



ISE-PIC でのサービスのモニターリングと トラブルシューティング

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

- **モニターリング**：ネットワーク上のアクセスアクティビティの状態を表す意味のあるデータのリアルタイム表示を提供します。これを把握することにより、操作の状態を簡単に解釈し、作用することができます。
- **トラブルシューティング**：ネットワーク上のアクセスの問題を解決するための状況に応じたガイダンスを提供します。また、ユーザーの懸念に対応してタイムリーに解決策を提供できます。
- **レポート**：トレンドを分析し、システムパフォーマンスおよびネットワーク アクティビティをモニターするために使用できる、標準レポートのカタログを提供します。レポートをさまざまな方法でカスタマイズし、今後使用するために保存できます。レコードの検索時には、[ID (Identity)]、[エンドポイント ID (Endpoint ID)]、および [ノード (Node)] フィールドにワイルドカードと複数の値を使用できます。

モニターリング、トラブルシューティング、およびレポートの各ツールを使用して ISE-PIC を管理する方法についてはこのセクションで説明します。

- [ライブセッション \(2 ページ\)](#)
- [使用可能なレポート \(5 ページ\)](#)
- [Cisco ISE-PIC のアラーム \(9 ページ\)](#)
- [着信トラフィックを検証する TCP ダンプユーティリティ \(22 ページ\)](#)
- [ロギング メカニズム \(25 ページ\)](#)
- [Smart Call Home \(25 ページ\)](#)
- [Active Directory のトラブルシューティング \(27 ページ\)](#)
- [その他のトラブルシューティング情報の入手 \(42 ページ\)](#)
- [その他の参考資料 \(47 ページ\)](#)
- [通信、サービス、およびその他の情報 \(47 ページ\)](#)

ライブセッション

次の表では、[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セッションが表示されます。メインメニューバーから [ライブセッション (Live Sessions)] を選択します。

表 1: 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 (Updated)	何らかの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 (Action)	[アクション (Actions)] アイコンをクリックして [アクション (Actions)] ポップアップウィンドウを開きます。次を実行できます。 <ul style="list-style-type: none"> • セッションのクリア • 現行ユーザーのセッションステータスの確認
エンドポイント ID (Endpoint ID)	エンドポイントの一意の識別子を表示します。通常は MAC または IP アドレスです。
ID (Identity)	エンドポイントデバイスのユーザー名を表示します。
IP アドレス (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。
サーバー (Server)	ログを生成した PIC 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。

フィールド名	説明
セッション送信元 (Session Source)	RADIUSセッションまたはPassiveIDセッションのいずれであるかを示します。
ユーザドメイン名 (User Domain Name)	ユーザーの登録済みDNS名を示します。
ユーザーNetBIOS名 (User NetBIOS Name)	ユーザーのNetBIOS名を示します。
プロバイダ (Provider)	<p>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と呼ばれます。</p> <ul style="list-style-type: none"> • 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) <p>異なるプロバイダからの2つのイベントがエンドポイントセッションから学習されると、ライブセッションページにこれらのプロバイダがカンマ区切り値として表示されます。</p>
MACアドレス (MAC Address)	クライアントのMACアドレスを表示します。

フィールド名	説明
エンドポイントチェック時刻 (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)	<p>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。</p> <ul style="list-style-type: none"> • [到達不要 (Unreachable)] • [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)	<p>(REST プロバイダの場合にのみ値が表示されます。) ターミナルサーバー (TS) エージェントにより割り当てられた最初のポートを示します。</p> <p>ターミナルサーバー (TS) 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です。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 TS 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 - ユーザーのマッピングが作成されます。</p>
TS エージェント ID (TS Agent ID)	(REST プロバイダ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 (TS) エージェントの一意の ID を表示します。

フィールド名	説明
AD ユーザー解決 ID (AD User Resolved Identities)	(AD ユーザーの場合にのみ値が表示されます。) 一致したアカウントの候補が表示されます。
AD ユーザー解決 DN (AD User Resolved DNs)	(AD ユーザーの場合にのみ値が表示されます。) AD ユーザーの識別名 (例: CN=chris,CN=Users,DC=R1,DC=com) を表示します。

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。

レポート名	説明	ロギング カテゴリ
IDC レポート		
AD コネクタ操作	AD コネクタ操作レポートは、ISE-PIC サーバーのパスワードの更新、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。
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)] を選択します。

レポート名	説明	ロギング カテゴリ
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)] を選択します。
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、指定の期間内のその時点でネットワーク上に存在していた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。	[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、ロギング カテゴリ [アカウントリング (Accounting)] および [RADIUS アカウントリング (RADIUS Accounting)] を選択します。

レポート名	説明	ロギング カテゴリ
正常性の概要	<p>正常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、ダッシュボードは過去 24 時間のデータしか表示しませんが、このレポートを使用するとより多くの履歴データを確認できます。</p> <p>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。</p> <p>[CPU 使用率 (CPU Usage)] テーブルには、各種 ISE-PIC 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。</p>	<p>[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、ロギング カテゴリ [管理監査および操作監査 (Administrative and Operational Audit)]、[システム診断 (System Diagnostics)]、[システム統計情報 (System Statistics)] を選択します。</p>
操作監査	<p>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、ISE-PIC ノードの登録、またはアプリケーションの再起動。</p>	<p>[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。</p>

レポート名	説明	ロギング カテゴリ
PassiveID	<p>Passive ID レポートを使用すると、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。</p>	<p>[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。</p>
pxGrid 管理者の監査	<p>pxGrid 管理者の監査レポートは、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リバの追加、およびパブリッシャとサブスクリバの削除など、pxGrid の管理処理の詳細を提供します。</p> <p>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。</p> <p>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。</p>	—

レポート名	説明	ロギング カテゴリ
システム診断	<p>システム診断レポートは ISE-PIC ノードのステータスの詳細を提供します。ISE-PIC 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。</p> <p>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、ISE-PIC の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。</p>	<p>[管理 (Administration)] > [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)]。</p>
ユーザー変更パスワードの監査	<p>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。</p>	<p>[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。</p>

Cisco ISE-PIC のアラーム

アラームは、ネットワークの状態を通知し、[アラーム (Alarms)] ダッシュレットに表示されます。アラームには、[クリティカル (Critical)]、[警告 (Warning)]、および [情報 (Information)] の 3 つのアラームシビラティ (重大度) があります。データ消去イベントなど、システム アクティビティの情報も提供されます。システム アクティビティについてどのように通知するかを設定したり、それらを完全に無効にしたりできます。また、特定のアラームのしきい値を設定できます。

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

イベントが繰り返し発生した場合、同じアラームは約1時間抑制されます。イベントが繰り返し発生する間は、トリガーに応じて、アラームが再び表示されるのに約1時間かかる場合があります。

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

表 2: Cisco ISE-PIC のアラーム

アラーム名	アラームの説明	アラームの解決方法
管理および操作の監査の管理		
展開のアップグレードの失敗 (Deployment Upgrade Failure)	ISE PIC ノードでアップグレードに失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE ログを確認します。
アップグレードバンドルのダウンロードの失敗 (Upgrade Bundle Download failure)	アップグレードバンドルのダウンロードが ISE-PIC ノードで失敗しました。	アップグレードが失敗した原因と修正措置について、失敗したノードの ADE ログを確認します。
CRL で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続 (Secure LDAP connection reconnect due to CRL found revoked certificate)	CRL チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
OCSP で失効した証明書が見つかったことによるセキュア LDAP 接続の再接続 (Secure LDAP connection reconnect due to OCSP found revoked certificate)	OCSP チェックの結果、LDAP 接続で使用された証明書が失効していることが検出されました。	OCSP 設定が有効であることを確認します。LDAP サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して LDAP サーバーにインストールします。
CRL で失効した証明書が見つかったことによるセキュア syslog 接続の再接続 (Secure syslog connection reconnect due to CRL found revoked certificate)	CRL チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	CRL 設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。

アラーム名	アラームの説明	アラームの解決方法
OCSPで失効した証明書が見つかったことによるセキュアな syslog 接続の再接続 (Secure syslog connection reconnect due to OCSP found revoked certificate)	OCSP チェックの結果、syslog 接続で使用された証明書が失効していることが検出されました。	OCSP設定が有効であることを確認します。syslog サーバー証明書とその発行元の証明書が失効していないことを確認します。失効している場合は、新しい証明書を発行して syslog サーバーにインストールします。
管理者アカウントがロック/無効 (Administrator account Locked/Disabled)	パスワードの失効または不正なログイン試行のために、管理者アカウントがロックされているか、または無効になっています。詳細については、管理者パスワードポリシーを参照してください。	管理者パスワードは、GUI または CLI を使用して、他の管理者によってリセットできます。
ERS が非推奨の URL を検出 (ERS identified deprecated URL)	ERS が非推奨の URL を検出しました。	要求された URL が非推奨であるため、使用しないでください。
ERS が古い URL を検出 (ERS identified out-dated URL)	ERS が古い URL を検出しました。	要求された URL が古いため、新しいものを使用してください。この URL は今後のリリースで削除されません。
ERS 要求 Content-Type ヘッダーが最新ではありません。	ERS 要求 Content-Type ヘッダーが最新ではありません。	要求 Content-Type ヘッダーで指定された要求のリソースバージョンが最新ではありません。これはリソーススキーマが変更されたことを意味します。いくつかの属性が追加または削除された可能性があります。古いスキーマをこのまま処理するために、ERS エンジンでデフォルト値が使用されます。
ERS XML 入力が XSS またはインジェクション攻撃の原因です (ERS XML input is a suspect for XSS or Injection attack)	ERS XML 入力が XSS またはインジェクション攻撃の原因になっています。	XML 入力を確認してください。

アラーム名	アラームの説明	アラームの解決方法
バックアップに失敗 (Backup Failed)	Cisco ISE-PIC のバックアップ操作に失敗しました。	Cisco ISE-PIC とリポジトリ間のネットワーク接続を確認します。次の点を確認します。 <ul style="list-style-type: none"> リポジトリに使用するクレデンシャルが正しいこと。 リポジトリに十分なディスク領域があること。 リポジトリ ユーザーが書き込み特権を持っていること。
CA サーバーがダウン (CA Server is down)	CA サーバーがダウンしています。	CA サービスが CA サーバーで稼働中であることを確認します。
CA サーバーが稼働中 (CA Server is Up)	CA サーバーは稼働中です。	CA サーバーが稼働中であることを管理者に通知します。
証明書の有効期限 (Certificate Expiration)	この証明書はまもなく有効期限が切れます。これが失効すると、Cisco ISE-PIC がクライアントとのセキュアな通信を確立しないようにします。	証明書を交換します。信頼できる証明書の場合、発行元の認証局 (CA) にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE-PIC を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書が失効 (Certificate Revoked)	管理者は、内部 CA がエンドポイントに発行した証明書を取り消しました。	ISE-PIC フローに従って最初から新しい証明書を使用してプロビジョニングします。
証明書プロビジョニング初期化エラー (Certificate Provisioning Initialization Error)	証明書プロビジョニングの初期化に失敗しました。	複数の証明書でサブジェクトの CN (CommonName) 属性が同じ値になっており、証明書チェーンを構築できません。システム内のすべての証明書を確認します。

アラーム名	アラームの説明	アラームの解決方法
証明書の複製に失敗 (Certificate Replication Failed)	セカンダリ ノードへの証明書の複製に失敗しました。	証明書がセカンダリ ノードで無効であるか、他の永続的なエラー状態があります。セカンダリ ノードに矛盾する証明書が存在しないかどうかを確認します。見つかった場合は、セカンダリノードに存在するその証明書を削除し、プライマリの新しい証明書をエクスポートしてから削除し、その後インポートすることによって複製を再実行します。
証明書の複製に一時的に失敗 (Certificate Replication Temporarily Failed)	セカンダリ ノードへの証明書の複製に一時的に失敗しました。	証明書は、ネットワークの停止などの一時的な条件によりセカンダリ ノードに複製されませんでした。複製は、成功するまで再実行されます。
証明書が失効 (Certificate Expired)	この証明書の期限が切れています。Cisco ISE-PIC がクライアントとのセキュアな通信を確立しないようにします。ノードツーノード通信も影響を受ける場合があります。	証明書を交換します。信頼できる証明書の場合、発行元の認証局 (CA) にお問い合わせください。CA 署名付きローカル証明書の場合、CSR を生成し、CA に新しい証明書を作成してもらいます。自己署名したローカル証明書の場合、Cisco ISE-PIC を使用して、有効期限を延長します。使用されなくなった場合、証明書を削除できます。
証明書要求転送に失敗 (Certificate Request Forwarding Failed)	証明書要求転送に失敗しました。	受信する証明書要求が送信者からの属性に一致することを確認します。
設定が変更 (Configuration Changed)	Cisco ISE 設定が更新されています。このアラームは、ユーザーとエンドポイントに設定変更があってもトリガーされません。	設定変更が想定どおりであるかどうかを確認します。

アラーム名	アラームの説明	アラームの解決方法
CRL の取得に失敗 (CRL Retrieval Failed)	サーバーから CRL を取得できません。これは、指定した CRL が使用できない場合に発生することがあります。	ダウンロード URL が正しく、サービスに使用可能であることを確認します。
DNS 解決に失敗 (DNS Resolution Failure)	ノードで DNS 解決に失敗しました。	コマンド ip name-server で設定した DNS サーバーが到達可能であることを確認してください。 「CNAME <hostname of the node> に対する DNS 解決が失敗しました (DNS Resolution failed for CNAME <hostname of the node>)」というアラームが表示された場合は、各 Cisco ISE ノードの A レコードとともに CNAME RR を作成できることを確認します。
ファームウェアの更新が必要 (Firmware Update Required)	このホスト上でファームウェアの更新が必要です。	Cisco Technical Assistance Center (TAC) に問い合わせてファームウェアアップデートを入手してください。
仮想マシン リソースが不十分 (Insufficient Virtual Machine Resources)	このホストでは、CPU、RAM、ディスク容量、IOPS などの仮想マシン (VM) リソースが不十分です。	Cisco ISE Hardware Installation Guide に指定されている VM ホストの最小要件を確認します。
NTP サービスの障害 (NTP Service Failure)	NTP サービスがこのノードでダウンしています。	これは、NTP サーバーと Cisco ISE-PIC ノードとの間に大きな時間差 (1,000 秒を超える) があるために発生することがあります。NTP サーバーが正しく動作していることを確認し、 ntp server <servername> CLI コマンドを使用して NTP サービスを再起動して、時間を同期します。

アラーム名	アラームの説明	アラームの解決方法
NTP 同期に失敗 (NTP Sync Failure)	このノードに構成されているすべての NTP サーバーが到達不能です。	CLI で show ntp コマンドを実行してトラブルシューティングを行います。Cisco ISE-PIC から NTP サーバーに到達可能であることを確認します。NTP 認証が設定されている場合、キー ID と値がサーバーの対応する値に一致することを確認します。
スケジュールされた設定バックアップなし (No Configuration Backup Scheduled)	Cisco ISE-PIC 設定バックアップがスケジュールされていません。	設定バックアップのスケジュールを作成します。
操作 DB 消去に失敗 (Operations DB Purge Failed)	操作データベースから古いデータを消去できません。このことは、M&T ノードがビジー状態である場合に発生する可能性があります。	[データ消去の監査 (Data Purging Audit)] レポートをチェックし、 <code>used_space</code> が <code>threshold_space</code> を下回ることを確認します。CLI を使用して M&T ノードにログインし、消去操作を手動で実行します。
複製に失敗 (Replication Failed)	セカンダリ ノードは複製されたメッセージを消費できませんでした。	Cisco ISE-PIC の GUI にログインし、展開ページから手動同期を実行します。影響を受ける Cisco ISE-PIC ノードを登録解除してから登録します。
復元に失敗 (Restore Failed)	Cisco ISE-PIC の復元操作に失敗しました。	Cisco ISE-PIC とリポジトリ間のネットワーク接続を確認します。リポジトリに使用するクレデンシャルが正しいことを確認します。バックアップファイルが破損していないことを確認します。CLI で reset-config コマンドを実行して、正常な既知の最終バックアップを復元します。
パッチに失敗 (Patch Failure)	パッチ プロセスがサーバーで失敗しました。	サーバーにパッチ プロセスを再インストールします。
パッチに成功 (Patch Success)	パッチ プロセスがサーバーで成功しました。	-

アラーム名	アラームの説明	アラームの解決方法
複製が停止 (Replication Stopped)	ISE-PIC ノードがプライマリノードから設定データを複製できませんでした。	Cisco ISE-PIC の GUI にログインして [Deployment (展開)] ページから手動同期を実行するか、または影響を受けた Cisco ISE-PIC ノードを登録解除してから必須フィールドで再登録します。
エンドポイント証明書が期限切れ (Endpoint certificates expired)	エンドポイント証明書が日次スケジュール ジョブで期限切れとマークされました。	エンドポイント デバイスを再登録して新しいエンドポイント証明書を取得してください。
エンドポイント証明書が消去 (Endpoint certificates purged)	期限切れのエンドポイント証明書が日次スケジュール ジョブによって消去されました。	アクションは必要ありません。これは、管理者が開始したクリーンアップ操作です。
複製低速エラー (Slow Replication Error)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速情報 (Slow Replication Info)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
複製低速警告 (Slow Replication Warning)	低速またはスタックした複製が検出されました。	ノードが到達可能であり、展開の一部であることを確認してください。
EST サービスの停止	EST サービスが停止しています。	CA および EST サービスが稼働しており、証明書サービスのエンドポイントサブ CA 証明書チェーンが完了したことを確認します。
EST サービスの稼働	EST サービスが稼働しています。	EST サービスが稼働中であることを管理者に通知します。
Smart Call Home の通信障害	Smart Call Home メッセージが正常に送信されませんでした。	Cisco ISE-PIC と Cisco システムの間でネットワーク接続があることを確認します。
テレメトリ メッセージの障害	テレメトリ メッセージが正常に送信されませんでした。	Cisco ISE と Cisco システムの間でネットワーク接続があることを確認します。

アラーム名	アラームの説明	アラームの解決方法
ISE サービス		
AD コネクタを再起動する必要があります (AD Connector had to be restarted)	AD コネクタが突然シャットダウンし、再起動が必要となりました。	この問題が連続して発生する場合は、Cisco TAC にお問い合わせください。
Active Directory フォレストが使用不可 (Active Directory forest is unavailable)	Active Directory フォレスト GC (グローバルカタログ) が使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
認証ドメインが使用不可 (Authentication domain is unavailable)	認証ドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。
ID マッピングの認証非アクティビティ (ID Map. Authentication Inactivity)	ユーザー認証イベントが過去 15 分に ID マッピング サービスによって収集されませんでした。	これがユーザー認証が想定される時間 (たとえば、勤務時間) である場合は、Active Directory ドメイン コントローラへの接続を確認します。
設定されたネーム サーバーがダウン (Configured nameserver is down)	設定されたネーム サーバーがダウンしているか、使用できません。	DNS 設定とネットワーク接続を確認します。
AD : マシン TGT のリフレッシュに失敗 (AD: Machine TGT refresh failed)	ISE-PIC サーバー TGT (チケット認可チケット) の更新に失敗しました。これは AD 接続とサービスに使用されます。	Cisco ISE-PIC のマシンアカウントが存在し、有効であることを確認します。また、クロックスキュー、複製、Kerberos 設定やネットワークエラーも確認します。
AD : ISE アカウントパスワードの更新に失敗 (AD: ISE account password update failed)	ISE-PIC サーバーは、AD のマシンアカウントパスワードを更新できませんでした。	Cisco ISE-PIC のマシンアカウントパスワードが変更されていないこと、およびマシンアカウントが無効でなく制限もされていないことを確認します。KDC への接続を確認します。
参加しているドメインが使用不可 (Joined domain is unavailable)	参加しているドメインが使用できず、認証、許可、およびグループと属性の取得に使用できません。	DNS 設定、Kerberos 設定、エラー状態、およびネットワーク接続を確認します。

アラーム名	アラームの説明	アラームの解決方法
ID ストアが使用不可 (Identity Store Unavailable)	Cisco ISE-PIC のポリシーサービスノードは設定された ID ストアに到達できません。	Cisco ISE-PIC と ID ストア間のネットワーク接続を確認します。
AD : ISE のマシンアカウントにグループを取得するために必要な権限がない	Cisco ISE-PIC のマシンアカウントにグループを取得するために必要な権限がありません。	Cisco ISE-PIC のマシンアカウントに Active Directory のユーザーグループを取得する権限があるかどうかを確認します。
システムの状態		
ディスク I/O 使用率が高い (High Disk I/O Utilization)	Cisco ISE-PIC システムは、ディスク I/O 使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
ディスク領域の使用率が高い (High Disk Space Utilization)	Cisco ISE-PIC システムは、ディスク領域の使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
負荷平均が高い (High Load Average)	Cisco ISE-PIC システムは、負荷平均が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラアクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。

アラーム名	アラームの説明	アラームの解決方法
メモリ使用率が高い (High Memory Utilization)	Cisco ISE-PIC システムは、メモリ使用率が高くなっています。	システムに十分なリソースがあるかどうかを確認します。システムの実際の作業量、たとえば、認証数、プロファイラ アクティビティなどを確認します。負荷を分散するためにさらにサーバーを追加します。
操作DBの使用率が高い (High Operations DB Usage)	ノードをモニタする Cisco ISE-PIC は、syslog データの量が想定よりも多くなっています。	操作データの消去設定ウィンドウを確認して削減します。
ヘルス ステータスが使用不可	モニタリングノードは Cisco ISE-PIC ノードからヘルスステータスを受信しませんでした。	Cisco ISE-PIC ノードが稼働中であることを確認します。Cisco ISE-PIC ノードがモニタリングノードと通信できることを確認します。
プロセスがダウン (Process Down)	Cisco ISE-PIC プロセスの 1 つが動作していません。	Cisco ISE-PIC アプリケーションを再起動します。
OCSP トランザクションしきい値に到達 (OCSP Transaction Threshold Reached)	OCSP トランザクションしきい値に到達しました。このアラームは、内部 OCSP サービスが大量のトラフィックに到達するとトリガーされます。	システムに十分なリソースがあるかどうかを確認してください。
ライセンスリング		
PIC ライセンスの期限切れ (PIC License Expired)	Cisco ISE-PIC ノードにインストールされたライセンスの期限が切れました。	シスコアカウントチームにお問い合わせ、新しいライセンスを購入してください。
PIC ライセンスが 30 日以内に期限が切れます (PIC License expiring within 30 Days)	Cisco ISE-PIC ノードにインストールされたライセンスが 30 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。
PIC のライセンスが 60 日以内に期限が切れます (License expiring within 60 Days)	Cisco ISE-PIC ノードにインストールされたライセンスが 60 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。
PIC のライセンスが 90 日以内に期限が切れます (License expiring within 90 Days)	Cisco ISE-PIC ノードにインストールされたライセンスが 90 日後に期限切れになります。	ISE-PIC ライセンスの延長については、シスコの営業チームにお問い合わせください。

アラーム名	アラームの説明	アラームの解決方法
システム エラー		
ログ収集エラー (Log Collection Error)	コレクタプロセスをモニターする Cisco ISE-PIC がポリシーサービスノードから生成された監査ログを保持できません。	これは、ポリシー サービスノードの実際の機能に影響を与えません。その他の解決のために TAC に連絡してください。
スケジュールされているレポートのエクスポートに失敗 (Scheduled Report Export Failure)	設定されたリポジトリにエクスポートされたレポート (CSV ファイル) をコピーできません。	設定されたリポジトリを確認します。それが削除されていた場合は、再度追加します。それが使用できないか、またはそれに到達できない場合は、リポジトリを再設定して有効にします。

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

アラーム設定

次の表では、[アラーム設定 (Alarm Settings)] ウィンドウ ([設定 (Settings)] > [アラーム設定 (Alarm Settings)]) のフィールドについて説明します。

フィールド名	説明
アラームタイプ (Alarm Type)	アラームタイプ。
アラーム名 (Alarm Name)	アラームの名前。
説明 (Description)	アラームの説明。
推奨されるアクション (Suggested Actions)	アラームがトリガーされたときに実行されるアクション。
ステータス (Status)	アラームルールの有効化または無効化。

フィールド名	説明
重大度	アラームの重大度レベルを選択します。有効なオプションは次のとおりです。 <ul style="list-style-type: none"> • [重大 (Critical)]: 重大なエラーの条件を示します。 • [警告 (Warning)]: 正常ではあるものの重要な状態を示します。これがデフォルトの条件です。 • [情報 (Info)]: 情報メッセージを示します。
syslog メッセージを送信 (Send Syslog Message)	Cisco ISE-PIC で生成される各システムアラームの syslog メッセージを送信します。
複数の電子メールアドレスをカンマで区切って入力	電子メールアドレスまたは ISE-PIC 管理者名あるいはその両方のリスト。
電子メールのメモ (0 ~ 4,000 文字)	システムアラームに関連付けるカスタムテキストメッセージ。

カスタム アラームの追加

シスコ ISE-PIC には、5つのデフォルトのアラームタイプ（設定変更、高ディスク I/O 使用率、高ディスク容量使用率、高メモリ使用率、ISE 認証非アクティブ）があります。シスコ定義のシステムアラームは [アラーム設定 (Alarms Settings)] ページ ([設定 (Settings)] > [アラーム設定 (Alarms Settings)]) に表示されます。システムアラームだけを編集できます。

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

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

アラームを追加するには、次の手順を実行します。

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

ステップ 2 [アラームの設定 (Alarm Configuration)] タブで、[追加 (Add)] をクリックします。

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

アラームタイプに基づいて、追加の属性が [アラームの設定 (Alarm Configuration)] ページに表示されます。たとえば、設定変更アラームには、[オブジェクト名 (Object Name)]、[オブジェクトタイプ (Object Types)] および [管理者名 (Admin Name)] フィールドが表示されます。さまざまな基準で同じアラームの複数のインスタンスを追加できます。

ステップ 4 [送信 (Submit)] をクリックします。

着信トラフィックを検証する TCP ダンプユーティリティ

パケットをスニффイングする TCP ダンプユーティリティを使用して、予定していたパケットがノードに到達したかどうかを確認できます。たとえば、レポートに示されている着信認証またはログがない場合、着信トラフィックがないのではないかと疑われる場合があります。このような場合、検証するためにこのツールを実行できます。

TCP ダンプオプションを設定し、ネットワークトラフィックからデータを収集して、ネットワークの問題をトラブルシューティングできます。



注意 TCP ダンプを起動すると、以前のダンプファイルは自動的に削除されます。以前のダンプファイルを保存するには、新しい TCP ダンプセッションを開始する前に、「TCP ダンプファイルの保存」の項の説明に従ってタスクを実行します。

ネットワークトラフィックのモニターリングでの TCP ダンプの使用

始める前に

[TCP ダンプ (TCP Dump)] ウィンドウの [ネットワーク インターフェイス (Network Interface)] ドロップダウンリストには、IPv4 または IPv6 アドレスが設定されているネットワーク インターフェイス カード (NIC) のみが表示されます。VMware のデフォルトでは、すべての NIC が接続されるため、すべての NIC に IPv6 アドレスが設定されて、[ネットワーク インターフェイス (Network Interface)] ドロップダウンリストに表示されます。

ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [TCP ダンプ (TCP Dump)] を選択します。

ステップ 2 [ホスト名 (HostName)] ドロップダウンリストから、TCP ダンプユーティリティのソースを選択します。

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

ステップ 4 [無差別モード (Promiscuous Mode)] トグルボタンをクリックして、[オン (On)] または [オフ (Off)] にします。デフォルトは [オン (On)] です。

無差別モードは、ネットワーク インターフェイスがシステムの CPU にすべてのトラフィックを渡すデフォルトパケット スニッフイング モードです。この設定のままにすることを推奨します。

ステップ 5 [フィルタ (Filter)] フィールドに、フィルタ処理のもとになるブール式を入力します。

サポートされている標準 TCP ダンプフィルタ式は、次のとおりです。

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

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

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



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

TCP ダンプ ファイルの保存

始める前に

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



(注) Cisco ISE CLI を使用して TCP ダンプにアクセスすることもできます。詳細については、『[Cisco Identity Services Engine CLI リファレンス ガイド](#)』を参照してください。

ステップ 1 [操作 (Operations)] > [トラブルシューティング (Troubleshoot)] > [診断ツール (Diagnostic Tools)] > [一般ツール (General Tools)] > [TCP ダンプ (TCP Dump)] を選択します。

ステップ 2 [フォーマット (Format)] ドロップダウンリストからオプションを選択します。[可読 (Human Readable)] がデフォルトです。

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

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

TCP ダンプの設定

次の表では、ネットワーク インターフェイスのパケットの内容をモニターし、ネットワークで問題が発生したときにはトラブルシューティングするために使用する `tcpdump` ユーティリティ ページ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、[トラブルシューティング (Troubleshoot)] です。

表 3: TCP ダンプの設定

オプション	使用上のガイドライン
ステータス	<ul style="list-style-type: none"> • [停止済み (Stopped)] : tcpdump ユーティリティは実行されていません。 • [開始 (Start)] : tcpdump ユーティリティによるネットワークのモニターリングを開始する場合にクリックします。 • [停止 (Stop)] : tcpdump ユーティリティを停止する場合にクリックします。
ホスト名 (Host Name)	モニターするホストの名前をドロップダウンリストから選択します。
ネットワーク インターフェイス (Network Interface)	<p>モニターするネットワーク インターフェイスの名前をドロップダウンリストから選択します。</p> <p>(注) IPv4 アドレスまたは IPv6 アドレスを持つすべてのネットワーク インターフェイス カード (NIC) を Cisco ISE 管理者ポータルに表示されるように設定する必要があります。</p>
無差別モード (Promiscuous Mode)	<ul style="list-style-type: none"> • [オン (On)] : 無差別モードを有効にする場合にクリックします (デフォルト)。 • [オフ (Off)] : 無差別モードを無効にする場合にクリックします。 <p>無差別モードがデフォルトのパケット スニフリング モードです。有効に設定しておくことを推奨します。このモードでは、ネットワーク インターフェイスはすべてのトラフィックをシステムの CPU に渡します。</p>
フィルタ	<p>フィルタリング基準として使用するブール式を入力します。サポートされている標準 tcpdump フィルタ式 :</p> <pre>ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123</pre>

オプション	使用上のガイドライン
フォーマット (Format)	tcpdump ファイルのフォーマットを選択します。
ダンプファイル (Dump File)	<p>最後のダンプファイルに記録された、次のようなデータを表示します。</p> <p>Last created on Wed Apr 27 20:42:38 UTC 2011 by admin</p> <p>File size: 3,744 bytes Format: Raw Packet Data Host Name: Positron Network Interface: GigabitEthernet 0 Promiscuous Mode: On</p> <ul style="list-style-type: none"> • [ダウンロード (Download)]: 最新のダンプファイルをダウンロードする場合にクリックします。 • [削除 (Delete)]: 最新のダンプファイルを削除する場合にクリックします。

ロギングメカニズム

Cisco ISE-PIC ロギングメカニズム

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。

Smart Call Home

Smart Call Home (SCH) は、ネットワーク内の Cisco ISE-PIC デバイスを監視し、重大なイベントに関して電子メールで知らせます。電子メールには、環境情報と修復に関するアドバイスが記載されたリアルタイムのアラートが含まれています。

- [シスコアカウント (Cisco Account)]: SCH からの電子メールを受信できるようにシスコアカウントを入力します。この ID は、お客様に影響する重大な問題が SCH によって発見された場合の連絡にも使用される場合があります。
- [トランスポートゲートウェイ (Transport Gateway)]: セキュリティを強化するために、Cisco ISE とシスコの外部テレメトリ サーバーの間でプロキシを使用することができます。

そうする場合は、このオプションをオンにして、プロキシサーバーの FQDN を入力します。

シスコでは、Cisco.com からダウンロードできるトランスポートゲートウェイ用のソフトウェアを提供しています。このソフトウェアは、Linux サーバー上で実行されます。RHEL サーバーでの Transport Gateway ソフトウェアの導入方法については、『[Smart Call Home Deployment Guide](#)』を参照してください。

SCH 機能の有効化については、[Smart Call Home サービスの登録 \(26 ページ\)](#) を参照してください。

Smart Call Home プロファイル

Smart Call Home プロファイルは、デバイスでモニターされるイベントのタイプを決定します。Cisco ISE-PIC には、次のデフォルトプロファイルがあります。

- ciscotac-1 : 匿名レポートのために使用されます
- isesch-1 : Smart Call Home 機能のために使用されます

匿名レポートのために使用されるデフォルトプロファイル (ciscotac-1) を編集することはできません。

Anonymous Reporting

Cisco ISE-PIC は、ユーザーの展開に関する非機密情報を安全に収集します。このデータは、Cisco ISE-PIC の使用状況をより詳しく把握し、製品と製品が提供するさまざまなサービスを向上させる目的で収集されます。

デフォルトでは、anonymous reporting は有効になっています。anonymous reporting を使用不可にするには、ISE-PIC 管理者ポータル[[設定 \(Settings\)](#)] > [[Smart Call Home](#)]で行うことができます。

Smart Call Home サービスの登録

ステップ 1 [[設定 \(Settings\)](#)] > [[Smart Call Home](#)] を選択します。

ステップ 2 次のいずれかを実行します。

- SCH のすべての機能をオンにする (Turn on full SCH capability)
- デフォルト SCH テレメトリ設定を保持して匿名データのみを送信する (Keep the default SCH telemetry settings and send only anonymous data)
- すべて無効にする (Disable everything)

ステップ 3 ([SCH のすべての機能をオンにする (Turn on full SCH capability)] オプションを選択した場合のみ) [[登録ステータス \(Registration Status\)](#)] エリアに電子メールアドレスを入力します。

ステップ 4 (オプション) [Transport Gateway] チェックボックスをオンにして、Transport Gateway の URL を入力します。

ステップ 5 [保存 (Save)] をクリックします。

SCH のすべての機能を有効にしている場合は、アクティベーションリンクが記載された電子メールを受信します。アクティベーションリンクをクリックして記載されている指示に従い、登録を完了します。

Active Directory のトラブルシューティング

Active Directory と Cisco ISE-PIC の統合の前提条件

この項では、Cisco ISE-PIC と統合する Active Directory を設定するために必要な手動での作業手順について説明します。ただしほとんどの場合、Cisco ISE-PIC が Active Directory を自動的に設定するようにできます。次に、Cisco ISE-PIC と Active Directory を統合するための前提条件を示します。

- AD ドメイン設定の変更に必要な Active Directory ドメイン管理者クレデンシャルがあることを確認します。
- Cisco ISE-PIC サーバーと Active Directory 間の時間を同期するために Network Time Protocol (NTP) サーバー設定を使用します。Cisco ISE-PIC CLI で NTP を設定できます。
- Cisco ISE-PIC の参加先ドメインでは、少なくとも 1 つのグローバルカタログサーバーが動作し、Cisco ISE-PIC からアクセス可能である必要があります。

さまざまな操作の実行に必要な Active Directory アカウント権限

参加操作	脱退処理	Cisco ISE-PIC マシン アカ ント
<p>参加操作には、次のアカウント権限が必要です。</p> <ul style="list-style-type: none"> Active Directory を検索する権限 (Cisco ISE-PIC マシンアカウントがあるかどうかの確認) ドメインに Cisco ISE-PIC マシン アカウントを作成する権限 (マシン アカウントが存在しない場合) 新しいマシン アカウントに属性を設定する権限 (Cisco ISE-PIC マシン アカウント パスワード、SPN、dnsHostname など) 	<p>脱退操作には、次のアカウント権限が必要です。</p> <ul style="list-style-type: none"> Active Directory を検索する権限 (Cisco ISE-PIC マシンアカウントがあるかどうかの確認) ドメインから Cisco ISE-PIC マシンアカウントを削除する権限 <p>強制脱退 (パスワードなしの脱退) を実行する場合、ドメインからマシンアカウントは削除されません。</p>	<p>Active Directory 接続と通信する Cisco ISE-PIC マシン アカウントには、次の権限が必要です。</p> <ul style="list-style-type: none"> パスワードを変更する。 接続されるユーザーおよびマシンに対応するユーザーおよびマシンオブジェクトを読み取る権限 情報を取得するために Active Directory をクエリする権限 (信頼ドメイン、代替の UPN サフィックスなど) tokenGroups 属性を読み取る権限 <p>Active Directory でマシン アカウントを事前に作成できます。SAM の名前が Cisco ISE-PIC アプライアンスのホスト名と一致する場合は、参加操作中に検索して再利用します。</p> <p>複数の参加操作が実行される場合、参加ごとに複数のマシン アカウントが Cisco ISE-PIC 内で保持されます。</p>



(注) 参加操作または脱退操作に使用するクレデンシャルは Cisco ISE-PIC に保存されません。新規作成された Cisco ISE-PIC マシンアカウントのログイン情報のみが保存されます。

Microsoft Active Directory のセキュリティポリシー「ネットワーク アクセス : SAM へのリモートの呼び出しを許可するクライアントを制限する」が改訂されました。このため、Cisco ISE は 15 日ごとにマシンアカウントのパスワードを更新できない場合があります。マシンアカウントのパスワードが更新されない場合、Cisco ISE は Microsoft Active Directory を介してユーザー

を認証しません。このイベントを通知するために、Cisco ISE ダッシュボードに [AD : ISE アカウントパスワードの更新に失敗 (AD: ISE account password update failed)] アラームが表示されます。



- (注) この問題は、Windows Server 2016 Active Directory 以降および Windows 10 バージョン 1607 の制限により発生します。この制限を克服するには、Windows Server 2016 Active Directory 以降または Windows 10 バージョン 1607 を Cisco ISE と統合する場合、レジストリ：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam のレジストリ値を non-zero から空白に設定して、すべてにアクセスを提供する必要があります。これにより、Cisco ISE がそのマシンのアカウントパスワードを更新できるようになります。

セキュリティポリシーにより、ユーザーはローカルセキュリティアカウントマネージャ (SAM) データベース内と Microsoft Active Directory 内のユーザーとグループを列挙できます。Cisco ISE がマシンアカウントのパスワードを更新できるようにするには、Microsoft Active Directory の設定が正しいことを確認します。影響を受ける Windows オペレーティングシステムと Windows Server のバージョン、ネットワークにおけるこのセキュリティポリシーの意味、必要な変更の詳細については、以下を参照してください。

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>

通信用に開放するネットワークポート

プロトコル	ポート (リモートローカル)	ターゲット	注記
DNS (TCP/UDP)	49152 以上の乱数	DNS サーバー/AD ドメイン コントローラ	—
MSRPC	445	ドメインコントローラ	—
Kerberos (TCP/UDP)	88	ドメインコントローラ	MS AD/KDC
LDAP (TCP/UDP)	389	ドメインコントローラ	—
LDAP (GC)	3268	グローバル カタログ サーバー	—
NTP	123	NTP サーバー/ドメイン コントローラ	—
IPC	80	セカンダリ ISE-PIC ノードの場合	—

Active Directory でISE-PIC

ISE-PIC では、Active Directory ドメインコントローラによって生成される Active Directory ログイン監査イベントを利用して、ユーザーログイン情報を収集します。ISE ユーザーが接続を行い、ユーザーログイン情報を取得できるように、Active Directory サーバーを適切に設定する必要があります。ここでは、ISE-PIC をサポートするように Active Directory ドメインコントローラを設定する方法（Active Directory 側からの設定）について説明します。

をサポートするように Active Directory ドメインコントローラを設定するには（Active Directory 側からの設定）、次の手順に従います：



(注) すべてのドメインのすべてのドメインコントローラを設定する必要があります。

1. ISE-PIC から Active Directory の参加ポイントとドメインコントローラを設定します。 [Active Directory 参加ポイントの追加および参加ポイントへの Cisco ISE-PIC ノードの参加](#) および [#unique_218](#) を参照してください。
2. ドメイン コントローラごとに WMI を設定します。 [#unique_219](#) を参照してください。
3. Active Directory で次の操作を実行します。
 - [パッシブ ID サービス の Active Directory の設定](#) (30 ページ)
4. (オプション) Active Directory で ISE により実行された自動設定のトラブルシューティングを行うには、次の操作を実行します。
 - [Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定](#) (35 ページ)
 - [ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限](#) (35 ページ)
 - [ドメイン コントローラで DCOM を使用するための権限](#) (37 ページ)
 - [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定](#) (39 ページ)
 - [AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与](#) (40 ページ)

パッシブ ID サービス の Active Directory の設定

ISE-PIC、ユーザー ログイン情報を収集するため、Active Directory ドメインコントローラにより生成される Active Directory ログイン監査イベントが使用されます。ISE-PIC は Active Directory に接続し、ユーザー ログイン情報を取得します。

次の手順は、Active Directory ドメイン コントローラから実行する必要があります。

ステップ 1 該当する Microsoft のパッチが Active Directory ドメイン コントローラにインストールされていることを確認します。

- Windows Server 2008 には次のパッチが必要です。

- <http://support.microsoft.com/kb/958124>

このパッチは Microsoft の WMI のメモリリークを修正し、ISE がドメインコントローラとの正常な接続を確立できないようにします。

- <http://support.microsoft.com/kb/973995>

このパッチは、Microsoft WMI の別のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

- Windows Server 2008 R2 では、（SP1 がインストールされていない場合）次のパッチが必要です。

- <http://support.microsoft.com/kb/981314>

このパッチは、Microsoft WMI のメモリ リークを解消します。このメモリ リークは、Active Directory ドメイン コントローラが必要なユーザー ログイン イベントをドメイン コントローラのセキュリティ ログに書き込むのを散発的に妨げます。

- <http://support.microsoft.com/kb/2617858>

このパッチは、Windows Server 2008 R2 での予期しない起動やログインプロセスの遅れを解消します。

- Windows プラットフォームの WMI 関連問題には、次のリンクにリストされているパッチが必要です。

- <http://support.microsoft.com/kb/2591403>

これらのホットフィックスは、WMI サービスおよび関連コンポーネントの動作と機能に関連付けられます。

ステップ 2 Active Directory がユーザー ログイン イベントを Windows セキュリティ ログに記録するのを確認します。

[監査ポリシー (Audit Policy)] の設定 ([グループポリシー管理 (Group Policy Management)] の設定の一部) が、正常なログインによって Windows セキュリティログに必要なイベントが生成されるように設定されていることを確認します (これはデフォルトの Windows 設定ですが、この設定が適切であることを明示的に確認する必要があります)。

ステップ 3 ISE-PIC が Active Directory に接続するための十分な権限を持つ Active Directory ユーザーを設定する必要があります。次の手順では、管理ドメイングループのユーザー、または管理ドメイングループではないユーザーに対して権限を定義する方法を示します。

- Active Directory ユーザーが Domain Admin グループのメンバーである場合に必要な権限
- Active Directory ユーザーが Domain Admin グループのメンバーでない場合に必要な権限

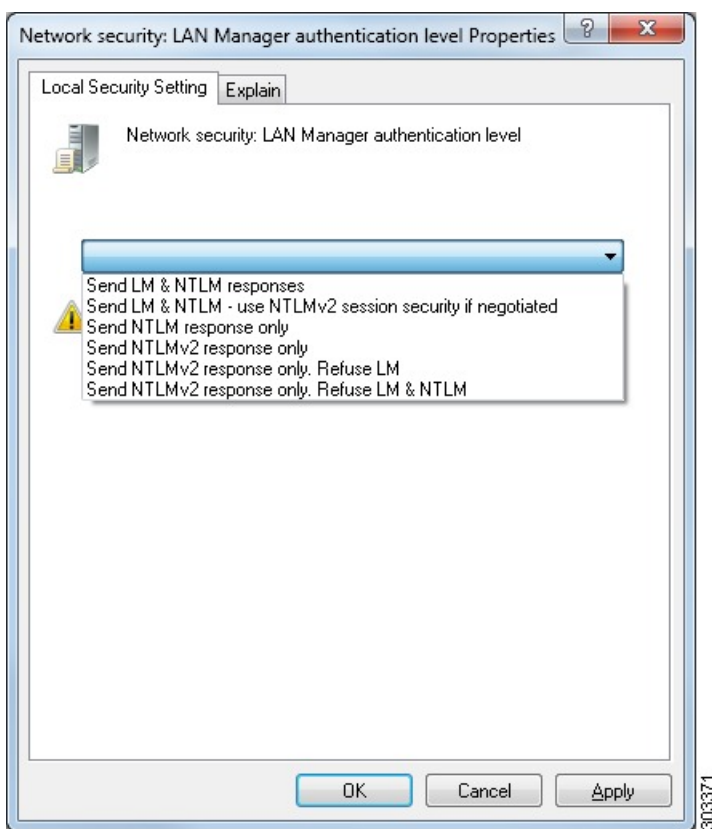
ステップ 4 ISE-PIC によって使用される Active Directory ユーザーは、NT Lan Manager (NTLM) v1 または v2 のいずれかによって認証を受けることができます。ISE-PIC と Active Directory ドメイン コントローラ間の正常な認証済み接続を確実にを行うために、Active Directory NTLM の設定が ISE-PIC NTLM の設定と合っていることを確認する必要があります。次の表に、すべての Microsoft NTLM オプションと、サポート対象の ISE-PIC NTLM アクションを示します。ISE-PIC が NTLMv2 に設定される場合、記載されている 6 つのオプションがすべてサポートされます。NTLMv1 をサポートするように ISE-PIC が設定されている場合、最初の 5 つのオプションだけがサポートされます。

表 4: ISE-PIC と AD NTLM のバージョン設定に基づいてサポートされる認証タイプ

ISE-PIC ISE NTLM の設定オプション および Active Directory (AD) NTLM の設定オプション (NTLMv1 NTLMv2)	NTLMv1	NTLMv2
LM & NTLM 応答を送信接続を許可 接続を許可 (Send LM & NTLM responses connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
LM & NTLM を送信: ネゴシエー トされた接続が許可された場合に NTLMv2 セッションセキュリティ を使用接続を許可 (Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみ NTLM 応答を送信接続を許可 (Send NTLM response only connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
接続が許可された場合にのみ NTLMv2 応答を送信接続を許可 (Send NTLMv2 response only connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます
NTLMv2 応答のみを送信 (Send NTLMv2 response only)。LM を拒 否接続を許可接続を許可 (Refuse LM connection is allowed connection is allowed)	接続が受け入れられます	接続が受け入れられます

ISE-PICのNTLMの設定オプション および Active Directory (AD) NTLM の設定オプション (NTLMv1 NTLMv2)	NTLMv1	NTLMv2
NTLMv2応答のみを送信 (Send NTLMv2 response only)。LM & NTLMを拒否接続を拒否接続を許可 (Refuse LM & NTLM connection is refused connection is allowed)	接続は拒否されます	接続が受け入れられます

図 1: MS NTLM 認証タイプのオプション



ステップ 5 Active Directory ドメイン コントローラで `dllhost.exe` へのトラフィックを許可するファイアウォールルールを作成していることを確認します。

ファイアウォールをオフにするか、または次のポートへの特定の IP (ISE-PIC IP アドレス) のアクセスを許可することができます。

- TCP 135 : 一般的な RPC ポート。非同期 RPC 発信をすると、このポートでリスニングしているサービスが、クライアントに、この要求を処理できるコンポーネントが使用しているポートを通知します。
- UDP 137 : NetBIOS 名前解決

- UDP 138 : NetBIOS データグラム サービス
- TCP 139 : NetBIOS セッション サービス
- TCP 445 : SMB

数値の大きいポートは動的に割り当てられ、手動で設定できます。ターゲットとして %SystemRoot%\System32\dlhhost.exe を追加することを推奨します。このプログラムは、ポートを動的に管理します。

すべてのファイアウォールルールを、特定の IP アドレス (ISE-PIC IP) に割り当てることができます。

Windows 監査ポリシーの設定

監査ポリシー (グループポリシー管理設定の一部) が正常なログインを許可していることを確認します。これには、AD ドメイン コントローラ マシンの Windows セキュリティ ログに必要なイベントを生成する必要があります。これはデフォルトの Windows 設定ですが、この設定が正しいことを確認する必要があります。

ステップ 1 [スタート] > [Programs] > [Administrative Tools] > [Group Policy Management] を選択します。

ステップ 2 [Domains] で関連するドメインに移動し、ナビゲーション ツリーを展開します。

ステップ 3 [Default Domain Controller Policy] を選択し、右クリックして、[編集] を選択します。

グループ ポリシー管理エディターが表示されます。

ステップ 4 [デフォルトのドメインコントローラ ポリシー (Default Domain Controllers Policy)] > [コンピュータ設定 (Computer Configuration)] > [ポリシー (Policies)] > [Windows 設定 (Windows Settings)] > [セキュリティ設定 (Security Settings)] の順に選択します。

- Windows Server 2003 または Windows Server 2008 (R2 以外) の場合は [ローカルポリシー (Local Policies)] > [監査ポリシー (Audit Policy)] の順に選択します。2つのポリシー項目 ([Audit Account Logon Events] と [Audit Logon Events]) で、対応する [Policy Setting] に [Success] 状態が直接的または間接的に含まれていることを確認します。[Success] 状況を間接的に含めるには、[Policy Setting] に [Not Defined] を設定します。この場合、上位ドメインから有効値が継承されるため、[Success] 状態を明示的に含めるようにその上位ドメインの [Policy Setting] を設定する必要があります。
- Windows Server 2008 R2 および Windows 2012 の場合、[Advanced Audit Policy Configuration] > [Audit Policies] > [Account Logon] を選択します。2つのポリシー項目 ([Audit Kerberos Authentication Service] と [Audit Kerberos Service Ticket Operations]) に対応する [Policy Setting] に、前述のように [Success] 状態が直接または間接的に含まれていることを確認します。

(注) Active Directory ドメイン コントローラの設定で RC4 暗号が無効になっている場合を除き、Cisco ISE は Active Directory との通信に Kerberos プロトコルで RC4 暗号を使用します。Active Directory で [ネットワークセキュリティ : Kerberos] で許可される暗号タイプを設定 (Network Security: Configure Encryption Types Allowed for Kerberos)] オプションを使用すると、Kerberos プロトコルで許可される暗号タイプを設定できます。

ステップ 5 [監査ポリシー] の項目設定が変更されている場合は、`gpupdate /force` を実行して新しい設定を強制的に有効にする必要があります。

Microsoft Active Directory ユーザーがドメイン管理グループに属しているときの権限の設定

Windows 2008 R2、Windows Server 2012 および Windows Server 2012 R2 の場合、ドメイン管理グループは、デフォルトで Windows オペレーティングシステムの特定のレジストリ キーを完全に制御することはできません。Microsoft Active Directory の管理者は、Microsoft Active Directory ユーザーに次のレジストリキーに対する完全制御権限を提供する必要があります。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

次の Microsoft Active Directory バージョンでは、レジストリを変更する必要はありません。

- Windows 2003
- Windows 2003R2
- Windows 2008

完全な制御を許可するには、まず Microsoft Active Directory 管理者がキーの所有権を取得する必要があります。

ステップ 1 キーアイコンを右クリックし、[所有者 (Owner)] タブを選択します。

ステップ 2 [アクセス許可 (Permissions)] をクリックします。

ステップ 3 [詳細設定 (Advanced)] をクリックします。

ドメイン管理グループに属していない Microsoft Active Directory ユーザー の権限

Windows 2012 R2 の場合は、Microsoft AD ユーザーに次のレジストリキーに対する完全制御権限を提供します。

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell で次のコマンドを使用して、レジストリキーに完全な権限が付与されているかどうかを確認します。

- ```
get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```
- ```
get-acl -path "hkml:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```

Microsoft AD ユーザーがドメイン管理者グループではなく、ドメインユーザーグループに所属している場合は、次の権限が必要です。

- ISE-PIC がドメインコントローラに接続できるようにするには、レジストリキーを追加します。
- [ドメイン コントローラで DCOM を使用するための権限 \(37 ページ\)](#)
- [WMI ルート/CIMv2 名前空間にアクセスするための権限の設定 \(39 ページ\)](#)

これらの権限は、次のバージョンの Microsoft AD でのみ必要となります。

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ドメインコントローラへの ISE-PIC の接続を許可するためにレジストリキーを追加

ISE-PIC がドメインユーザーとして接続し、ログイン認証イベントを取得できるようにするには、ドメインコントローラにいくつかのレジストリ キーを手動で追加する必要があります。エージェントはドメインコントローラまたはドメイン内のマシンには必要ありません。

次のレジストリのスクリプトは追加するキーを示しています。これをコピーしてテキストファイルに貼り付け、.reg の拡張子でファイルを保存し、ファイルをダブルクリックすることでレジストリの変更を行うことができます。レジストリ キーを追加するには、ルート キーのオーナーである必要があります。

Windows Registry Editor Version 5.00

```
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
```

```
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

```
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

DllSurrogate キーの値には、2つのスペースが含まれていることを確認します。レジストリを手動で更新する場合は、2つのスペースのみを含める必要があります、引用符は含めないでください。レジストリを手動で更新する際は、AppID、DllSurrogate、およびその値に引用符が含まれていないことを確認してください。

前述のスクリプトに示すように、ファイルの末尾の空の行を含めて、空の行は保持します。

Windows コマンドプロンプトで次のコマンドを使用して、レジストリキーが作成され、正しい値が設定されているかどうかを確認します。

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

ドメインコントローラで DCOM を使用するための権限

ISE-PIC パッシブ ID サービスに使用される Microsoft Active Directory ユーザーには、ドメインコントローラサーバーで DCOM を使用する権限が必要です。 `dcomcnfg` コマンドラインツールを使用して権限を設定します。

-
- ステップ 1** コマンドラインから `dcomcnfg` ツールを実行します。
 - ステップ 2** [コンポーネントサービス (Component Services)] を展開します。
 - ステップ 3** [コンピュータ (Computers)] > [マイコンピュータ (My Computer)] を展開します。
 - ステップ 4** メニューバーで [アクション (Action)] を選択し、[プロパティ (Properties)] をクリックして [COM セキュリティ (COM Security)] をクリックします。
 - ステップ 5** Cisco ISE がアクセスと起動の両方に使用するアカウントには許可権限が必要です。4つのオプション ([アクセス権限 Access Permissions]) と [起動およびアクティブ化の権限 (Launch and Activation Permissions)] の両方に対する [制限の編集 (Edit Limits)] と [デフォルトの編集 (Edit Default)] のすべてに Microsoft Active Directory ユーザーを追加します。
 - ステップ 6** [アクセス権限 (Access Permissions)] と [起動およびアクティブ化の権限 (Launch and Activation Permissions)] の両方に対してローカルアクセスとリモートアクセスをすべて許可します。

図 2: [アクセス権限 (Access Permissions)] に対するローカルアクセスとリモートアクセス

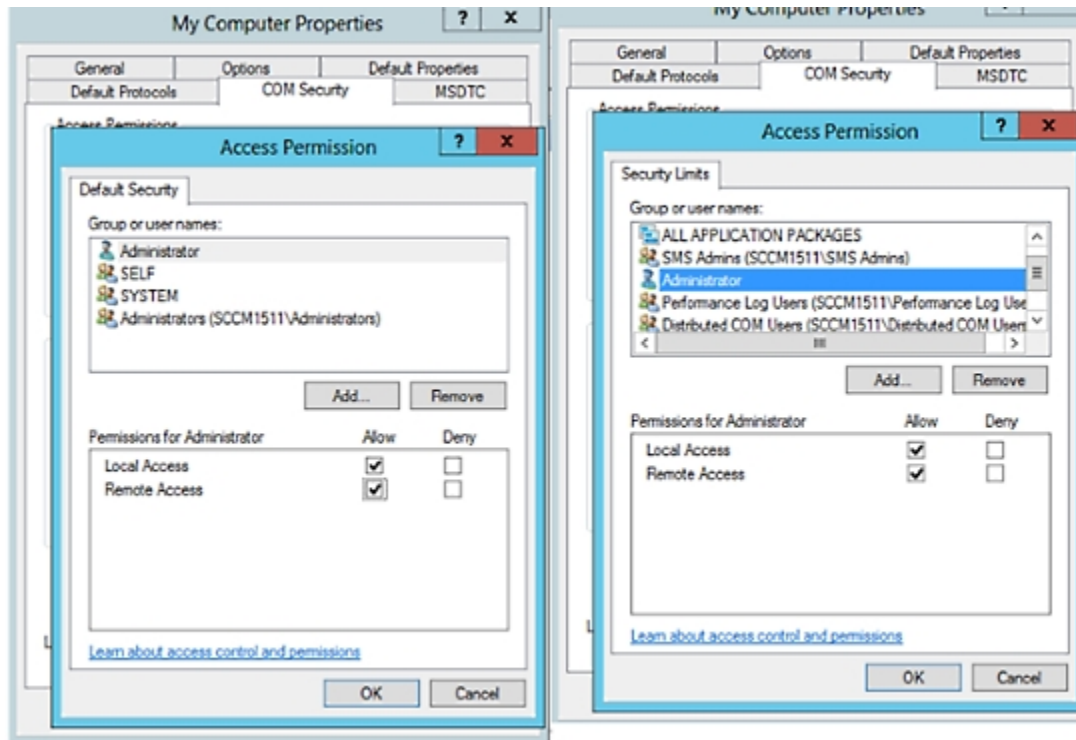
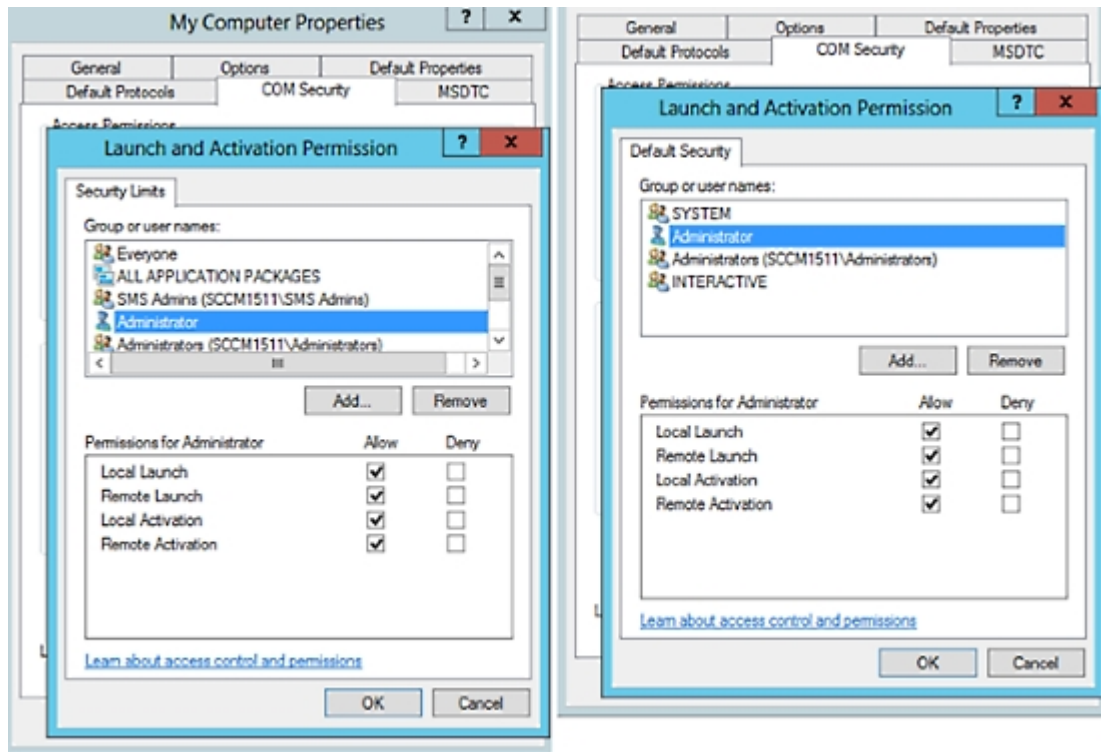


図 3: [起動およびアクティブ化の権限 (Launch and Activation Permissions)] のローカルアクセスとリモートアクセス

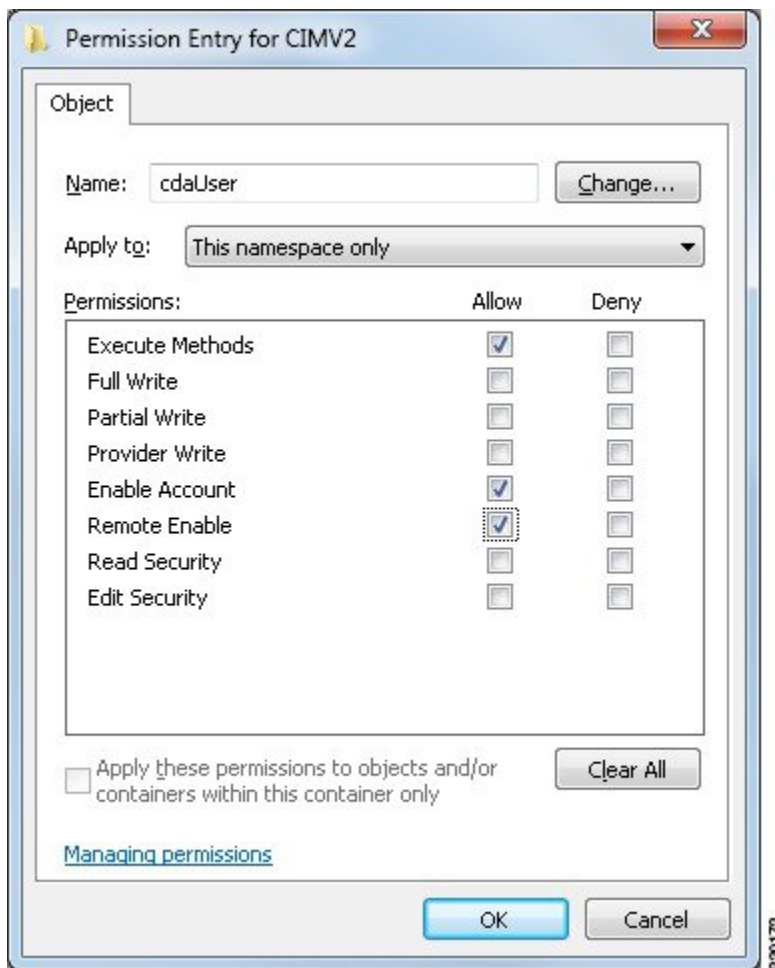


WMI ルート/CIMv2 名前空間にアクセスするための権限の設定

デフォルトでは、Microsoft Active Directory ユーザーには実行メソッドおよびリモートの有効化のための権限がありません。wmimgmt.msc MMC コンソールを使用してアクセス権を付与できます。

- ステップ 1 [スタート (Start)] > [実行 (Run)] を選択し、wmimgmt.msc と入力します。
- ステップ 2 [WMI Control] を右クリックし、[プロパティ (Properties)] をクリックします。
- ステップ 3 [セキュリティ (Security)] タブで、[ルート (Root)] を展開し、[CIMV2] を選択します。
- ステップ 4 [セキュリティ (Security)] をクリックします。
- ステップ 5 次のイメージに示すように、Microsoft Active Directory ユーザーを追加し、必要な権限を設定します。

AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与



AD ドメインコントローラのセキュリティイベントログへのアクセス権の付与

Windows 2008 以降では、ISE-PIC ID マッピング ユーザーを Event Log Reader と呼ばれるグループに追加することで、AD ドメイン コントローラのログへのアクセス権を付与できます。

Windows のすべての旧バージョンでは、次に示すようにレジストリ キーを編集する必要があります。

ステップ 1 セキュリティ イベント ログへのアクセス権を委任するには、アカウントの SID を検索します。

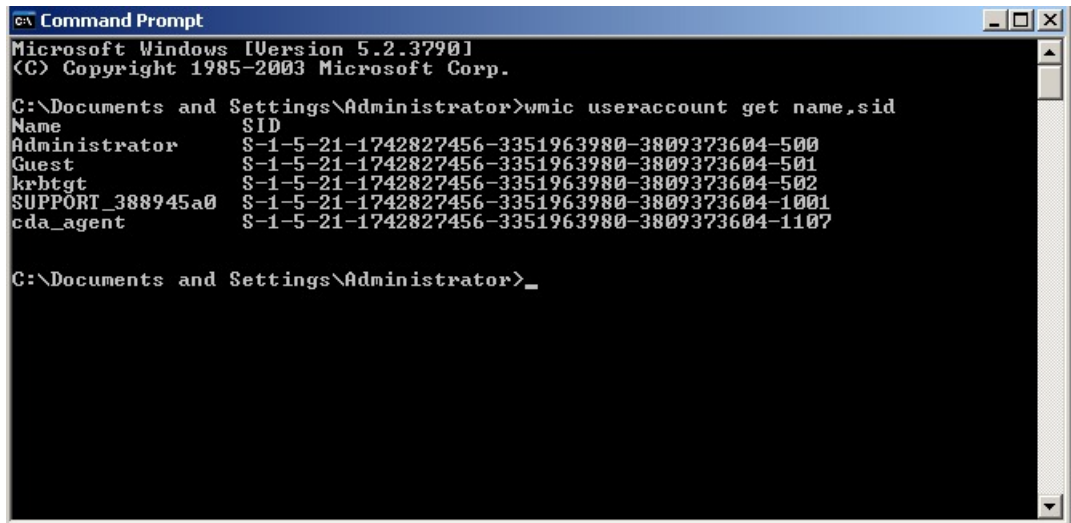
ステップ 2 すべての SID アカウントを表示するには、次の図に示すように、コマンドラインから次のコマンドを使用します。

```
wmic useraccount get name,sid
```

特定のユーザー名とドメインに対して、次のコマンドを使用することもできます。

```
wmic useraccount where name="iseUser" get domain,name,sid
```


図 4: すべての SID アカウントの表示



```

c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>wmic useraccount get name,sid
Name                SID
Administrator      S-1-5-21-1742827456-3351963980-3809373604-500
Guest               S-1-5-21-1742827456-3351963980-3809373604-501
krbtgt              S-1-5-21-1742827456-3351963980-3809373604-502
SUPPORT_388945a0    S-1-5-21-1742827456-3351963980-3809373604-1001
cda_agent           S-1-5-21-1742827456-3351963980-3809373604-1107

C:\Documents and Settings\Administrator>_

```

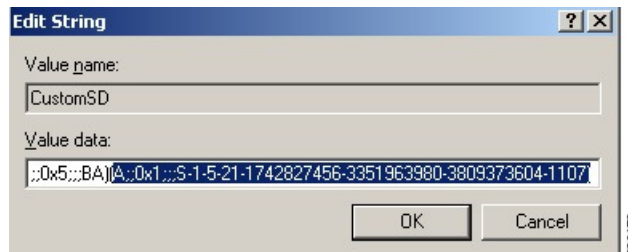
ステップ 3 SID を見つけ、レジストリ エディタを開き、次の場所を参照します。

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog

ステップ 4 [セキュリティ (Security)] をクリックし、[CustomDS] をダブルクリックします。

たとえば、ise_agent アカウント (SID: S-1-5-21-1742827456-3351963980-3809373604-1107) への読み取りアクセスを許可するには、「(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)」と入力します。

図 5: CustomSD 文字列の編集



ステップ 5 ドメインコントローラ上で WMI サービスを再起動します。次の 2 とおりの方法で WMI サービスを再起動できます。

a) CLI から次のコマンドを実行します。

```
net stop winmgmt
```

```
net start winmgmt
```

b) Services.msc を実行します。これにより、Windows サービス管理ツールが開きます。Windows サービス管理ウィンドウで、「Windows Management Instrumentation」サービスを検索し、右クリックして [再起動] を選択します。

その他のトラブルシューティング情報の入手

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



- (注) サポートバンドルおよびデバッグログにより、高度なトラブルシューティング情報が TAC に提供されます。サポートバンドルおよびデバッグログは解釈が困難です。Cisco ISE-PIC で提供されるさまざまなレポートおよびトラブルシューティングツールを使用して、ネットワークで直面している問題を診断およびトラブルシューティングできます。

Cisco ISE-PIC のサポートバンドル

サポートバンドルに含めるログを設定できます。たとえば、特定のサービスのログをデバッグログに含めるように設定できます。また、日付に基づいてログをフィルタリングできます。

ダウンロードできるログは、次のように分類されます。

- 完全な設定データベース：Cisco ISE-PIC 設定データベースは、可読の XML 形式です。問題をトラブルシューティングする場合、このデータベース設定を別の Cisco ISE ノードにインポートして、シナリオを再現できます。
- デバッグログ：ブートストラップ、アプリケーション設定、ランタイム、展開、公開キーインフラストラクチャ (PKI) 情報、およびモニターリングとレポートがキャプチャされます。

デバッグログによって、特定の Cisco ISE コンポーネントのトラブルシューティング情報が提供されます。デバッグログを有効にするには、「Logging」の第 11 章を参照してください。デバッグログを有効にしない場合、情報メッセージ (INFO) はすべてサポートバンドルに含まれます。詳細については、[Cisco ISE-PIC デバッグログ \(44 ページ\)](#) を参照してください。

- ローカルログ：Cisco ISE で実行されるさまざまなプロセスからの syslog メッセージが含まれています。
- コアファイル：クラッシュの原因の特定に役立つ重要な情報が含まれています。これらのログは、アプリケーションがクラッシュしたためアプリケーションにヒープダンプが含まれている場合に作成されます。
- モニターリングおよびレポートログ：アラートおよびレポートに関する情報が含まれています。
- システムログ：Cisco Application Deployment Engine (ADE) 関連の情報が含まれています。

- ポリシー設定：Cisco ISE で設定されたポリシーが人間が読み取れる形式で含まれていません。

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

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

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

モニタリングログによって、モニタリング、レポート、およびトラブルシューティング機能に関する情報が提供されます。ログのダウンロードの詳細については、[Cisco ISE-PIC ログファイルのダウンロード \(43 ページ\)](#) を参照してください。

サポートバンドル

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

Cisco ISE-PIC ログファイルのダウンロード

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

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

始める前に

- デバッグログとデバッグログレベルを設定する必要があります。

ステップ 1 [管理 (Administration)] > [ロギング (Logging)] > [ログのダウンロード (Download Logs)] > [アプライアンスノードリスト (Appliance node list)] を選択します。

ステップ 2 サポートバンドルをダウンロードするノードをクリックします。

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

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

ステップ 4 サポートバンドルを生成する [開始日 (From date)] と [終了日 (To date)] を入力します。

ステップ 5 次のいずれかを実行します。

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

ステップ 6 [サポート バンドルの作成 (Create Support Bundle)] をクリックします。

ステップ 7 [ダウンロード (Download)] をクリックして、新しく作成されたサポート バンドルをダウンロードします。

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

次のタスク

特定のコンポーネントのデバッグログをダウンロードします。

Cisco ISE-PIC デバッグ ログ

デバッグ ログには、さまざまな Cisco ISE-PIC コンポーネントのトラブルシューティング情報が含まれています。デバッグログには、過去30日間に生成された重大なアラームと警告アラーム、過去7日間に生成された情報アラームが含まれています。問題を報告しているときに、これらのデバッグログを有効にして、問題の診断と解決のためにこれらのログを送信するよう求められる場合があります。



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

デバッグ ログの入手

ステップ 1 デバッグログを入手するコンポーネントを設定します。

ステップ 2 デバッグ ログをダウンロードします。

Cisco ISE-PIC コンポーネントおよび対応するデバッグログ

(注) 次のリストに、ISE で使用可能なすべてのコンポーネントを示します。この表には ISE-PIC に関連していないコンポーネントも含まれています。

表 5: コンポーネントおよび対応するデバッグ ログ

コンポーネント	デバッグ ログ
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
ライセンス	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
クライアント	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
ゲスト アクセス管理	guest.log
ゲスト アクセス	guest.log
MyDevices	guest.log

コンポーネント	デバッグ ログ
ポータル (Portal)	guest.log
ポータル セッション マネージャ	guest.log
ポータル Web アクション	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mmt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
ポスチャ	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

デバッグ ログのダウンロード

ステップ 1 [管理 (Administration)] > [ロギング (Logging)] > [ログのダウンロード (Download Logs)] を選択します。

ステップ 2 [アプライアンスノードリスト (Appliance node list)] で、デバッグログをダウンロードするノードをクリックします。

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

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

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

必要に応じて、このプロセスを繰り返して他のログファイルをダウンロードできます。次に、[デバッグ ログ (Debug Logs)] ウィンドウからダウンロードできるその他のデバッグログを示します。

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

その他の参考資料

次のリンクには、Cisco ISE で作業するときを使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#)にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

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。