し、レポートをスケジュールする曜日を選択できます。スケジュールされたレポートを実行する時間を決定できます。

生成されたレポートに関する電子メール通知を送受信することもできます。これらの電子メール通知により、スケジュールされたレポートが正常に実行されたかどうかが通知され、リポジトリの詳細、スケジュールされたレポートの時刻なども含まれます。

時間単位の頻度でレポートをスケジュールする場合は、レポートを複数の日にわたって実行することはできますが、日をまたぐ時間枠を設定することはできません。

たとえば、時間単位のレポートを 2019 年 5 月 4 日から 5 月 8 日までスケジューリングする場合は、時間間隔を各日の午前 6 時から午後 11 時までに設定することはできますが、ある日の午後 6 時から翌日の午前 11 時までに設定することはできません。後者の場合、Cisco ISE は、時間範囲が無効であることを示すエラー メッセージを表示します。

次のレポートはスケジュールできません。

- 認証概要（Authentication Summary）
- 健全性の概要
- RBACL ドロップ概要

（注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。

- ゲスト スポンサー概要
- エンドポイント プロファイルの変更
- ネットワーク デバイスのセッション ステータス

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]**>**[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから、スケジュールするレポートを選択します。

ステップ 2 （オプション）選択したレポートが開いたら、レポートに適用するフィルタを適用します。

ステップ 3 ウィンドウの右上隅にある [スケジュール（Schedule）] ボタンをクリックします。

ステップ 4 [スケジュールとして保存（Save as Schedule）] ダイアログボックスが開きます。

ステップ 5 スケジュールジョブの名前、説明、電子メール、日付、時刻などの詳細を入力します。

ステップ 6 [リポジトリ（Repository）] ドロップダウンリストから、スケジュールされたレポートを保存する外部リポジトリを選択します。詳細については、『Cisco ISE Administrator Guide』の「Backup and Restore Repositories」セクションにある「Table 1. Supportability Matrix for External Repositories」を参照してください。

ステップ 7 [頻度（Frequency）] ドロップダウンリストから、必要に応じてスケジュールの頻度を選択します。たとえば、過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [過去12時間（Last 12 hours）] データフィールドを選択します。

ステップ 8 必要に応じて [開始日（Start Date）] と [終了日（End Date）] を選択し、[保存（Save）] をクリックします。

ステップ 9 選択したすべてのフィルタは、スケジュール時にレポートに自動的に適用されます。

ステップ 10 ウィンドウの下部にある [スケジュールされたレポート（Scheduled Reports）] セクションで、作成されたスケジュールと適用されたフィルタを確認できます。

必要に応じて、スケジュールされたレポートを編集および削除することもできます。[スケジュールされたレポート（Scheduled Reports）] ドロップダウンリスト（**[操作（Operations）]** > **[レポート（Reports）]** > **[スケジュールされたレポート（Scheduled Reports）]**）から、スケジュールされたレポートを選択します。[スケジュールの編集（Edit Schedule）] をクリックして、スケジュールされたレポートを変更し、[保存（Save）] をクリックします。スケジュール設定されたレポートを削除するには、[スケジュールの削除（Delete Schedule）] をクリックします。

ユースケース：スケジュール済みレポート

当日の午前 12 時に前日のデータを取得するには、次の手順に従ってレポートをスケジュールします。

ステップ 1 [レポート（Reports）] ウィンドウ（**[操作（Operations）]** > **[レポート（Reports）]**）で、左側に表示される [レポート（Reports）] ドロップダウンメニューから、スケジュールするレポートを選択します。

ステップ 2 （オプション）選択したレポートが開いたら、レポートに適用するフィルタを適用します。

ステップ 3 このシナリオで、前日のデータを取得するには、[ログ取得時（Logged at）] フィールドを選択し、[昨日（Yesterday）] フィルタを適用します。これにより、スケジュールされたレポートが実行されるたびに前日のデータが返されます。過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [スケジュールとして保存（Save as Schedule）] ダイアログボックスの [過去12時間のデータ（Last 12 hours data）] フィールドを選択します。

ステップ 4 ウィンドウの右上隅にある [スケジュール（Schedule）] ボタンをクリックします。

ステップ 5 [スケジュールとして保存（Save as Schedule）] ダイアログボックスが開きます。

ステップ 6 スケジュールジョブの名前、説明、電子メール、日付、時刻などの詳細を入力します。

ステップ 7 [リポジトリ（Repository）] ドロップダウンリストから、スケジュールされたレポートを保存する外部リポジトリを選択します。詳細については、『Cisco ISE Administrator Guide』の「Backup and Restore Repositories」セクションにある「Table 1. Supportability Matrix for External Repositories」を参照してください。

ステップ 8 [頻度（Frequency）] ドロップダウンリストから、必要に応じてスケジュールの頻度を選択します。たとえば、過去 12 時間のデータのみが必要な場合は、レポートのスケジュール時に [過去12時間（Last 12 hours）] データフィールドを選択します。

ステップ 9 必要に応じて [開始日（Start Date）] と [終了日（End Date）] を選択し、[保存（Save）] をクリックします。

ステップ 10 選択したすべてのフィルタは、スケジュール時にレポートに自動的に適用されます。

ステップ 11 ウィンドウの下部にある [スケジュールされたレポート（Scheduled Reports）] セクションで、作成されたスケジュールと適用されたフィルタを確認できます。

（注）

- スケジュールされたレポートのほとんどは、.csv 形式でエクスポートされます。ただし、Radius 認証、Radius アカウンティング、TACACS 認証、TACACS アカウンティング、および操作監査のスケジュールされたレポートは、.csv ファイルを含む .zip フォルダにエクスポートされます。
- 外部の管理者（Active Directory の管理者など）が電子メール ID フィールドを指定せずにスケジュール設定されたレポートを作成すると、電子メール通知は送信されません。
- 内部または外部の Cisco ISE ユーザーの削除は、その特定のユーザーによって作成されたスケジュールされたレポートを削除した後にのみ行い、ユーザーの削除後にアクティブなスケジュールが実行されないようにする必要があります。
- Cisco ISE レポートの保存またはスケジューリング（フィルタの適用）は、PAN からのみ実行できます。
- スケジュールされたレポートジョブは、プライマリ MnT とセカンダリ MnT ノードの両方で実行されます。プライマリ MnT がダウンしている場合、セカンダリ MnT がスケジュールを実行します。このようなシナリオでは、セカンダリ MnT が最初にプライマリ MnT に ping を送信します。ping が失敗した場合にのみ、セカンダリ MnT はスケジュールされたエクスポートジョブを実行します。
- Cisco ISE 3.1 パッチ 1 以降、エクスポートされたレポートの日付のフォーマットが YYYY-MM-DD から DD-MM-YY に変更されました。時間のフォーマットが hh:mm:ss.sss から hh:mm:ss.sss AM/PM（24 時間形式から 12 時間形式）に変更されました。

Cisco ISE のアクティブな RADIUS セッション

Cisco ISE では、ライブ セッション用の動的な許可変更（CoA）機能が提供されます。この機能を使用すると、アクティブなRADIUSセッションを動的に制御できます。次のタスクを実行するために再認証または接続解除要求をネットワーク アクセス デバイス（NAD）に送信できます。

- 認証に関連する問題のトラブルシューティング：[セッション再認証（Session reauthentication）] オプションを使用して、再認証を試みることができます。ただし、アクセスを制限するためにこのオプションを使用しないでください。アクセスを制限するには、シャットダウン オプションを使用します。
- 問題のあるホストのブロック：[ポート シャットダウンによるセッション終了（Session termination with port shutdown）] オプションを使用して、ネットワークに大量のトラフィックを送信する、ウイルスなどに感染したホストをブロックできます。ただし、RADIUS プロトコルでは、シャットダウンされたポートを再度有効にするための方法は現在サポートされていません。
- エンドポイントでの IP アドレス再取得の強制：サプリカントまたはクライアントを持たないエンドポイントに対して [ポート バウンスでのセッション終了（Session termination with port bounce）] オプションを使用し、VLAN 変更後に DHCP 要求を生成できます。
- エンドポイントへの更新された許可ポリシーのプッシュ：[セッション再認証（Session reauthentication）] オプションを使用して、管理者の裁量に基づいた既存のセッションの許可ポリシーの変更などの、更新されたポリシー設定を適用できます。たとえば、ポスチャ確認が有効である場合にエンドポイントが最初にアクセスを許可されると、通常、エンドポイントは隔離されます。エンドポイントのアイデンティティおよびポスチャが確認された後、Session reauthentication コマンドをエンドポイントに送信して、エンドポイントがそのポスチャに基づいて実際の許可ポリシーを取得できるようにすることが可能です。

デバイスによって CoA コマンドが認識されるためには、適切にオプションを設定することが重要です。

CoA が適切に動作するには、動的な許可変更を必要とする各デバイスの共有秘密情報を設定する必要があります。Cisco ISE では、デバイスからのアクセス要求、およびデバイスへの CoA コマンドの発行において、共有秘密情報設定が使用されます。

（注） このリリースの Cisco ISE では、表示可能な認証されたエンドポイント セッションの最大数が 100,000 に制限されています。

関連トピック

RADIUS セッションの許可の変更 （54 ページ）

RADIUS セッションの許可の変更

ネットワークの一部のネットワーク アクセス デバイスでは、リロード後にアカウンティング停止パケットまたはアカウンティング オフ パケットが送信されないことがあります。このため、[セッション ディレクトリ（Session Directory）] の下のレポートでは、有効なセッションと期限切れのセッションの 2 つのセッションが表示される場合があります。

アクティブな RADIUS セッションの許可を動的に変更する場合や、アクティブな RADIUS セッションの接続を解除する場合には、最新のセッションを選択する必要があります。

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 セッションの表示（Show Live Session）] にビューを切り替えてください。

ステップ 3 CoA を発行する RADIUS セッションの CoA リンクをクリックし、次のいずれかのオプションを選択します。

- [SAnet セッション クエリー（SAnet Session Query）]：SAnet でサポートされるデバイスからのセッションに関する情報をクエリーするために使用します。
- [セッション再認証（Session reauthentication）]：セッションを再認証します。CoA をサポートする ASA デバイスに確立されるセッションにこのオプションを選択すると、セッションポリシープッシュ CoA が呼び出されます。
- [最後の方式でのセッション再認証（Session reauthentication with last）]：そのセッションに対して、最後に成功した認証方式を使用します。
- [再実行によるセッション再認証（Session reauthentication with rerun）]：設定されている認証方式を最初から実行します。

  （注） [最後の方式でのセッション再認証（Session reauthentication with last）] オプションおよび [再実行によるセッション再認証（Session reauthentication with rerun）] オプションは、Cisco IOS ソフトウェアで現在サポートされていません。

- [セッション終了（Session termination）]：単にセッションを終了します。スイッチは、異なるセッションでクライアントを再認証します。
- [ポート バウンスでのセッション終了（Session termination with port bounce）]：セッションを終了し、ポートを再起動します。
- [ポート シャットダウンによるセッション終了（Session termination with port shut down）]：セッションを終了し、ポートをシャットダウンします。

ステップ 4 [実行（Run）] をクリックして、選択した再認証または終了オプションとともに CoA を発行します。

CoA に失敗した場合は、次の理由が考えられます。

- デバイスで CoA がサポートされていない。
- アイデンティティまたは許可ポリシーに変更があった。
- 共有秘密が一致しない。

使用可能なレポート

次の表に、事前設定済みレポートをカテゴリ別に分類して示します。また、レポートの機能およびロギング カテゴリについても説明します。

ロギングカテゴリのsyslogを生成するには、[ログのシビラティ（重大度）レベル（Log Severity Level）] を [情報（Info）] に設定します。

- **[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択します。
- syslog を生成する必要があるロギングカテゴリをクリックします。
- [ログ重大度レベル（Log Severity Level）] ドロップダウンリストから、[情報（Info）] を選択します。
- [保存（Save）] をクリックします。

（注） Cisco ISE リリース 2.6 以降では、IPv6 アドレスを使用するユーザーには次のイベントが監査レポートに記録されます。ログイン/ログアウト、パスワードの変更、および運用変更など。管理者ログイン、ユーザーの変更パスワードの監査、および運用監査レポートでは、IPv4 と IPv6 のレコード別にログをフィルタリングできます。

レポート名	説明	ロギング カテゴリ
Audit		
適応型ネットワーク制御の監査	適応型ネットワーク制御の監査レポートは、RADIUS アカウンティングに基づきます。つまり、エンドポイントごとにすべてのネットワークセッションの履歴レポートを表示します。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] および [RADIUSアカウンティング（RADIUS Accounting）] を選択します。
管理者ログイン	管理者ログインレポートには、GUI ベースの管理者ログインイベントと成功した CLI ログインイベントに関する情報が提供されます。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）] をクリックします。
変更設定監査	変更設定監査レポートは、指定した期間内の設定変更の詳細を提供します。機能をトラブルシューティングする必要がある場合、このレポートは、最新の設定変更が問題の原因となったかどうかを決定するのに役立ちます。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational Audit）] をクリックします。

レポート名	説明	ロギング カテゴリ
データ消去の監査		—

レポート名	説明	ロギング カテゴリ
	データ消去の監査レポートは、ロギングデータが消去されている時間を記録します。 このレポートは、データ消去の 2 つのソースを反映します。 毎日午前 4 時に、Cisco ISE は、[管理（Administration）] > [メンテナンス（Maintenance）] > [データ消去（Data Purging）] ウィンドウで設定した基準に一致するロギングファイルがあるかどうかを確認します。あった場合は、ファイルが削除され、このレポートに記録されます。さらに、Cisco ISE は、ログファイルに使用される記憶容量（しきい値）を常に 80% 以下に保ちます。1 時間ごとに、Cisco ISE はこの割合を確認し、しきい値に再び到達するまで、最も古いデータが削除されます。この情報もこのレポートに記録されます。 ディスク容量使用率が高い場合、しきい値の 80%（すなわち合計ディスク容量の 60%）で、「`ISE モニターノードはもうすぐ割り当てられている最大量を超えます（ISE Monitor node(s) is about to exceed the maximum amount allocated）`」というアラートメッセージが表示されます。その後、しきい値の 90%（すなわち合計ディスク容量の 70%）	

レポート名	説明	ロギング カテゴリ
	で、「ISE モニターノードは割り当てられている最大量を超えました（ISE Monitor node(s) has exceeded the maximum amount allocated）」というアラートメッセージが表示されます。	
エンドポイントのアクティビティ消去	エンドポイントのアクティビティ消去レポートを使用すると、エンドポイントのアクティビティ消去の履歴を確認できます。このレポートは、プロファイラロギングカテゴリが有効である必要があります。（このカテゴリはデフォルトで有効になっている点に注意してください。）	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] を選択します。
内部管理者の概要	内部管理者の概要レポートを使用すると、管理者ユーザーのエンタイトルメントを確認できます。このレポートから、管理者ログイン レポートおよび変更設定監査レポートにもアクセスでき、それにより、管理者ごとにこれらの詳細を表示できます。	—
操作監査	操作監査レポートは、次のような操作の変更に関する詳細を提供します。バックアップの実行、Cisco ISE ノードの登録、またはアプリケーションの再起動。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択して、[管理および操作の監査（Administrative and Operational audit）] を選択します。

レポート名	説明	ロギング カテゴリ
pxGrid管理者の監査	pxGrid管理者の監査レポートは、プライマリ PANでのクライアントの登録、クライアントの登録解除、クライアントの承認、トピックの作成、トピックの削除、パブリッシャとサブスクライバの追加、およびパブリッシャとサブスクライバの削除など、pxGridの管理処理の詳細を提供します。 すべてのレコードに、ノードで処理を実行した管理者の名前が示されます。 管理者およびメッセージの基準に基づいて、pxGrid管理者の監査レポートをフィルタできます。	—
セキュアな通信の監査	セキュアな通信の監査レポートには、認証の失敗、ブレークインの可能性がある試み、SSHログイン、失敗したパスワード、SSHログアウト、無効なユーザーアカウントなどが含まれる、Cisco ISE管理CLIのセキュリティ関連イベントに関する監査の詳細が提供されます。	—
User Change Password Audit	ユーザー変更パスワードの監査レポートは、従業員のパスワード変更に関する検証を表示します。	

レポート名	説明	ロギング カテゴリ
TrustSec 監査	TrustSec 監査ログには次の内容が含まれます。 • TrustSec コンポーネントの管理（作成、名前変更、更新、削除）。 • TrustSec 対応 NAD への SGACL および SGT の導入 • TrustSec セッション。 Cisco ISE が Catalyst Center と統合され、SD Access が Catalyst Center によって管理されている場合、このログは空です。	—
デバイス管理		
TACACS 認証の概要	[TACACS認証概要（TACACS Authentication Summary）] レポートには、最も一般的な認証および認証失敗の理由の詳細が示されています。	—
TACACS アカウンティング	TACACSアカウンティングレポートは、デバイスセッションのアカウンティングの詳細を提供します。ユーザーおよびデバイスの生成された時刻およびログに記録された時刻に関する情報が表示されます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、[TACACSアカウンティング（TACACS Accounting）] をクリックします。
失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）	[失敗の理由別上位Nの認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）	[ネットワークデバイス別上位Nの認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワークデバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザー別上位Nの認証（Top N Authentication by User）	[ユーザー別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザー名ごとの合格および不合格の認証数が表示されます。	—
診断		

レポート名	説明	ロギング カテゴリ
AAA の診断	AAA の診断レポートは、Cisco ISE とユーザー間のすべてのネットワークセッションの詳細を提供します。ユーザーがネットワークにアクセスできない場合、トレンドを識別し、問題が特定のユーザーに隔離されているか、またはより広範囲の問題を示しているかを識別するために、このレポートを確認できます。 （注） ISE は、ユーザー認証が進行中のときにエンドポイントのアカウンティング停止要求をサイレントにドロップする場合があります。ただし、ISE はユーザー認証が完了した後、すべてのアカウンティング要求の認識を開始します。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[ポリシー診断（Policy Diagnostics）]、[IDストア診断（Identity Stores Diagnostics）]、[認証フロー診断（Authentication Flow Diagnostics）]、および [RADIUS診断（RADIUS Diagnostics）]。

レポート名	説明	ロギング カテゴリ
AD コネクタ操作	AD コネクタ操作レポートは、Cisco ISE サーバーのパスワードのリフレッシュ、Kerberos チケットの管理、DNS クエリ、DC 検出、LDAP、および RPC 接続管理など、AD コネクタが実行する操作のログを提供します。 AD の障害がいくつか発生している場合、このレポートで詳細を確認して考えられる原因を特定できます。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ADコネクタ（AD Connector）] を選択します。
エンドポイントプロファイルの変更	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	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）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）] を選択します。

レポート名	説明	ロギング カテゴリ
健全性の概要	健全性の概要レポートは、ダッシュボードのような詳細を提供します。ただし、ダッシュボードには過去24時間のデータのみが表示されます。また、このレポートを使用して、より多くの履歴データを確認できます。 データの一貫したパターンを調べるためにこのデータを評価できます。たとえば、大多数の従業員が就業時間を開始するときに、非常に高い CPU 使用率が予想されます。これらのトレンドの不整合がわかれば、潜在的な問題を識別できます。 [CPU 使用率（CPU Usage）] テーブルには、各種 Cisco ISE 機能の CPU 使用率（%）が表示されます。**show cpu usage** CLI コマンドの出力がこのテーブルに表示されるため、これらの値を、展開内で発生している問題と関連付け、原因を特定することができます。	—

レポート名	説明	ロギング カテゴリ
ISE カウンタ	ISE カウンタ レポートには、さまざまな属性のしきい値が示されます。各種属性の値の収集間隔は異なり、またデータは表形式で表示されます。5 分間隔で収集される属性と 5 分よりも長い間隔で収集される属性があります。 このデータを評価してトレンドを確認し、しきい値よりも高い値を検出した場合には、展開内で発生している問題にこの情報を関連付け、考えられる原因を特定できます。 Cisco ISE はデフォルトでこれらの属性の値を収集します。**application configure ise** コマンドを使用して、Cisco ISE CLI からこのデータ収集を無効にすることができます。カウンタ属性の収集を有効または無効にするには、**オプション 14** を選択します。	—
主要パフォーマンス測定指標	主要パフォーマンス測定指標レポートには、展開に接続しているエンドポイントの数と、1 時間あたりに各 PAN が処理する RADIUS 要求の数に関する統計情報が表示されます。このレポートには、サーバーの平均負荷、要求あたりの平均遅延、および平均トランザクション数/秒が示されます。	—

レポート名	説明	ロギング カテゴリ
設定が誤っている NAS	設定が誤っている NAS レポートは、通常、アカウンティング情報を頻繁に送信するときに、アカウンティング頻度が不正確な NAD に関する一般情報を提供します。修正処置を行い、設定が誤っている NAD を修正すると、レポートはレポートに修正済み確認を表示します。 （注） このレポートを実行するには、**RADIUS 抑制**を有効にする必要があります。	—
設定が誤っているサプリカント	設定が誤っているサプリカントのレポートは、特定のサプリカントが実行した失敗試行のため、設定が誤っているサプリカントの一覧および統計情報を提供します。修正処置を行い、設定が誤っているサプリカントを修正すると、レポートはレポートに修正済み確認を表示します。 （注） このレポートを実行するには、**RADIUS 抑制**を有効にする必要があります。	—

レポート名	説明	ロギング カテゴリ
ネットワーク デバイスのセッション ステータス	ネットワークデバイスのセッションステータス概要レポートを使用すると、直接スイッチにログインせずにスイッチ設定を表示することができます。 Cisco ISE は SNMP クエリを使用してこれらの詳細にアクセスするので、ネットワークデバイスは SNMP v1 または v2c を使用して設定されている必要があります。 ユーザーにネットワークの問題が発生している場合に、このレポートは、問題がスイッチの設定に関連しているかまたは Cisco ISE に関連しているかを識別するのに役立ちます。	—

レポート名	説明	ロギング カテゴリ
OCSP Monitoring	OCSP モニタリング レポートは、Online Certificate Status Protocol（OCSP）サービスのステータスを指定します。Cisco ISE が正常に証明書サーバーに連絡し、証明書ステータス監査を提供できるかどうかを識別します。また、Cisco ISE によって実行されたすべての OCSP 証明書検証操作の概要も提供されます。適切な/失効したプライマリ/セカンダリ証明書に関連する情報を OCSP サーバーから取得します。Cisco ISE は、応答をキャッシュし、後続の OCSP モニタリング レポートの生成に使用します。キャッシュがクリアされる場合は、OCSP サーバーから情報を取得します。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[システム診断（System Diagnostics）] を選択します。
RADIUS エラー	RADIUS エラーレポートを使用すると、ドロップされた RADIUS 要求（未知のネットワーク アクセス デバイスからの廃棄された認証またはアカウンティング要求）、EAP 接続タイムアウトおよび未知の NAD をチェックできます。 （注） 過去 5 日間のレポートのみを表示できます。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[失敗した試行（Failed Attempts）] を選択します。

レポート名	説明	ロギング カテゴリ
システム診断	システム診断レポートは Cisco ISE ノードのステータスの詳細を提供します。Cisco ISE ノードが登録できない場合、このレポートを確認して問題をトラブルシューティングすることができます。 このレポートでは、最初に複数の診断ロギング カテゴリを有効にする必要があります。これらのログを収集すると、Cisco ISE パフォーマンスに悪影響を及ぼすことがあります。したがって、これらのカテゴリはデフォルトで有効ではなく、データを収集するのに十分な時間だけ有効にする必要があります。そうでない場合は、30 分後に自動的に無効になります。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[内部操作診断（Internal Operations Diagnostics）]、[分散管理（Distributed Management）]、および [管理者の認証と許可（Administrator Authentication and Authorization）]。
エンドポイントとユーザー		

レポート名	説明	ロギング カテゴリ
認証概要	認証概要レポートは、RADIUS 認証に基づいています。それにより、最も一般的な認証および認証失敗の原因（ある場合）を特定することができます。たとえば、ある Cisco ISE サーバーが他のサーバーよりもはるかに多くの認証を処理している場合、負荷を適切に分散するためにユーザーを別の Cisco ISE サーバーに再割り当てする場合があります。 （注） [認証概要（Authentication Summary）] レポートまたはダッシュボード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。	—

レポート名	説明	ロギング カテゴリ
クライアント プロビジョニング	クライアントプロビジョニング レポートは、特定のエンドポイントに適用されるクライアントプロビジョニング エージェントについて示します。このレポートを使用すると、各エンドポイントに適用されるポリシーを確認し、次にこれを使用して、エンドポイントが正しくプロビジョニングされたことを確認することができます。 （注） エンドポイントが ISE に接続されない（セッションが確立されない）場合、またはネットワークアドレス変換（NAT）アドレスがセッションで使用される場合、エンドポイントの MAC アドレスは [エンドポイントID（Endpoint ID）] 列に表示されません。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ポスチャおよびクライアントプロビジョニングの監査（Posture and Client Provisioning Audit）] および [ポスチャおよびクライアントプロビジョニングの診断（Posture and Client Provisioning Diagnostics）] を選択します。

レポート名	説明	ロギング カテゴリ
現在のアクティブなセッション	現在アクティブなセッションレポートを使用すると、指定の期間内にネットワーク上に存在する者に関する詳細を含むレポートをエクスポートできます。 ユーザーがネットワークにアクセスできない場合、セッションが認証または終了されているかどうか、またはセッションに別の問題があるかどうかを確認できます。	—
外部モバイル デバイス管理	外部モバイルデバイス管理レポートは、Cisco ISE と外部モバイル デバイス管理（MDM）サーバー間の統合に関する詳細を提供します。 このレポートを使用すると、MDM サーバーに直接ログインせずに、MDM サーバーによってプロビジョニングされたエンドポイントを確認することができます。また、登録および MDM コンプライアンス ステータスなどの情報が表示されます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、[MDM] を選択します。

レポート名	説明	ロギング カテゴリ
パッシブ ID	パッシブ ID レポートでは、ドメイン コントローラへの WMI 接続の状態をモニターし、関連する統計情報（受信した通知の数、1 秒あたりのユーザー ログイン/ログアウト回数など）を収集することができます。 （注） この方法で認証されたセッションには、レポートの認証の詳細がありません。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[IDマッピング（Identity Mapping）] を選択します。
手動証明書プロビジョニング	手動証明書プロビジョニング レポートには、証明書プロビジョニング ポータル経由で手動でプロビジョニングされたすべての証明書がリストされます。	—
条件によるポスチャ アセスメント	条件によるポスチャ アセスメント レポートでは、ISE に設定されたポスチャ ポリシー条件に基づいてレコードを表示し、最新のセキュリティ設定またはアプリケーションがクライアント マシンで利用可能かどうかを確認できます。	—

レポート名	説明	ロギング カテゴリ
エンドポイントによるポスチャ アセスメント	[エンドポイントによるポスチャ アセスメント（Posture Assessment by Endpoint）] レポートには、エンドポイントの時間、ステータス、PRA アクションなどの詳細な情報が提供されます。[詳細（Details）] をクリックして、エンドポイントの詳細情報を表示することができます。 （注） [エンドポイントによるポスチャ アセスメント（Posture Assessment by Endpoint）] レポートでは、エンドポイントのアプリケーションおよびハードウェア属性のポスチャ ポリシーの詳細は提供されません。[コンテキストの可視性（Context Visibility）] ページでのみこの情報を確認できます。	—

レポート名	説明	ロギング カテゴリ
プロファイリングされたエンドポイントの概要	プロファイリングされたエンドポイントの概要レポートは、ネットワークにアクセスしているエンドポイントに関するプロファイリングの詳細を提供します。 （注） Cisco IP Phone など、セッション時間を登録しないエンドポイントの場合、[エンドポイント（Endpoint）] セッション時間フィールドに、[該当なし（Not Applicable）] と表示されます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、[プロファイラ（Profiler）] を選択します。

レポート名	説明	ロギング カテゴリ
RADIUS アカウンティング（RADIUS Accounting）	RADIUS アカウンティング レポートは、ユーザーがネットワーク上に存在した時間を識別します。ユーザーがネットワークにアクセスできない場合、Cisco ISE がネットワーク接続問題の原因であるかどうか、このレポートを使用して識別できます。 （注） 暫定アップデートに、指定されたセッションの IPv4 または IPv6 アドレスの変更に関する情報が含まれている場合、Radius アカウンティング暫定アップデートは [RADIUS アカウンティング（RADIUS Accounting）] レポートに含まれています。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、[RADIUSアカウンティング（RADIUS Accounting）] を選択します。 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）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択してから、[RADIUS アカウンティング（RADIUS Accounting）] を選択します。
RADIUS 認証	RADIUS 認証レポートを使用すると、認証失敗および成功の履歴を確認できます。ユーザーがネットワークにアクセスできない場合、このレポートの詳細を確認して考えられる原因を識別できます。	**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択し、次のロギングカテゴリを選択します。[成功した認証（Passed Authentications）] および [失敗した試行（Failed Attempts）]。

レポート名	説明	ロギング カテゴリ
登録済みエンドポイント	登録済みエンドポイントレポートは、従業員によって登録されているすべてのパーソナルデバイスを表示します。	—
拒否エンドポイント	拒否エンドポイントレポートには、従業員が登録したパーソナル デバイスのうち、拒否されたデバイスまたはリリースされたデバイスがすべて表示されます。このレポートのデータは、Plus ライセンスをインストールしている場合にのみ使用可能です。	—
サプリカント プロビジョニング	サプリカントプロビジョニング レポートは、従業員のパーソナルデバイスにプロビジョニングされたサプリカントに関する詳細を提供します。	ポスチャおよびクライアント プロビジョニングの監査（Posture and Client Provisioning Audit）
エンドポイントによる上位承認	エンドポイント（MAC アドレス）別上位認証レポートは、ネットワークにアクセスするために各エンドポイントの MAC アドレスが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）
ユーザー別上位認証	ユーザー別上位認証レポートは、ネットワークにアクセスするために各ユーザーが Cisco ISE によって許可された回数を表示します。	成功した認証、失敗した試行（Passed Authentications, Failed Attempts）

レポート名	説明	ロギング カテゴリ
アクセス サービス別上位 N の認証（Top N Authentication by Access Service）	[アクセス サービス別上位 N の認証（Top N Authentication by Access Service）] レポートには、選択されたパラメータに基づいて、特定の期間におけるアクセス サービス タイプごとの合格および不合格の認証数が表示されます。	—
失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）	[失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）] レポートには、選択したパラメータに基づいて、特定の期間における失敗の理由別の認証の合計数が表示されます。	—
ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）	[ネットワーク デバイス別上位 N の認証（Top N Authentication by Network Device）] レポートには、選択されたパラメータに基づいて、特定の期間におけるネットワークデバイス名ごとの合格および不合格の認証数が表示されます。	—
ユーザー別上位Nの認証（Top N Authentication by User）	[ユーザー別上位 N の認証（Top N Authentication by User）] レポートには、選択したパラメータに基づいて、特定の期間におけるユーザー名ごとの合格および不合格の認証数が表示されます。	—
ゲスト		
AUP 受け入れステータス	AUP 受け入れステータス レポートには、すべてのゲスト ポータルからの AUP 承認の詳細が示されます。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。

レポート名	説明	ロギング カテゴリ
ゲスト アカウンティング	ゲスト アカウンティング レポートは、RADIUS アカウンティング レポートのサブセットです。アクティブなゲストまたはゲスト ID グループに割り当てられたすべてのユーザーがこのレポートに表示されます。	—

レポート名	説明	ロギング カテゴリ
プライマリゲストレポート		**[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択して、[成功した認証（Passed Authentications）] を選択します。

レポート名	説明	ロギング カテゴリ
	プライマリゲストレポートは、さまざまなゲストアクセスレポートからデータを結合し、異なるレポートソースからデータをエクスポートできるようにします。プライマリゲストレポートは、ゲストユーザーがアクセスしているWebサイトに関する詳細も提供します。このレポートは、セキュリティ監査の目的で使用し、ゲスト ユーザーがネットワークにアクセスした時間、およびそこで行った操作を示すことができます。 また、ゲストトラフィックに使用するネットワーク アクセス デバイス（NAD）のHTTPインスペクションを有効にする必要もあります。この情報は、NADによってCisco ISEに返送されます。 クライアントが最大同時セッションの制限数に到達した時期を確認するには、管理者ポータルから、[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）] の順に選択し、次を実行します。 **1.** 「認証フロー診断」のロギングカテゴリのログ レベルを [警告（WARN）] から [情報（INFO）] に上げます。 **2.** AAA	

レポート名	説明	ロギング カテゴリ
	診断の[ロギングカテゴリ（Logging Category）] の下で [LogCollectorターゲット（LogCollector Target）] を [使用可能（Available）] から [選択済み（Selected）] に変更します。	
デバイスのログインおよび監査	デバイスのログインおよび監査レポートは、デバイス ポータルのデバイスでユーザーが実行するログイン アクティビティと操作についての詳細を提供します。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[デバイス（My Devices）] を選択します。
スポンサーのログインおよび監査	スポンサーのログインおよび監査レポートは、スポンサー ポータルでのゲスト ユーザーのログイン、追加、削除、有効化、一時停止、および更新操作の詳細、ならびにスポンサーのログイン アクティビティの詳細を提供します。 ゲスト ユーザーを一括で追加すると、[ゲスト ユーザー（Guest Users）] カラムの下に表示されます。このカラムは、デフォルトでは非表示です。エクスポート時に、これらの一括処理されたユーザーもエクスポート ファイルに存在します。	**[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギングカテゴリ（Logging Categories）]** を選択し、[ゲスト（Guest）] を選択します。
SXP		
SXP バインディング	SXP バインディング レポートは、SXP 接続を介して交換される IP-SGT バインディングに関する情報を提供します。	—

レポート名	説明	ロギング カテゴリ
SXP 接続	このレポートを使用して、SXP接続のステータスをモニターしたり、ピア IP、SXP ノード IP、VPN 名、SXPモードなど、その接続に関連する情報を収集できます。	—
TrustSec		
RBACL ドロップ概要	RBACL ドロップ概要レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 ユーザーが特定のポリシーまたはアクセスに違反した場合、パケットがドロップされ、このレポートに示されます。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。	—

レポート名	説明	ロギング カテゴリ
ユーザー別上位N個の RBACL ドロップ	ユーザー別上位 N 個の RBACL ドロップ レポートは、拡張 Cisco ISE ライセンスのみで使用できる TrustSec 機能に固有です。 また、このレポートでは、ドロップされたイベントの NetFlow イベントを Cisco ISE に送信するようにネットワーク デバイスを設定する必要があります。 このレポートは、特定のユーザー別にポリシー違反（パケット ドロップに基づく）を表示します。 （注） RBACL 廃棄パケットのフローは、Cisco Catalyst 6500 シリーズ スイッチでのみ使用できます。	—
TrustSec ACI	このレポートには、IEPG、EEPG、エンドポイント、APIC のサブネット設定と同期された SGT および SXP のマッピングが一覧表示されます。これらの詳細は、TrustSec APIC 統合機能が有効になっている場合にのみ表示されます。	—

レポート名	説明	ロギング カテゴリ
TrustSec 展開の検証		—

レポート名	説明	ロギング カテゴリ
	このレポートを使用すると、最新の TrustSec ポリシーがすべてのネットワークデバイスで展開されているかどうか、Cisco ISE とネットワークデバイスで設定されたポリシーに不一致があるかどうかを確認できます。 検証プロセスの結果を表示するには、[詳細（Details）] アイコンをクリックします。次の詳細情報を表示できます。 • 検証プロセスの開始時期と終了時期 • 最新の TrustSec ポリシーがネットワークデバイスで正常に展開されているかどうか。また、最新の TrustSec ポリシーを展開するネットワークデバイスの名前およびIPアドレスを表示することもできます。 • Cisco ISE とネットワークデバイスで設定されたポリシーに不一致があるかどうか。デバイス名、IP アドレス、および各ポリシーの違いの対応するエラーメッセージが表示されます。 [アラーム（Alarms）] ダッシュレット（[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）] と [ホー	

レポート名	説明	ロギング カテゴリ
	ム（Home）] > [サマリー（Summary）]）で、TrustSec 展開の検証アラームを表示できます。 （注） • レポート作成にかかる時間は、展開内のネットワークデバイスと TrustSec グループの数に応じて異なります。 • TrustSec 展開の検証レポートのエラーメッセージの長さは、現在 480 文字に制限されています。480 文字を超えるエラーメッセージは切り捨てられます。最初から 480 文字のみがレポートに表示されます。	

レポート名	説明	ロギング カテゴリ
TrustSec ポリシーのダウンロード	このレポートには、ポリシー（SGT/SGACL）のダウンロードのためにネットワークデバイスによって送信された要求と、ISE によって送信された詳細が一覧表示されます。ワークフローモードを有効にしている場合、要求を実稼働マトリックスまたはステージング マトリックスに対してフィルタ処理することができます。	このレポートを表示するには、次の手順を実行する必要があります。 **1.** **[管理（Administration）]** > **[システム（System）]** > **[ロギング（Logging）]** > **[ロギングカテゴリ（Logging Categories）]** を選択します。 **2.** **[AAA診断（AAA Diagnostics）]** > **[RADIUS診断（RADIUS Diagnostics）]** を選択します。 **3.** RADIUS 診断の [ログシビラティ（重大度）レベル（Log Severity Level）] を DEBUG に設定します。
脅威中心型 NAC サービス		
アダプタのステータス	アダプタのステータス レポートには、脅威および脆弱性のアダプタのステータスが表示されます。	—
COA イベント	脆弱性イベントがエンドポイントに受信されると、Cisco ISE はそのエンドポイントの CoA をトリガーします。CoA イベント レポートには、これらの CoA イベントのステータスが表示されます。また、これらのエンドポイントの新旧の認証ルールとプロファイルの詳細が表示されます。	—
脅威イベント	脅威イベント レポートには、設定したさまざまなアダプタから Cisco ISE が受信した脅威イベントがすべて表示されます。	—

レポート名	説明	ロギング カテゴリ
脆弱性アセスメント	脆弱性アセスメント レポートには、エンドポイントで行われているアセスメントに関する情報が提供されます。このレポートを表示して、設定されたポリシーに基づいてアセスメントが行われているかどうかを確認することができます。	—

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 *6 : 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。

フィールド名	説明
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.`
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。

認証遅延

認証遅延は、認証プロセスが開始された時点からの RADIUS 認証プロセスの平均応答時間です。**[ダッシュボード（Dashboard）] > [システム概要（System Summary）]** ダッシュレットを

選択します。Cisco ISE 認証遅延は、**[ダッシュボード（Dashboard）]** > **[システム概要（System Summary）]** ダッシュレットから確認できます。

ドロップダウンリストから次の認証遅延タイムフレームを選択できます。

- [60 分（60 mins）]：このオプションでは、過去 60 分間に開始された認証の認証遅延が指定されます。
- [12 時間（12 hrs）]：このオプションでは、過去 24 時間に開始された認証プロセスの認証遅延が指定されます。

表示される応答時間はミリ秒（ms）単位です。

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 7: 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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
[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。

フィールド名	説明
[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。

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 *8 : 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。
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。

フィールド名	使用上のガイドライン
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。
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。

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 *9:* 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。

フィールド名	説明
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。
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。

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 *10 : 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.`
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。

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 11: 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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
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。

フィールド名	説明
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。
[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。

フィールド名	説明
[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。

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 *12 : 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。
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。

フィールド名	使用上のガイドライン
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。
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。

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 *13*：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。

フィールド名	説明
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。
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。

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。