Cisco Firepower NGFW におけるアイデンティティの認識と制御

目次

概要

Cisco Firepower® 次世代ファイアウォール（NGFW）は、ユーザアイデンティティをトラフィックフローに関連付けることで、ネットワークセキュリティと可視性を強化します。

Firepower Management Center（FMC）では、アイデンティティ統合の一環として次の情報が取得されます。

1. 設定したアイデンティティソースから取得されるユーザアイデンティティ情報：現行ユーザと IP アドレスのマッピング情報が FMC に提供されます。ユーザアイデンティティ情報は頻繁に更新されます。
2. Lightweight Directory Access Protocol（LDAP）を介して、または Active Directory サーバから取得されるユーザとグループ情報：レルムを設定することで、FMC のユーザデータベースに保存するユーザおよびグループデータが提供されます。レルムは、FMC と監視対象サーバ上のユーザアカウントを結び付けます。

FMC がユーザのログイン時に任意のアイデンティティソースからユーザデータを検出すると、ログインユーザが FMC のユーザデータベース内のユーザ一覧に照らし合わせて確認されます。ログインユーザが既存のユーザと一致した場合は、ログイン情報がそのユーザに割り当てられます。一致しなかった場合は、ユーザが新たに作成されます。

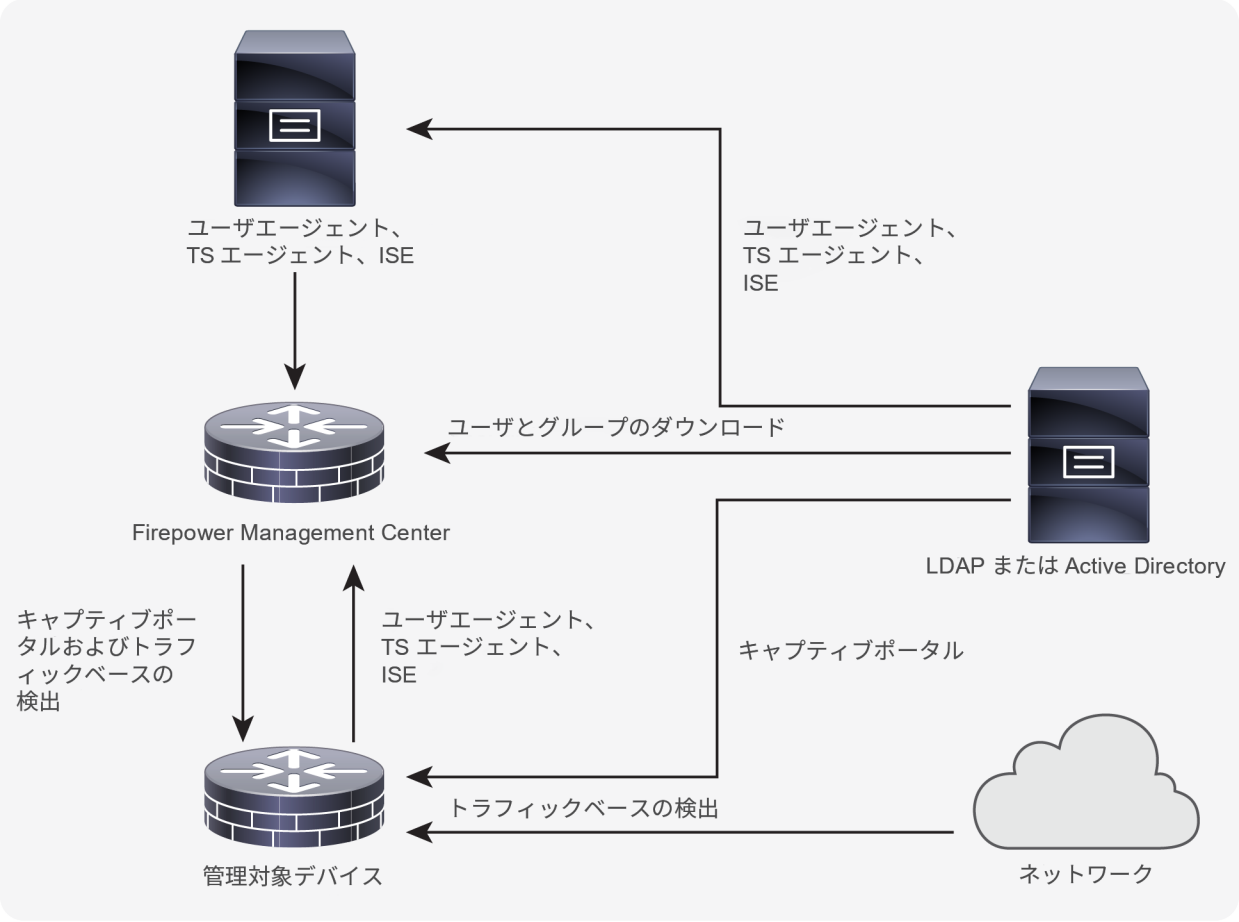

図 1.
FMC でのアイデンティティポリシー管理

Cisco Firepower は、さまざまなユーザ アイデンティティ ソースと連携して、システムを通過するネットワークトラフィックのアイデンティティを特定します。各アイデンティティソースは、ユーザ認識のためのユーザストアを備えています。また、アイデンティティとアクセス コントロール ポリシーを使用してユーザアクセスを制御できます。さまざまなアイデンティティソースの概要を次の表に示します。

表 1. FMC のユーザ アイデンティティソース

ユーザ アイデンティティ ソース	ポリシー	サーバ要件	タイプ	認証タイプ	ユーザ認識	ユーザ制御
Cisco® Identity Services Engine（ISE）/ISE Passive Identity Connector（ISE-PIC）	アイデンティティ	Microsoft Active Directory	Authoritative ログイン	パッシブ	あり	あり
キャプティブポータル	アイデンティティ	LDAP または Microsoft Active Directory	Authoritative ログイン	アクティブ	あり	あり
TS エージェント	アイデンティティ	Microsoft および Citrix ターミナルサーバ	Authoritative ログイン	パッシブ	あり	あり
Sourcefire User Agent*	アイデンティティ	Microsoft Active Directory	Authoritative ログイン	パッシブ	あり	あり
トラフィックベースの検出	ネットワーク検出	N/A	非 Authoritative ログイン	なし	あり	なし

***ISE/ISE-PIC 推奨**

上記の表から、認証タイプが 2 つあることがわかります。

1. **パッシブ認証：**パッシブアイデンティティ学習とは、セキュリティツールが Microsoft Active Directory（AD）などのサードパーティシステムからネットワーク上のユーザのユーザ名と IP アドレスをパッシブに学習する技術です。ネットワーク上のユーザアイデンティティの学習で使用される方法は、アイデンティティソースやユースケースによって異なります。上記のすべてのパッシブ アイデンティティ ソースでは、アイデンティティを取得するための追加のエンドユーザ操作は不要です。ファイアウォールによってユーザが透過的に認証されます。
2. **アクティブ認証：**ユーザは何らかの形式でやりとりを行い（キャプティブポータルなど）、事前に設定済みの管理対象デバイスを通して認証を行います。ドメインコントローラ（DC）は、ユーザの認証を実行する AD サーバコンポーネントの役割を果たします。つまり、ユーザ名とパスワードハッシュを受け取り、AD データベースに照らし合わせて検証します。

このドキュメントは、Cisco ISE を Cisco Firepower と統合して、ユーザのアイデンティティをパッシブに認識して制御するための高度なリファレンスガイドです。

Cisco ISE によるパッシブアイデンティティの概要

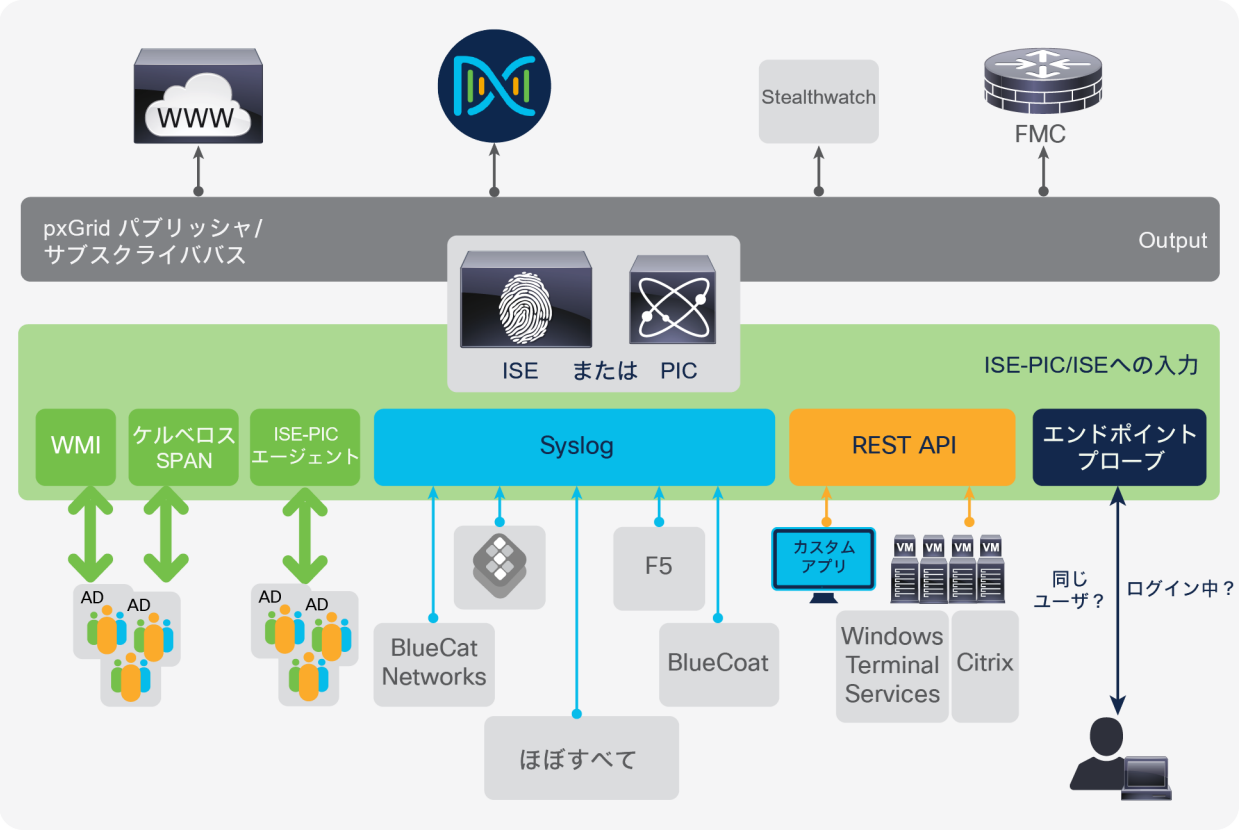

図 2.
ISE pxGrid プロバイダー/サブスクライバエコシステム

Cisco ISE または ISE-PIC（このドキュメント内では **ISE/ PIC** と総称）は、信頼できるアイデンティティソースであり、AD、LDAP、RADIUS、または RSA（Rivest-Shamir-Adleman）を使用して認証を行うユーザに関するユーザ認識データを提供します。ISE/PIC は、認証されたユーザアイデンティティを **Cisco pxGrid** サービスを介して **Cisco FMC** にパブリッシュします。ユーザアイデンティティは、さまざまなプロバイダーから収集され、Cisco ISE/PIC セッションディレクトリに保存されます。このドキュメント内のすべてのテストは、ISE バージョン 2.4 以降を使用して実施されていますが、特に明記されていない限り、ほとんどのシナリオは 2.2 以降であれば動作します。

ISE/PIC は、さまざまな理由から、パッシブアイデンティティのソースとして独自の地位を確立しています。**ISE/PIC はマルチベンダー セキュリティ エコシステムとして、**FMC、Cisco Stealthwatch®、Cisco DNA Center™、Web セキュリティアプライアンス（WSA）などのサブスクライバを Active Directory、Splunk、Infoblox などのサードパーティのアイデンティティ プロバイダー製品に接続して、アイデンティティの共有を可能にします。このサブスクライバのリストにはシスコの製品が次々と追加されています。

また、 ISE（ISE-PIC は除く）を完全に展開すると、有線およびワイヤレスネットワークから 802.1X のユーザ情報も使用できます。さらに、プロファイリングや CiscoTrustSec® と統合することで、デバイスタイプとスケーラブルグループタグ（SGT）を含めたファイアウォールポリシーを実現できます。

ISE/PIC では、認証されたユーザのセッション属性情報（ユーザ名、ドメインなど）を公開するセッションディレクトリが作成されます。次に pxGrid がこのセッションディレクトリをトピックとして FMC などのサブスクライバに

パブリッシュします。FMC がセッショントピックに登録すると、ISE/PIC は**モニタリングノード（MnT）**からセッションデータを一括してダウンロードするように FMC に対して指示します。 セッション情報の更新が検出されると、対応するセッションディレクトリが更新され、リアルタイムで FMC にパブリッシュされます。ISE-PIC が ISE 属性データを提供することも、ISE EPS 修復（エンドポイント保護サービス）をサポートすることもありません。

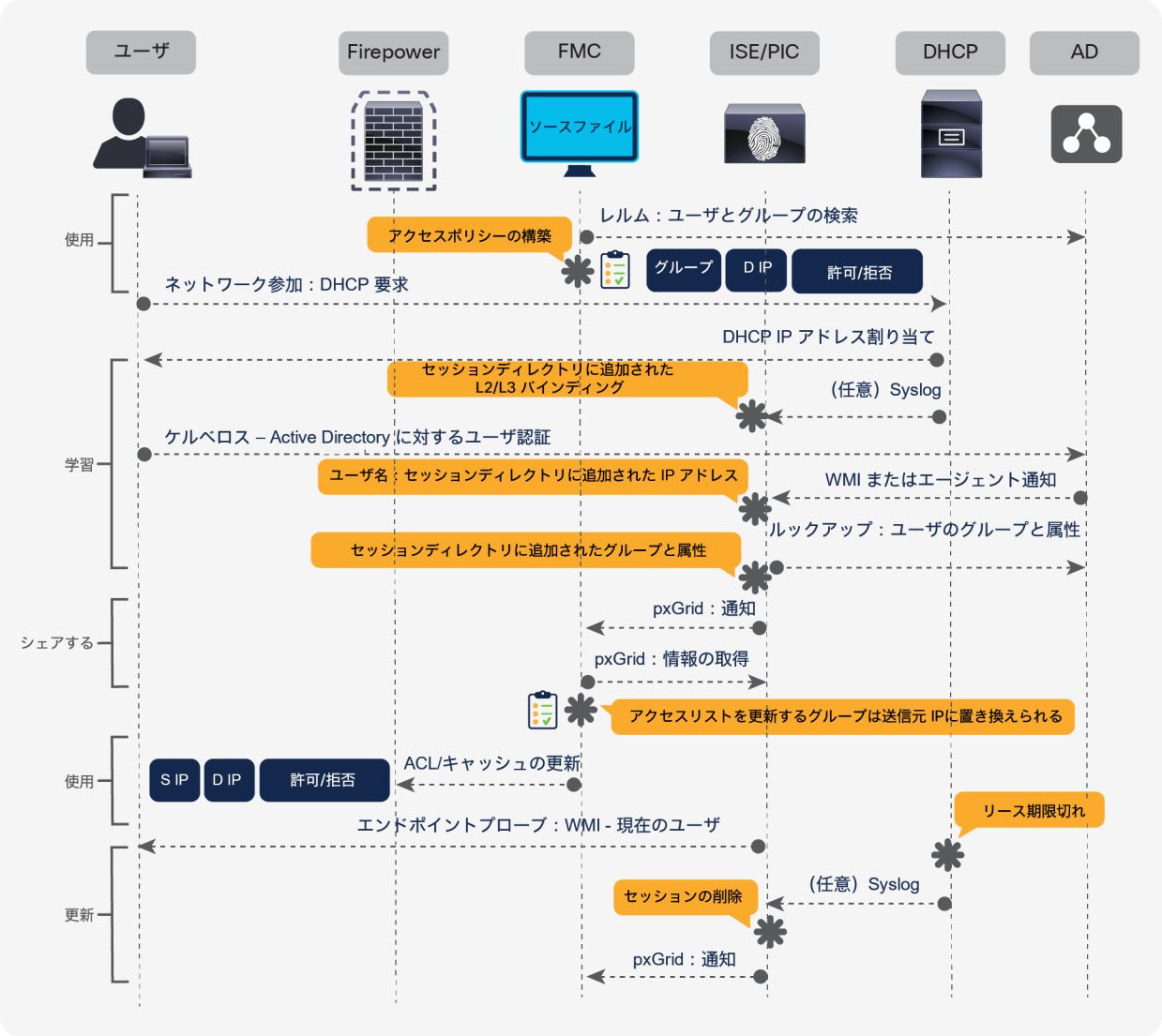

図 3.
FMC-ISE のワークフロー

次に示すように、プロバイダーとプローブにはさまざまなタイプがあります。

Active Directory（AD）

AD は、ユーザ名、IP アドレス、ドメイン名などのユーザアイデンティティ情報のソースとして最も一般的です。ISE/PIC バージョン 2.2 ～ v2.4 は、**Microsoft AD サーバ 2003 と 2003 R2（どちらも廃盤）のほかに 2008、2008 R2、2012、2012 R2、および 2016** をサポートしています。また、AD インフラストラクチャとのマルチドメインおよびマルチフォレスト統合に対応し、大規模なエンタープライズネットワーク全体を通して認証および属性の収集が可能です。また、最大 **50 の参加ポイント**をサポートしています。2 種類の AD ベースのプローブの詳細を以下で説明します。

Windows Management Instrumentation（WMI）

WMI は **Microsoft の通信メカニズム**であり、ISE/PIC がケルベロス認証チケットの生成や更新の対象となるセキュリティイベントにリモートから登録できるようにします。簡単に言うと、ISE/PIC は WMI を使用してドメインユーザのログインと更新の通知を受け取ることができるため、AD ドメインコントローラやメンバーサーバに外部エージェントをインストールする必要はありません。

ISE-PIC エージェント

ISE/PIC エージェントは、ISE/PIC 2.2 に導入された**ネイティブ Windows 32 ビットアプリケーション**であり、Active Directory ドメインコントローラまたはメンバーサーバにインストールできます。WMI の使用を好まない場合、エージェントプローブは、ユーザのアイデンティティ情報に Active Directory を使用する際の簡単で効率的なソリューションです。AD サーバへのエージェントのインストールも、ISE/PIC 管理 GUI からリモートで行えるようになったことで、大幅に簡素化されました。

SPAN

SPAN により、ISE/PIC で簡単かつ迅速にネットワークをリッスンしてユーザ情報を収集できます。このとき、Active Directory が ISE/PIC と直接連携するように設定する必要はありません。SPAN はネットワークトラフィックをモニタリングします、具体的にはケルベロスメッセージを検証して、ユーザのアイデンティティ情報（ユーザ名、IP アドレス、ドメイン名）を抽出します。

syslog

この機能により、RFC 対応の syslog メッセージを配信する任意のクライアント（アイデンティ データ プロバイダー）から受け取った syslog メッセージが解析されます。syslog メッセージには、InfoBlox、Blue Coat、BlueCat、Lucent などのプロバイダーから送られるイベント形式の syslog メッセージと DHCP syslog メッセージがあります。これらの syslog メッセージは解析され、MAC アドレスなどのユーザアイデンティティ情報が特定されます。アイデンティ情報は次にセッションディレクトリに追加されます。

API

Cisco ISE/PIC の API プロバイダー機能では、カスタマイズしたプログラムやシスコのターミナルサーバ（TS）エージェントから、組み込み ISE/PIC REST API サービスにユーザアイデンティティ情報をプッシュできます。これにより、ネットワークのプログラミング可能なクライアントをカスタマイズして、任意のネットワーク アクセス コントロール（NAC）システムから収集されたユーザアイデンティティをこのサービスに送信できます。さらに Cisco ISE/PIC API プロバイダーにより、Citrix サーバの TS エージェントをはじめとしたネットワーク アプリケーションとやりとりできます。このとき、すべてのユーザの IP アドレスは同じになりますが、各ユーザに固有のポートが割り当てられています。

パッシブ ID プロバイダーとサブスクライバの拡張マトリックス

表 2. パッシブ ID の拡張マトリックス

シナリオ	3515/3595 仮想アプライアンス
WMI または ISE AD エージェントを介してサポートされる最大 AD ドメインコントローラ数	100
最大 ISE-PIC エージェント数（エージェントと DC が 1 対 1 と想定）	100

シナリオ	3515/3595 仮想アプライアンス
エージェントあたりの推奨 DC 数（DC 上のエージェント）	1
エージェントあたりの推奨 DC 数（メンバーサーバ上のエージェント）	10
WMI（パッシブ ID サービス）に対応する推奨ポリシーサービスノード（PSN）数	2
最大 REST API プロバイダー数	50
最大 REST API EPS 数	1,000
最大 syslog プロバイダー数	70
最大 syslog EPS 数	400
インターバルごとにプローブされる最大エンドポイント数	100,000
最大 pxGrid サブスクライバ数	20
バインド（IP アドレス、MAC アドレス、ユーザ名）	300,000

表 3. FMC によるユーザ制限

Management Center モデル	最大ユーザダウンロード数
MC1600	50,000
MC2500	64,000
MC2600	64,000
MC4500	64,000
MC4600	64,000
ASA with FirePOWER Services	2,000
仮想	50,000

FMC の各 AD レルムは、1 つのドメインを指します。AD レルムの数に厳密な制限はありませんが、ダウンロードするユーザの合計数が上記の表の制限を超えないように注意してください。FMC バージョン 6.2.3 では、追加できる ISE/PIC の統合ポイントは 1 つだけです。FMC は、パッシブアイデンティティについて、Microsoft AD サーバ **2008、2008 R2、2012、2012 R2、および 2016** をすべての機能レベルでサポートしています。

次の項で説明するように、FMC と ISE/PIC を統合することで選択肢が広がります。たとえば、お客様のパッシブアイデンティティについてのニーズに応じたスケーラブルな導入が実現します。

使用するコンポーネント

- FMC および仮想 Firepower Thread Defense（FTD）バージョン 6.2.3
- シングルノード ISE-PIC バージョン 2.4
- Windows Server 2012 R2 搭載の AD ドメインコントローラおよびメンバーサーバ

前提条件

- ISE、ISE-PIC、および AD ドメイン管理の実務知識。初期設定ついては、https://www.cisco.com/c/ja_jp/support/docs/security/identity-services-engine/216120-ise-security-ecosystem-integration-guide.html の設定ガイドと ISE 統合ガイドを参照してください。
- Cisco Firepower の実務知識。詳細については、NGFW コミュニティを参照してください。
- 必要な権限を持つ AD クレデンシャル（導入シナリオによって異なります）。
- Cisco Firepower 互換性ガイドを使用して、ISE/PIC のバージョンが FMC と互換性があることを確認してください。

ISE-PIC の構成と統合

次の項では、ISE-PIC でパッシブアイデンティティを構成およびセットアップする手順について説明します。ここで紹介する UI は、ISE のパッシブ アイデンティティ ワーク センターと同じであるため、この手順はスタンドアロン型や分散型の ISE 環境でも使用できます。

ISE-PIC の Active Directory ドメインへの参加

はじめる前に

- Microsoft Active Directory サーバがネットワーク アドレス トランスレータの背後に配置されていないこと、またネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作で使用する Microsoft Active Directory アカウントが有効であり、[次回ログイン時にパスワードを変更（Change Password on Next Login）] が設定されていないことを確認します。
- ISE-PIC のエントリがドメイン ネーム サーバ（DNS）にあることを確認します。ISE-PIC からクライアントマシンの逆引き参照を適切に設定していることを確認します。
- 参加操作を実行する AD ユーザは、ドメイン管理者である必要はありませんが、次の権限が必要です。この条件は、使用するエージェントが WMI か ISE-PIC かにかかわらず適用されます。

表 4. AD アカウントの権限

参加操作	脱退操作	Cisco ISE マシンアカウント
参加操作で使用するアカウントには、次の権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがすでに存在するかどうかを確認） • ドメインに Cisco ISE 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 マシンアカウントのパスワード、SPN、dnsHostname など） 参加操作を実行するために、ドメイン管理者である必要はありません。	脱退操作で使用するアカウントには、次の権限が必要です。 • Active Directory を検索する権限（Cisco ISE マシンアカウントがすでに存在するかどうかの確認） • ドメインから Cisco ISE マシンアカウントを削除する権限 強制脱退（パスワードなしの脱退）を実行した場合、ドメインからマシンアカウントは削除されません。	Active Directory との通信に使用するために新しく作成する Cisco ISE マシンアカウントには、次の権限が必要です。 • 自分のパスワードを変更する権限 • 認証中のユーザ/マシンに対応するユーザ/マシンオブジェクトを読み取る権限 • 必要な情報（信頼ドメイン、代替 UPN サフィックスなど）を取得するために Active Directory の一部を照会する権限 • tokenGroups 属性を読み取る権限 Active Directory でマシンアカウントを事前作成できます。samAccountName の名前が Cisco ISE 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する必要があります。 複数の参加操作を実行すると、参加ごとに複数のマシンアカウントが Cisco ISE 内で保持されます。

ISE-PIC は、AD をプロバイダーとして迅速にセットアップするための段階的なウィザードを備えているため、AD ドメインへの参加プロセスは簡単です。

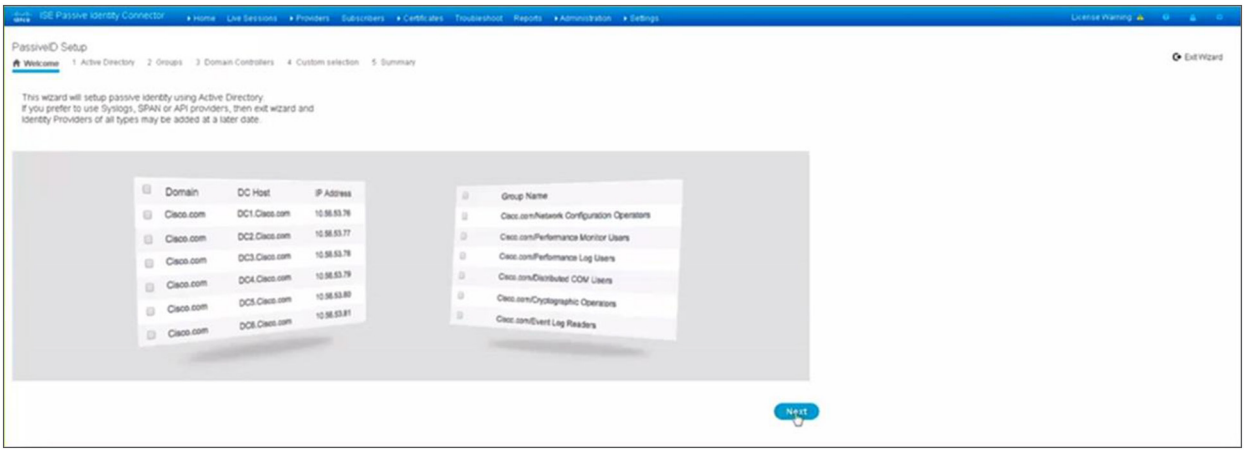

図 4.
ISE-PIC PassiveID ウィザード

このガイドでは、ISE-PIC PassiveID ウィザードは使用せず、各要素を個別に設定します。

1. [プロバイダー（Providers）] -> [Active Directory] の順に選択します。 Active Directory のランディングページが表示されます。ここで AD アイデンティティ プロバイダーを追加、編集、表示、削除できます。

図 5.
AD プロバイダー

2. [追加（Add）] をクリックします。

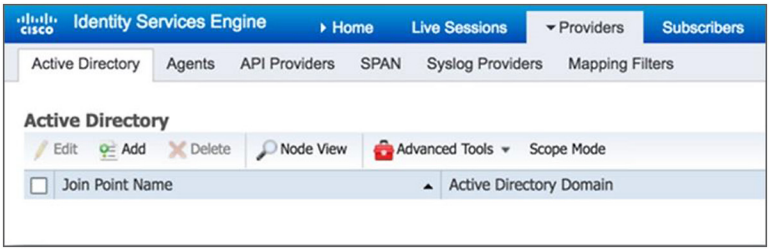

図 6.
AD 参加ポイント

3. 表示されるダイアログボックスで、設定する Active Directory 参加ポイントを素早く区別するための一意の名前を [参加ポイント名（Join Point Name）] フィールドに入力します。[Active Directory ドメイン（Active Directory Domain）] フィールドに AD のドメイン名を入力します。[送信（Submit）] をクリックします。

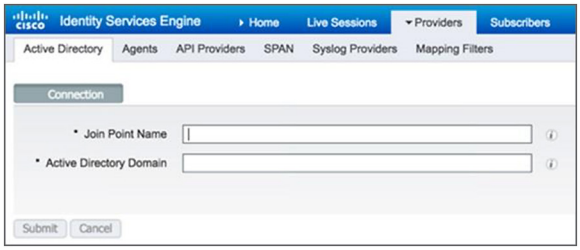

図 7.
AD 参加ポイントの設定

4. 設定した AD ドメインに ISE ノードを参加させるかを尋ねるプロンプトが表示されます。[はい（Yes）] をクリックします。

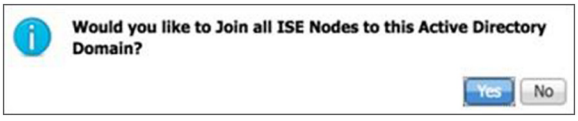

図 8.
AD 参加プロンプト

5. [ドメイン管理者（Domain Administrator）] フィールドに、前述した権限を持つドメインユーザの**ユーザプリンシパル名（UPN）**を入力します。[パスワード（Password）] フィールドには、このユーザのパスワードを入力します。これらのログイン情報はデフォルトでシステムに保存されます。これは、スタンドアロン型の ISE-PIC 環境に固有のものであり、今後何らかの変更を行う場合にもドメインのログイン情報を再入力する手間が省けます。ISE エンドポイントプローブが機能して、ユーザのログオフを検出するには、ログイン情報の保存が不可欠です。ISE（ISE-PIC は除く）では、特定のサブネットを複数の PSN にマッピングできます（特に地理的に広範囲に展開されている場合）。AD のログイン情報は、WMI が ISE に送信する AD イベントを収集する際にも使用されます。ユーザの組織ユニット（OU）が **CN=Computers,DC=someDomain,DC=someTLD** 以外の場合は、[組織ユニットの指定（Specify Organizational Unit）] フィールドにドメイン管理者の OU を入力することもできます。 [OK] をクリックします。

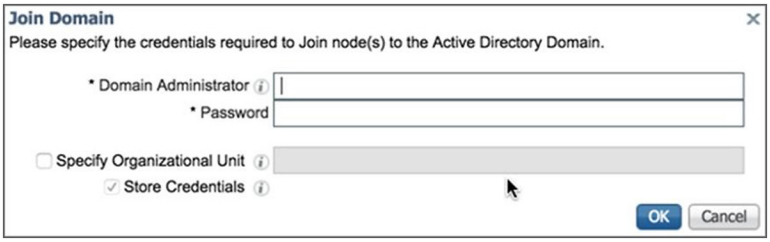

図 9.
ドメイン管理者のログイン情報

6. この時点で、ISE ノードは指定されたログイン情報を使用して AD ドメインに参加しようとします。ステータスで完了と表示されたら、[閉じる（Close）] をクリックします。
7. 使用する AD ユーザグループを設定します。作成した参加ポイントを**編集**します。[グループ（Groups）] タブをクリックします。

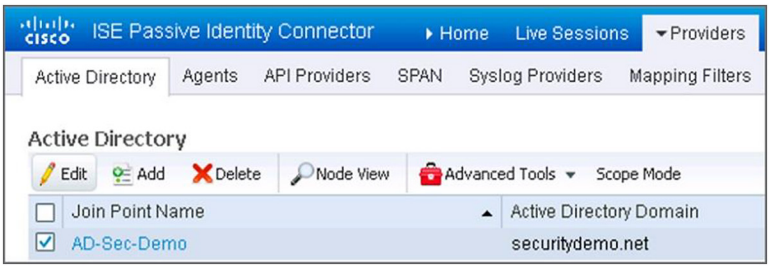

図 10.
参加ポイントの編集

8. グループは手動で追加することも、既存のグループを取得して選択することもできます。この例では、グループを取得して選択します。[グループの取得（Retrieve Groups）] をクリックすると、このドメインのユーザグループが表示されます。フィルタを使用して、グループのサブセットを取得することもできます。関連するすべてのグループを確認します。[OK] をクリックしてから、[保存（Save）] をクリックします。

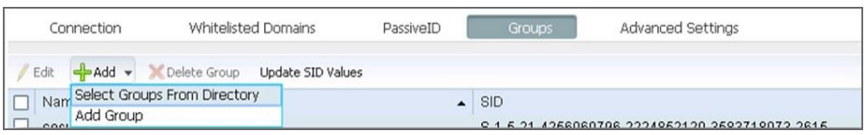

図 11.
グループをディレクトリから選択

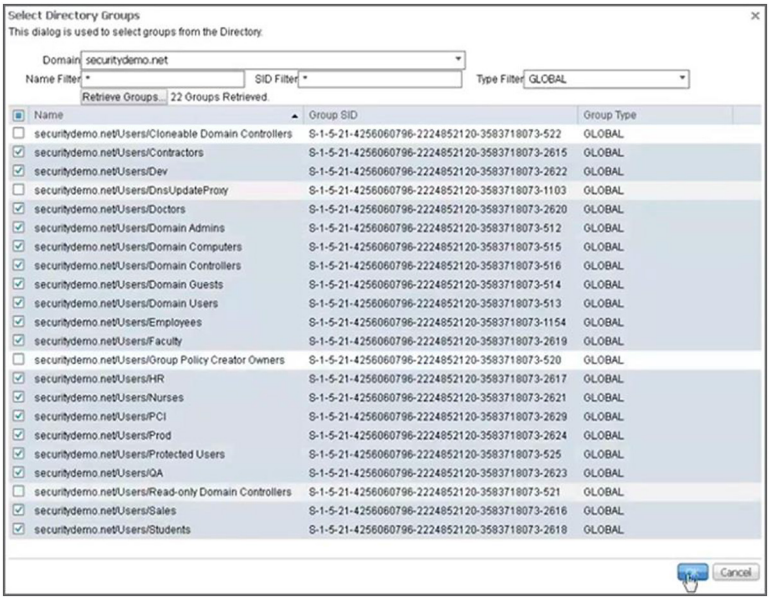

図 12.
グループをディレクトリから選択

9. 次に、監視対象の参加ポイントに追加するドメインコントローラを指定します。[プロバイダー（Providers）] -> [Active Directory] に移動して、作成した参加ポイントを編集します。

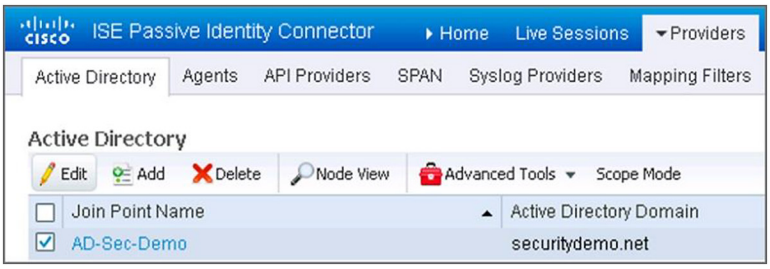

図 13.
AD 参加ポイントの編集

10. AD 参加ポイントで DC を追加したら、[プロバイダー（Providers）] -> [エンドポイントプローブ（Endpoint Probes）] の順に選択します。 エンドポイントプローブ機能は、AD 参加後に自動的に有効になり、すべてのユーザセッションで 4 時間ごとに実行されます。ユーザがまだログインしているか、またユーザの MAC アドレスと OS バージョンが確認されます。この機能を使用するには、エンドポイントでポート 445 番を有効にする必要があります。FMC サブスクライバは、ユーザがまだアクティブであるか、または切断しているかの通知を受け取ることができます。

図 14.
エンドポイントプローブ

11. **パッシブ ID の設定**を確認します。[履歴期間（History interval）] を分単位で入力すると、パッシブ ID サービスがログイン情報を再度読み取る時間間隔が定義されます。一方、[ユーザセッションのエージングタイム（User session aging time）] を指定すると、エンドポイントプローブでセッションが切断されない場合に、ユーザ ID セッションを維持する時間が定義されます。

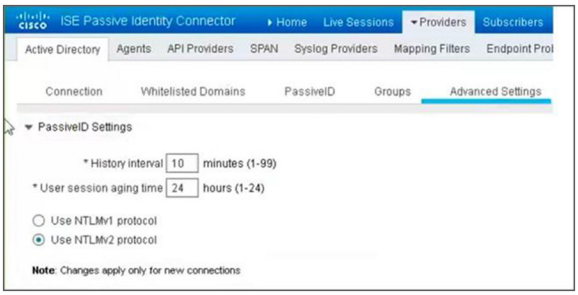

図 15.
パッシブ ID の設定

12. ISE と AD の統合を実現するための手順は他にもいくつかありますが、使用するプローブのタイプや AD ドメインのログインイベントのソースによって異なります。こうしたオプションについては、後項で説明します。

AD によるイベント転送の設定

Windows Event Forwarding（WEF）は、指定したコレクタでリモートソースからイベントを受信して保存することができる既存の Windows サービスです。イベントの集約はインシデント対応の重要な要素ですが、シスコのユースケースでは、分散型 AD 環境においてユーザと IP アドレスのマッピング情報をスケーラブルな方法で取得する上で、イベントの転送が特に重要な役割を果たします。イベント転送では、イベントコレクタである 1 つ以上のサーバがサブスクリプションマネージャとして機能する必要があります。また、サーバに送信するイベントサブスクリプションを設定する権限を管理者に付与する必要があります。イベントは **WinRM** 経由で送信されるため、ログ転送ソフトウェアを追加する必要はありません。WEF は Windows グループ ポリシー オブジェクト（GPO）を使用して簡単に設定できます。詳細については、https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/ を参照してください。

ISE-PIC と AD の統合

この項では、ISE/PIC と FMC を統合する際に可能な AD 導入オプションについて説明します。AD インフラストラクチャのサイズと使用するプローブのタイプに応じて、以下に示す方法を採用できます。通常、使用するプローブは、管理者の好みによって選択されます。

表 5.　　ISE-AD 導入サポートマトリックス

導入方式	ISE 2.4 に搭載された WMI	ISE 2.4 に搭載されたエージェント	WMI（今後のリリースで搭載予定）	エージェント（今後のリリースで搭載予定）
DC の直接監視	✓	✓	✓	✓
イベントを DC に転送して、DC で監視	✓	✓*	✓	✓
イベントを DC に転送して、メンバーサーバで監視	N/A	✓*	N/A	✓
イベントをメンバーサーバに転送して、メンバーサーバで監視	-	-	✓	✓

*CSCvj41029 のため、ISE/PIC バージョン 2.3 p5、2.4 p3 を使用します。

WMI をプローブとして使用：WMI を使用して DC を直接監視

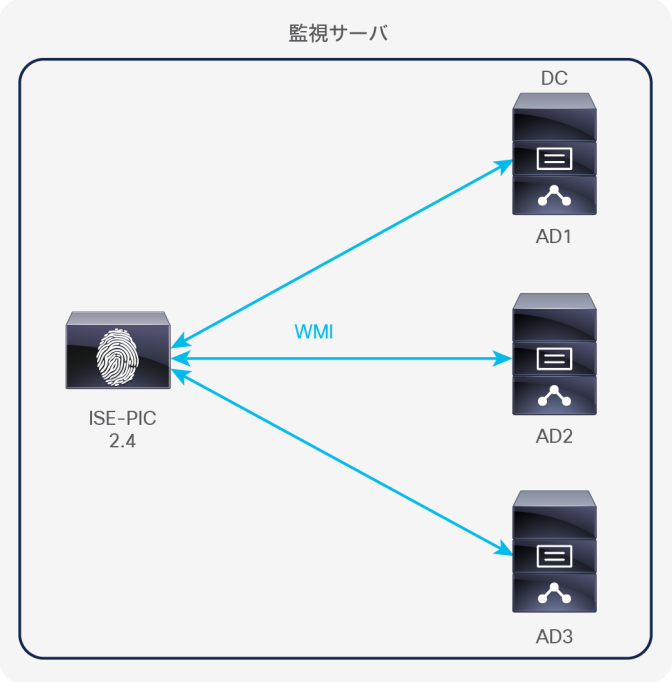

図 16.
DC の直接監視

ISE は WMI を介して DC と直接通信し、DC のセキュリティイベントに登録します。この接続方式は ISE 1.3 で導入され、AD インフラストラクチャの各 DC で WMI を設定する必要がありました。ISE 2.1 以降、WMI の設定は非常に簡単になりました。WMI の設定手順は次のとおりです。

1. 「ISE-PIC の Active Directory ドメインへの参加」のステップ 7 で作成した AD 参加ポイントを編集します。[パッシブ ID（passive ID）] タブに移動し、[DC の追加（Add DCs）] をクリックします。DC を選択して、[OK] をクリックします。

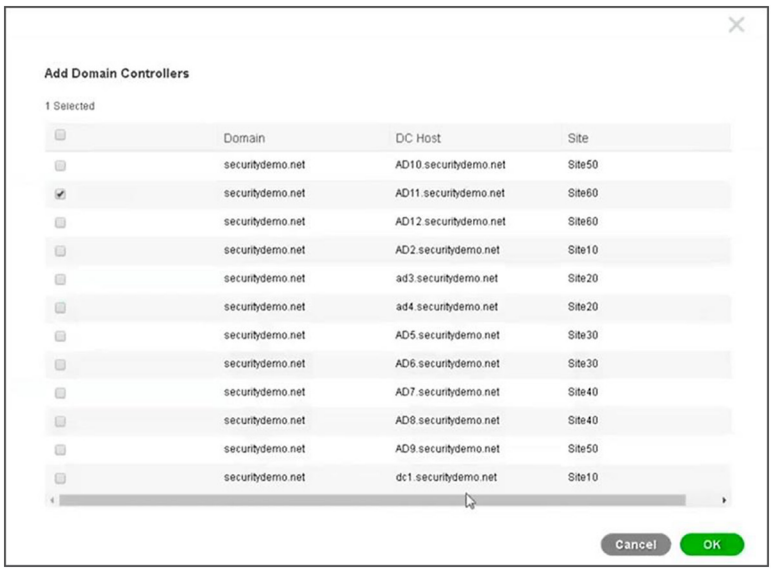

図 17.
ドメインコントローラの追加

2. 必要な DC を追加すると、[PassiveIDドメインコントローラ（PassiveID Domain Controllers）] リスト内に表示されます。追加した DC を選択して、[WMI の設定（Config WMI）] をクリックします。

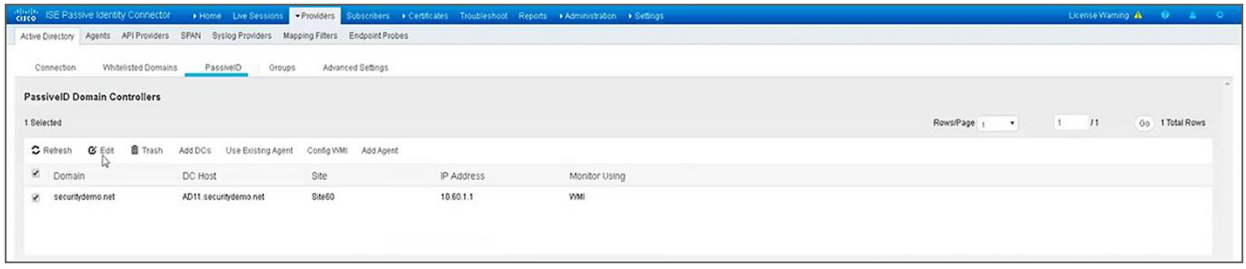

図 18.
WMI の設定

3. [WMI の設定中（Config WMI in process）] というメッセージが表示されます。

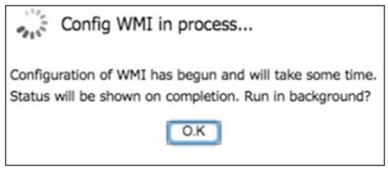

図 19.
WMI 設定中のメッセージ

このステップでは、バックグラウンドで次のアクションが実行されます。

a) ISE で使用される WMI クライアントの ID（**76A64158-CB41-11D1-8B02-00600806D9B**）を DC レジストリの 2 つの場所（**HKEY_CLASSES_ROOT\CLSID** および **HKLM\Software\Classes\Wow6432Node\CLSID**）に追加します。これにより、WMI は分散コンポーネント オブジェクト モデル（DCOM）によって有効なアプリケーションとして認識されます。

b) Windows アカウントに DCOM を使用するための権限を設定します。

c) [メソッドの実行（Execute Methods）] および [リモートの有効化（Remote Enable）] 権限を有効にして、WMI をリモートで使用する権限を設定します。

d) ユーザを**イベントログリーダー** および**分散 COM ユーザグループ**に追加して、 Windows アカウントにセキュリティイベントログの読み取りアクセス権を付与します。

e) Windows ファイアウォールの設定で、ISE との通信を許可します。

4. 設定プロセスが完了すると、成功メッセージが表示されます。

図 20.
WMI 設定成功のメッセージ

5. この時点で、ISE/PIC の [ライブセッション（Live Sessions）] 画面に移動して、登録している AD ドメインのログインイベントを表示できます。

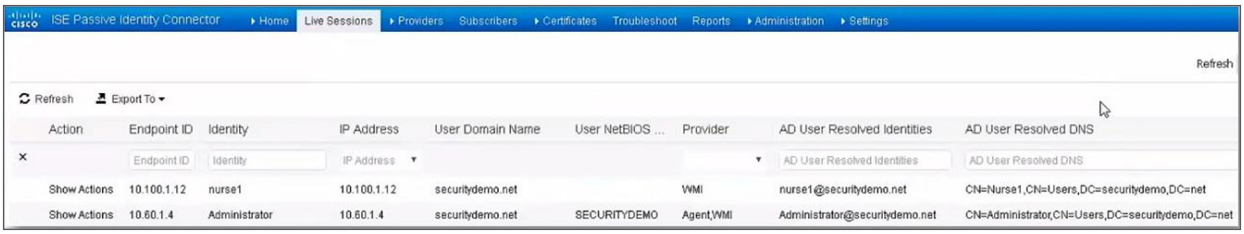

図 21.
ISE ライブログ

プローブとして WMI を使用：Windows Event Collector（WEC）として実行中の DC を監視

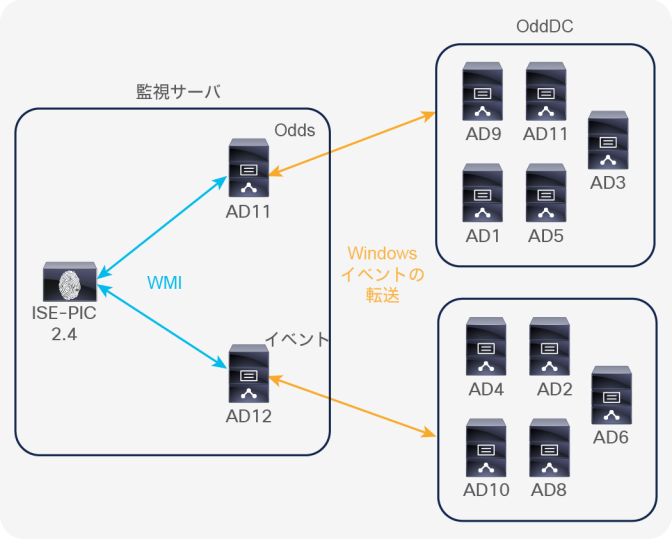

図 22.
イベントを DC に転送して、DC で監視

このシナリオでは、すべてのドメインのログオンイベントで生成されたログが、WEC として指定したドメインコントローラに転送されます。この方法では ISE/PIC バージョン 2.2 以降が必要です。AD インフラストラクチャ内のすべての DC で WMI を設定しなくても、監視を拡張できます。WMI の設定手順は次のとおりです。

1. まず最初に、選択した DC を WEC として設定します。
   a) DC で管理コマンドプロンプトを開き、**Windows Event Collector** ユーティリティを使用して WEC サービスを有効にします。有効にするためのコマンドは「wecutil qc」です。プロンプトが表示されたら、「Yes」と入力します。
   b) サーバのリモート管理を許可して、Windows ファイアウォールで必要なポートを開くには、WinRM ユーティリティを使用します。管理コマンドプロンプトで、「winrm qc」と入力します。このユーティリティは WinRM リスナーの作成時に、サービスに対するケルベルス認証用の**サービスプリンシパル名**も作成します。

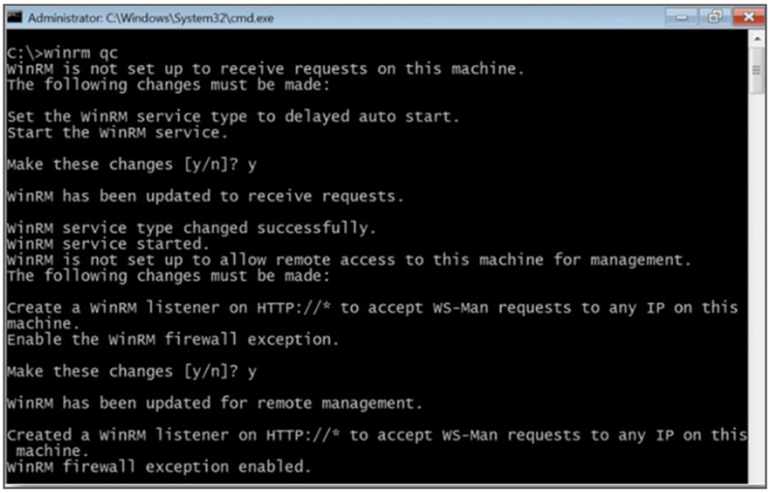

図 23.
WinRM の設定

c) [イベントビューア（Event Viewer）] に移動します。左側のペインで、[サブスクリプション（Subscriptions）] を右クリックし、[サブスクリプションの作成（Create Subscription）] を選択します。

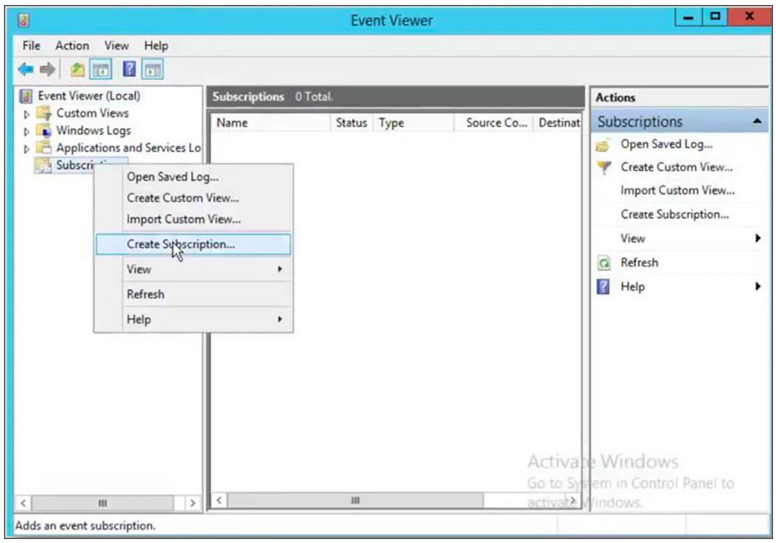

図 24.
Windows サブスクリプションの作成

d) サブスクリプション名を入力します。[ログ宛先（Destination log）] は「アプリケーション（Application）」または「システム（System）」に設定する必要があります。この例では、サブスクリプションタイプと送信元コンピュータは、[開始された送信元コンピュータ（Source computer initiated）] になっています。 [コンピュータグループの選択（Select Computer Groups）] をクリックして、コンピュータグループまたは個々の DC を追加します。[OK] をクリックします。

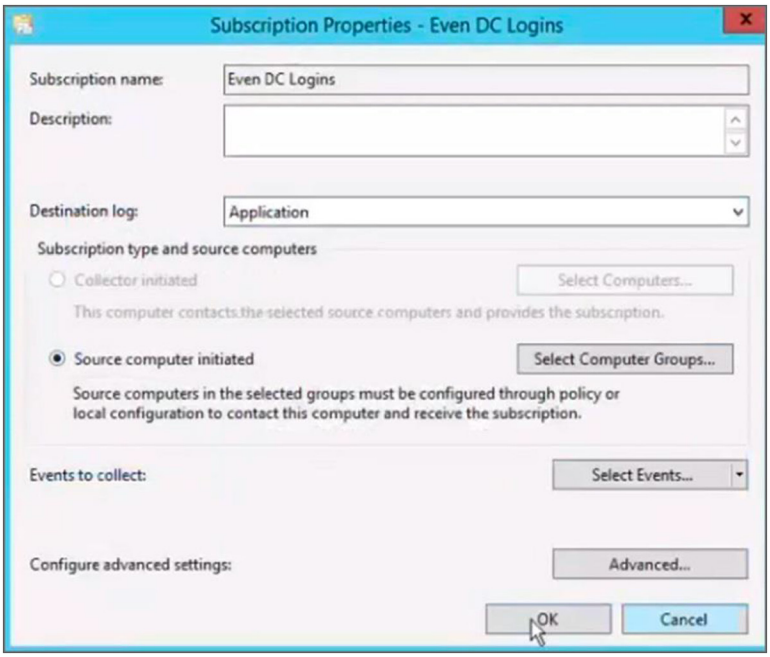

図 25.
サブスクリプション プロパティ

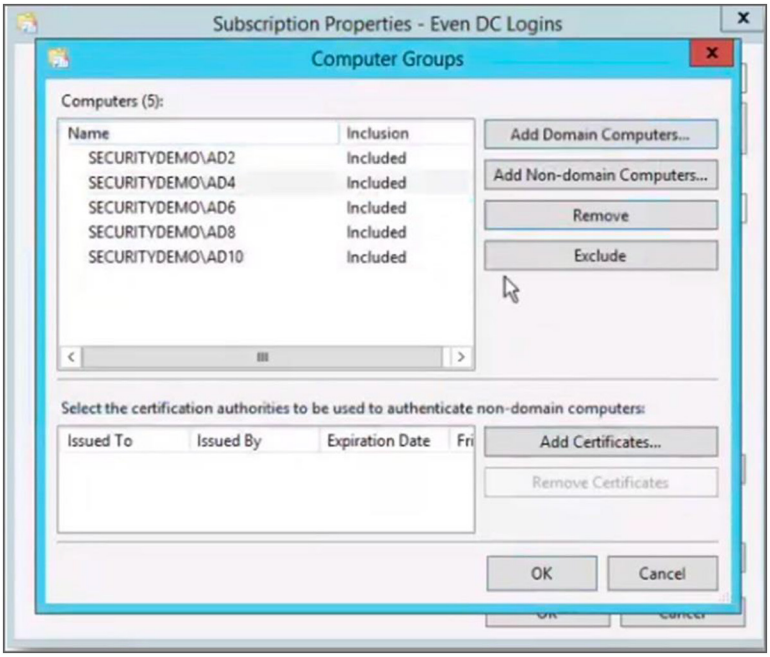

図 26.
DC をサブスクリプションに追加

e) 次に、[イベントの選択（Select Events）] をクリックして、すべてのイベントレベルを確認します。[ログ単位（By log）] のフィルタ条件を「セキュリティ（Security）」に変更します。具体的には **4624、4768、4769、**および **4770** のイベント ID でフィルタリングできます。 [OK] をクリックします。

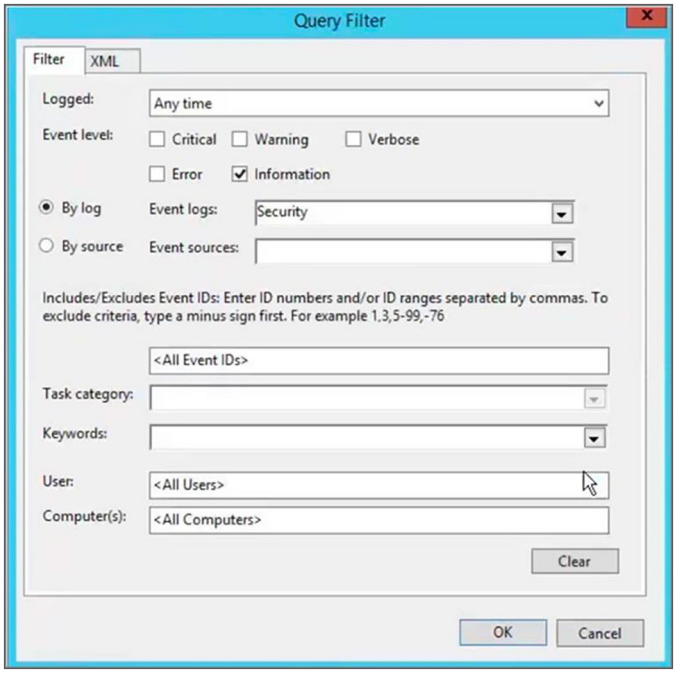

図 27.
サブスクリプション クエリ フィルタ

f) 最後に、**詳細設定**を行うため、[詳細設定（Advanced）] をクリックして、[遅延最小化（Minimize Latency）] を選択します。 [OK] をクリックしてから、もう一度 [OK] をクリックします。

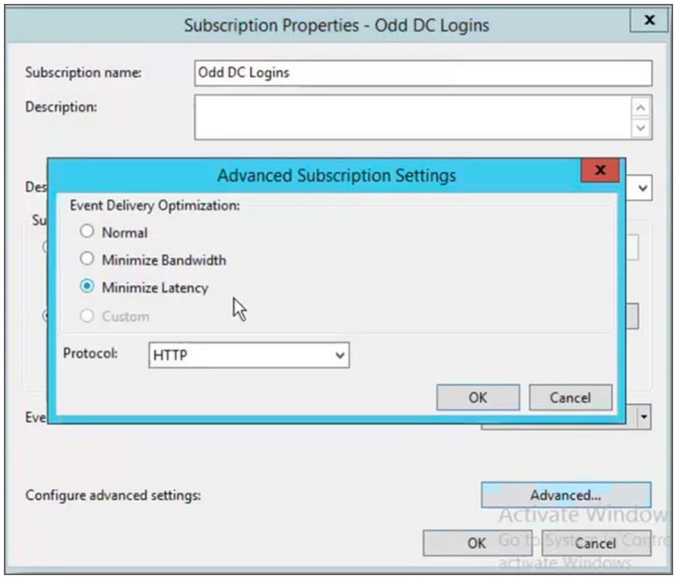

図 28.
サブスクリプションの詳細設定

g) WEC の WinRM サービスが DC のセキュリティイベントにアクセスできるようにするには、WEC の **wevtutilgl security** の出力から次の行をコピーする必要があります。これは、イベント ログ リーダー グループのサービスプリンシパルです。出力行に文字列（A;;0x1;;;NS）が含まれていない場合は、次のステップで使用するために、メモ帳などのリマインダで下記の文字列の後に付加します。この文字列によって、ネットワーク サービス アカウント（WinRMで使用）に読み取りアクセス権が追加され、セキュリティイベントログが読み取られます。

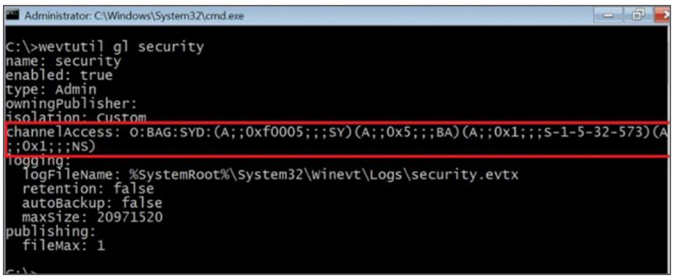

図 29.
セキュリティログにアクセスするためのセキュリティプリンシパルのコピー

2. GPO を使用して、指定した WEC にイベントを転送するように他の DC を設定します。
   a) グループ ポリシー ユーティリティを起動して、コンピュータ OU を右クリックします。[このドメインに GPO を作成してここにリンクする（Create a GPO in this domain, and link it here）] をクリックします。名前を付けて [OK] をクリックします。WEC サーバにイベントを転送する DC すべてにこの GPO を割り当てます。

b) 新しく作成した GPO を編集してから、[コンピュータ（Computer）] -> [ポリシー（Policies）] -> [管理テンプレート（Admin Templates）] -> [Windows コンポーネント（Windows Components）] -> [イベント転送（Event Forwarding）] -> [ターゲットサブスクリプションマネージャの設定（Configure target subscription manager）] に移動して、ターゲット サブスクリプション マネージャを変更します。次に [サーバアドレス（Server Address）] フィールドに「**Server=http://<fqdnofsubscriptionserver>:5985/wsman/SubscriptionManager/WEC**」と入力します。

c) サブスクリプションマネージャによるセキュリティ イベント アクセスを許可します。ステップ 1 の g）でコピーした文字列がここで役立ちます。[コンピュータ（Computer）] -> [ポリシー（Policies）] -> [管理テンプレート（Admin Templates）] -> [Windows コンポーネント（Windows Components）] -> [イベントログサービス（Event Log Service）] -> [セキュリティ（Security）] -> [ログアクセスの設定（Configure log access）] に移動して、コピーした O:BAG:SYD 行を貼り付けます。

d) GPO は次のようになります。

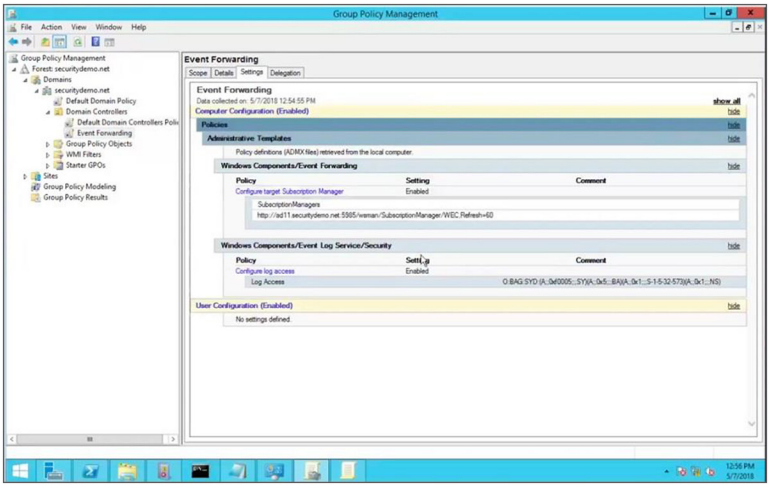

図 30.
GPO の設定

e) すべての DC でグループポリシーが更新されると、WEC で指定した宛先（**アプリケーションまたはシステム**）でドメインログインイベントが表示されるようになります。

3. ISE/PICでは、WEC で WMI を設定する必要があります。WMI の設定は、「WMI をプローブとして使用：WMI を使用して DC を直接監視」の手順に従います。

ISE-PIC エージェント：エージェントを使用して DC を直接監視

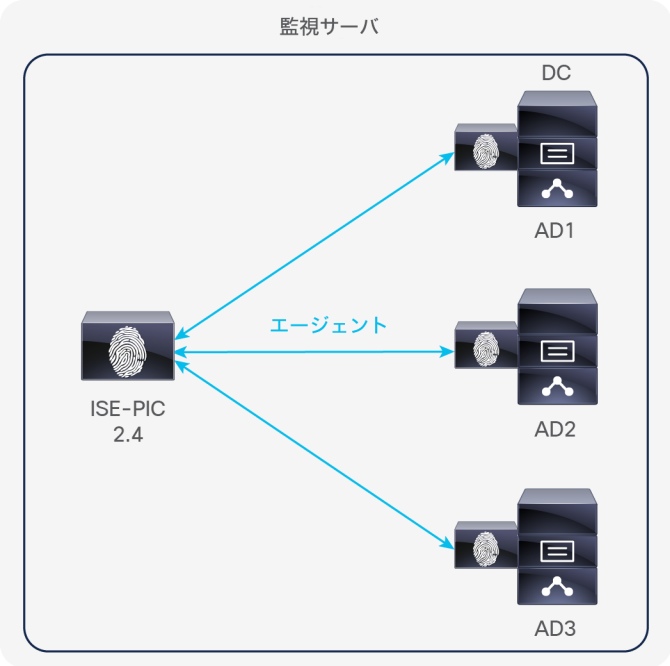

図 31.
DC を直接監視

ドメインのログオンイベントはすべてドメインコントローラに転送されます。ISE-PIC エージェントは、リモートまたはローカルでドメインコントローラ自体にインストールされ、ログオンイベントを監視して ISE/PIC ノードに結果を返します。この手順は次のとおりです。

1. 「ISE-PIC の Active Directory ドメインへの参加」のステップ 7 で作成した AD 参加ポイントを編集します。[パッシブ ID（passive ID）] タブに移動し、[DC の追加（Add DCs）] をクリックします。 DC を選択して、[OK] をクリックします。

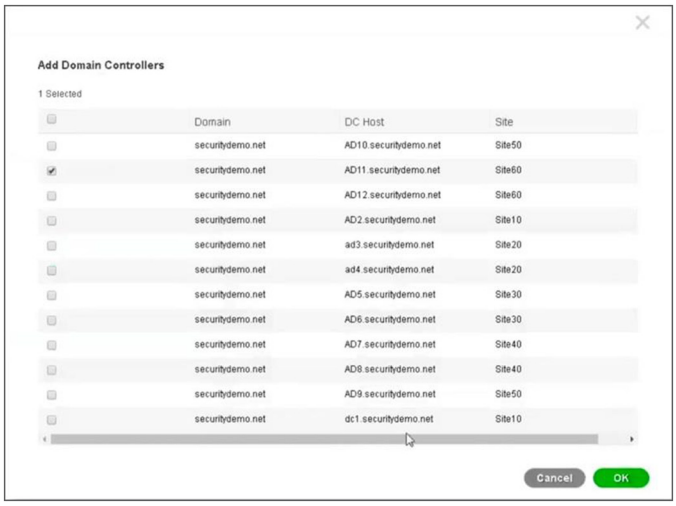

図 32.
ドメインコントローラの追加

2. 必要な DC を追加すると、[PassiveIDドメインコントローラ（Passive ID Domain Controllers）] リスト内に表示されます。監視する必要がある DC を選択して、[エージェントの追加（Add Agent）] をクリックします。
3. エージェントのポップアップで、エージェント名、エージェントをインストールするホストの完全修飾ドメイン名（FQDN）、およびエージェントのインストールに必要な権限を持つアカウントのユーザ名とパスワード（ドメイン管理者が望ましい）を入力します。[導入（Deploy）] をクリックします。

図 33.
エージェントの設定と導入

4. エージェントが導入されると、ISE/ PIC はサーバにログインして、エージェントの MSI（Microsoft Installer）ファイルをコピーおよびインストールします。このとき手動による操作は必要ありません。正常にインストールされると、インストール済みプログラムの一覧にエージェントが表示されます。

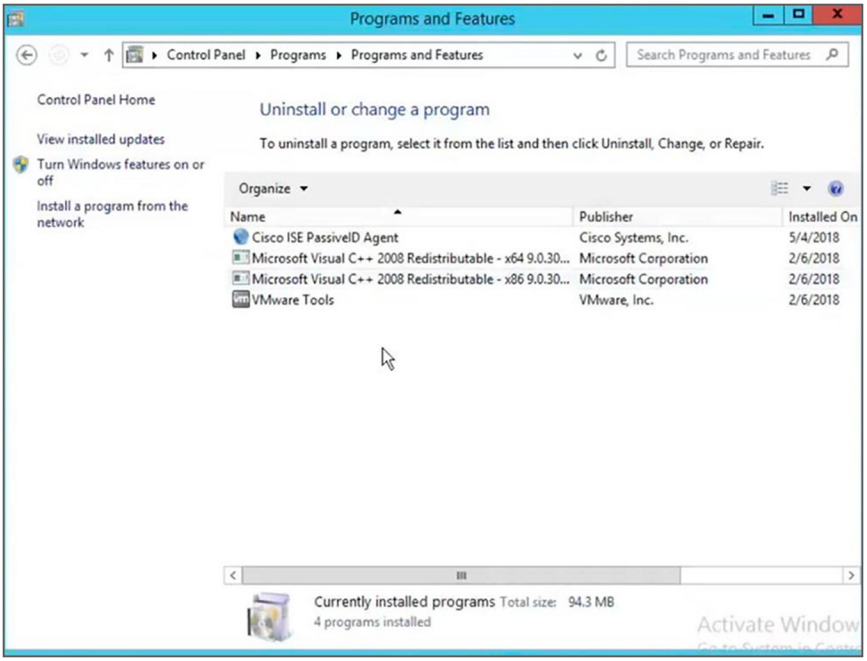

図 34.
ISE/PIC エージェントのインストール

5. ISE-PIC エージェントのローカル設定とログファイルは、Program Files/Cisco/Cisco ISE PassiveID Agent でも確認できます。

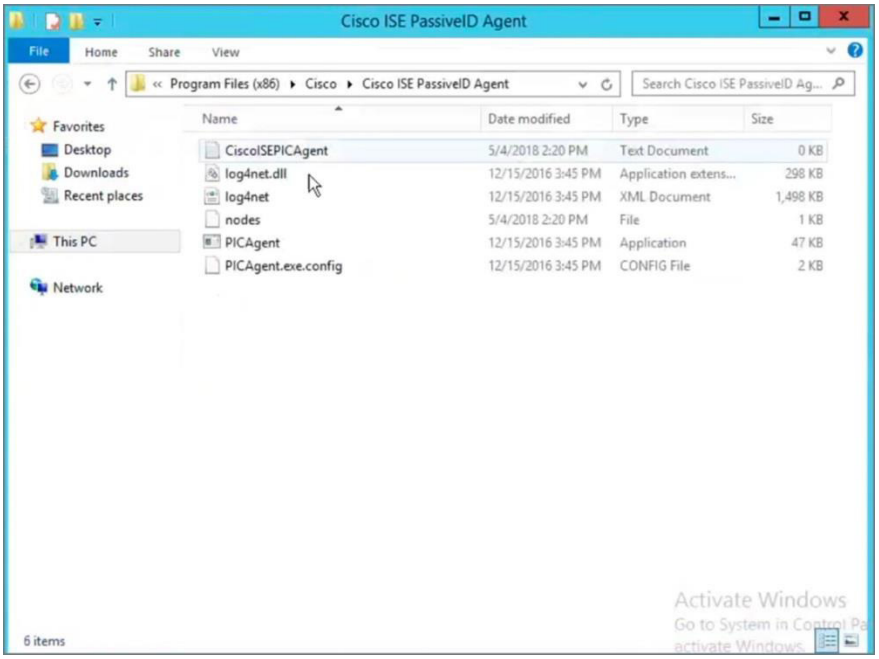

図 35.
ISE/PIC エージェントの設定とログファイルの場所

6. この時点で、エージェントが設定済みで、DC 上で実行されている場合は、ISE/PIC の [ライブセッション（Live Sessions）] 画面に移動して、登録している AD ドメインのログオンイベントを表示できます。

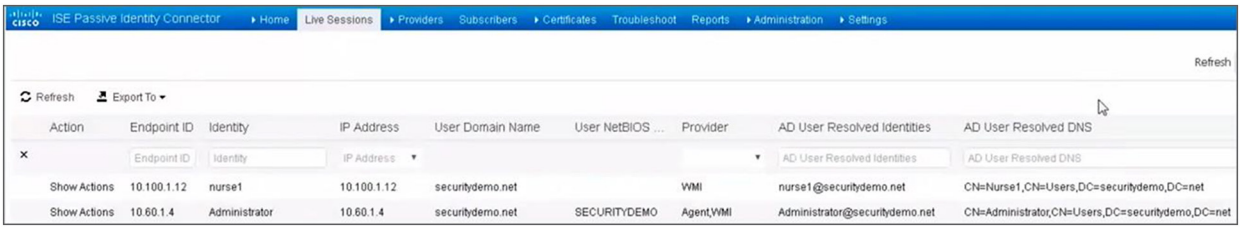

図 36.
ISE ライブログ

ISE-PIC エージェント：DC にインストールされ、Windows Event Collector（WEC）として実行中の DC を監視するエージェント

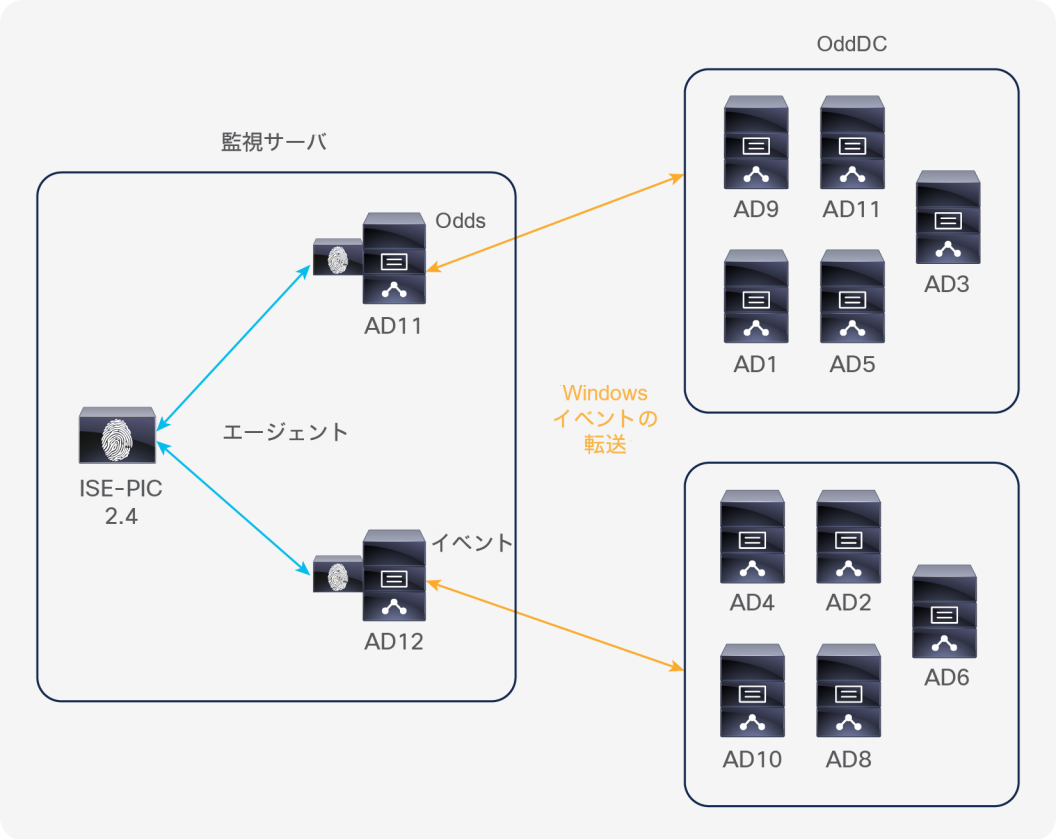

図 37.
イベントを DC に転送して、DC で監視

このシナリオでは、すべてのドメインのログオンイベントで生成されたログが、WEC として指定したドメインコントローラに転送されます。ISE-PIC エージェントは同じ DC にインストールされ、これらのイベントを監視して ISE ノードに結果を返します。この手順は次のとおりです。

1. 「プローブとして WMI を使用：Windows Event Collector（WEC）として実行中の DC を監視」のステップ 1 と 2 に従って、指定した DC への Windows イベント転送を設定します。
2. ISE/PIC サーバで、指定の DC にエージェントをインストールしてから、「ISE-PIC エージェント：エージェントを使用して DC を直接監視」のステップ 1 ～ 4 に従って同じ DC を監視します。
3. この時点でエージェントが設定済みで、DC 上で実行されている場合は、ISE/PIC の [ライブセッション（Live Sessions）] 画面に移動して、登録している AD ドメインのログオンイベントを表示できます。

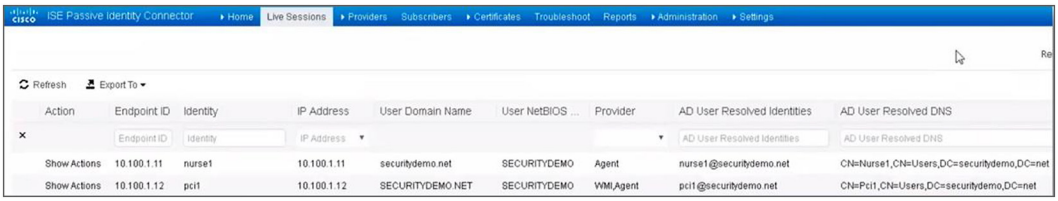

図 38.
ISE ライブログ

ISE-PIC エージェント：メンバーサーバにインストールされ、Windows Event Collector（WEC）として実行中の DC を監視するエージェント

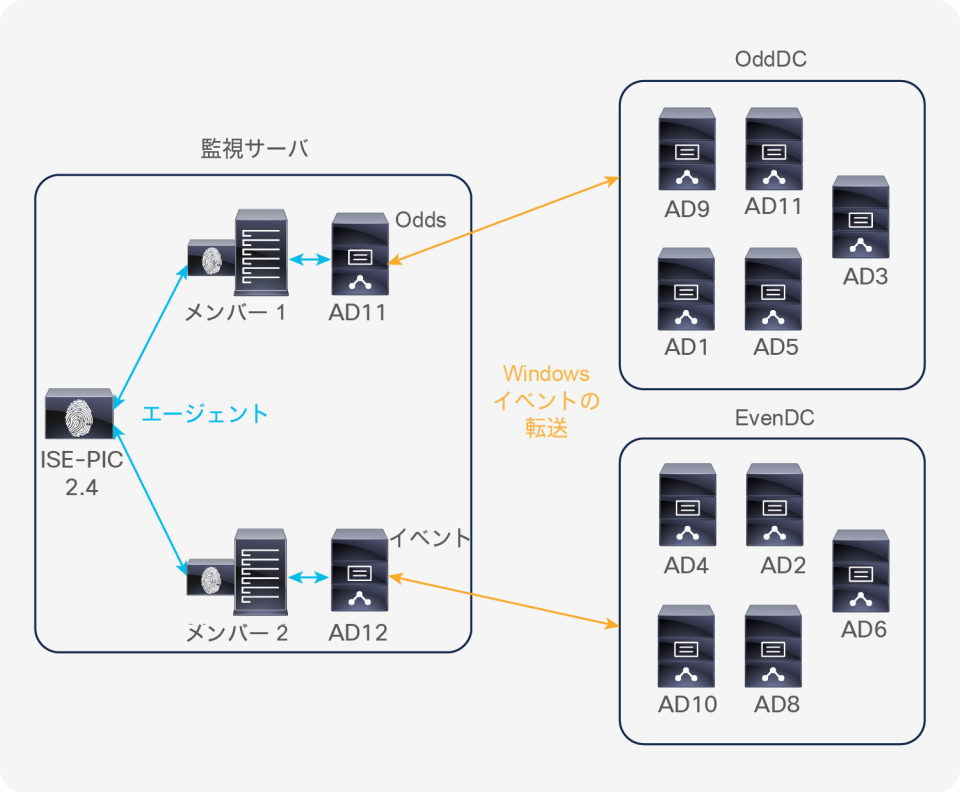

図 39.
イベントを DC に転送して、メンバーサーバで監視

ドメインのログオンイベントはすべて WEC として指定したドメインコントローラに転送されます。ISE-PIC エージェントは、メンバーサーバに自動または手動でインストールされ、WEC のイベントを監視して ISE ノードに結果を返します。これにより、DC 自体にエージェントをインストールしなくてもイベントを監視できます。この手順は次のとおりです。

1. 「プローブとして WMI を使用：Windows Event Collector（WEC）として実行中の DC を監視」のステップ 1 と 2 に従って、指定した DC への Windows イベント転送を設定します。
2. ISE/PIC サーバで、メンバーサーバにエージェントをインストールしてから、「ISE-PIC エージェント：エージェントを使用して DC を直接監視」のステップ 1 ～ 4 に従って WEC DC を監視します。
3. この時点でエージェントが設定済みで、メンバーサーバ上で実行されている場合は、ISE/PIC の [ライブセッション（Live Sessions）] 画面に移動して、登録している AD ドメインのログオンイベントを表示できます。

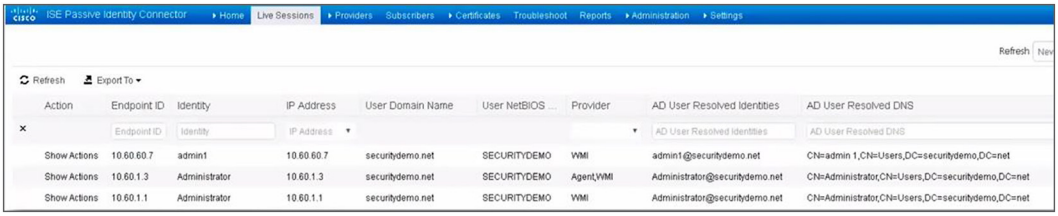

図 40.
ISE ライブログ

FMC の設定と統合

次の項では、ISE/PIC からユーザと IP アドレスのマッピング情報をダウンロードし、Active Directory サーバからユーザやユーザグループのデータベースをダウンロードするように FMC を設定します。FMC では上記の一連の情報が統合されます。これにより、NGFW でユーザベースのアクセス制御の適用が実現します。

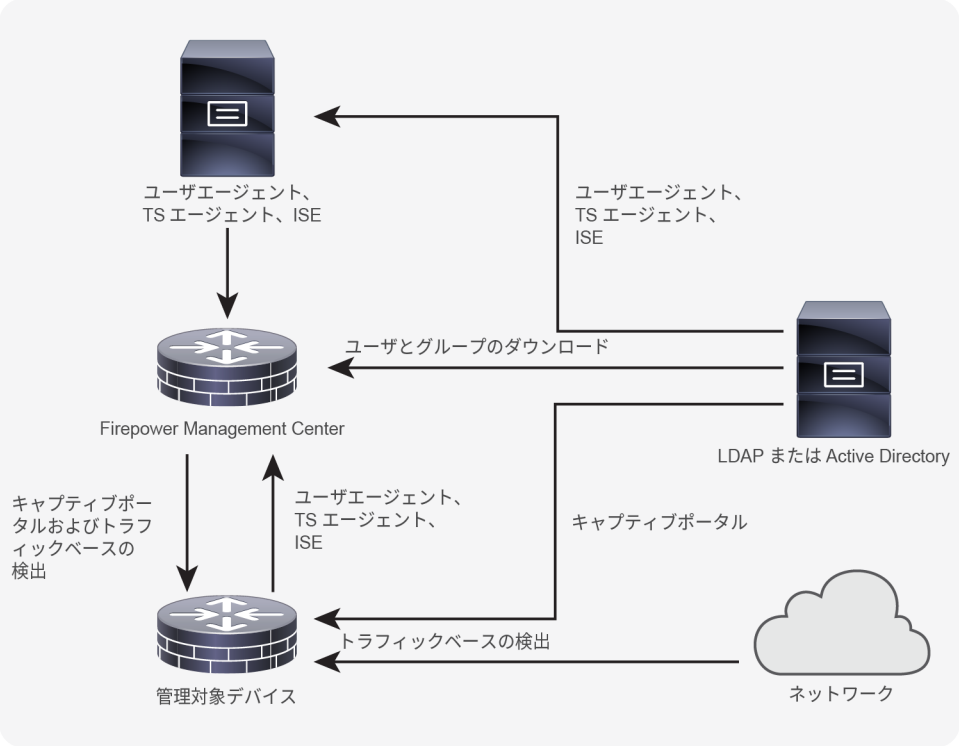

図 41.
AD および ISE との FMC 通信

Firepower 用語である AD レルム は、FMC と AD サーバ間の接続状況を示すために使用されます。FMC では、ユーザセッション情報がデフォルトで 24 時間保存されます。この値は、以下で作成するレルムを編集することで変更できます。FMC では、ユーザごとに次の情報とメタデータが取得されます。

- LDAP ユーザ名
- 姓名
- 電子メールアドレス
- 部門
- 電話番号

アクセス制御ポリシーに保存して使用できるユーザの最大数は、FMC モデルによって異なります。

FMC は pxGrid を介して ISE/PIC と連携し、ユーザセッションから TrustSec 情報に至るまで、豊富な情報を提供します。SGT タグを含むこれらの属性は、ユーザトラフィックにポリシーを適用する際に非常に役立ちます。このドキュメントを作成した時点では、送信元ベースの SGT が FMC アクセスポリシーでサポートされています。 pxGrid

は、シスコの優れたパブリッシュ/サブスクライブ通信バスであり、スケーラブルでセキュアなデータ共有システムとしてゼロから設計されました。

はじめる前に

- 予期しないユーザタイムアウトを回避するためには、FMC と ISE/PIC サーバの時刻を同期させる必要があります。
- FMC のさまざまなアイデンティティサービスに必要なポートを次の表に示します。

サービス	開放が必要なポート
AD レルム	TCP 389 アウトバウンド：非暗号化 TCP 636 アウトバウンド：暗号化 カスタマイズ可能
ISE/PIC	TCP 5222 アウトバウンド：pxGrid 通信 TCP 8910 アウトバウンド：pxGrid 一括ダウンロード

AD レルムの設定

1. FMC で [システム（System）] -> [統合（Integration）] -> [レルム（Realm）] の順に選択します。
2. 新しいレルムを作成するには、[新しいレルム（New Realm）] をクリックします。
3. [新しいレルムの追加（Add New Realm）] ポップアップで、次のガイドラインに従ってフィールドに入力します。
   a) [名前（Name）] と [説明（Description）] を入力し、[タイプ（Type）] を「AD」に設定します。
   b) [AD プライマリドメイン（AD Primary Domain）] には一意のドメインを入力します。
   c) [AD 参加ユーザ名（AD Join username）] と [パスワード（password）] は、AD レルムに参加する際に使用されます。AD ドメインにドメイン コンピュータ アカウントを作成するのに十分な権限が必要です。ユーザ名は完全修飾名にする必要があります。
   d) [ディレクトリユーザ名（Directory username）] と [パスワード（password）] には、関連するユーザとユーザグループを読み取るのに十分な権限を持つユーザアカウントのログイン情報を入力します。ユーザ名は完全修飾名にする必要があります。ここでは、前述の手順と同じログイン情報を使用できます。
   e) [ベース DN（Base DN）] は、FMC がユーザデータの検索を開始するサーバ上のディレクトリツリーです。
   f) [グループ DN（Group DN）] は、FMC がグループデータの検索を開始するサーバ上のディレクトリツリーです。
   g) 「メンバー（Member）」や「一意のメンバー（Unique Member）」などのグループ属性も指定できます。

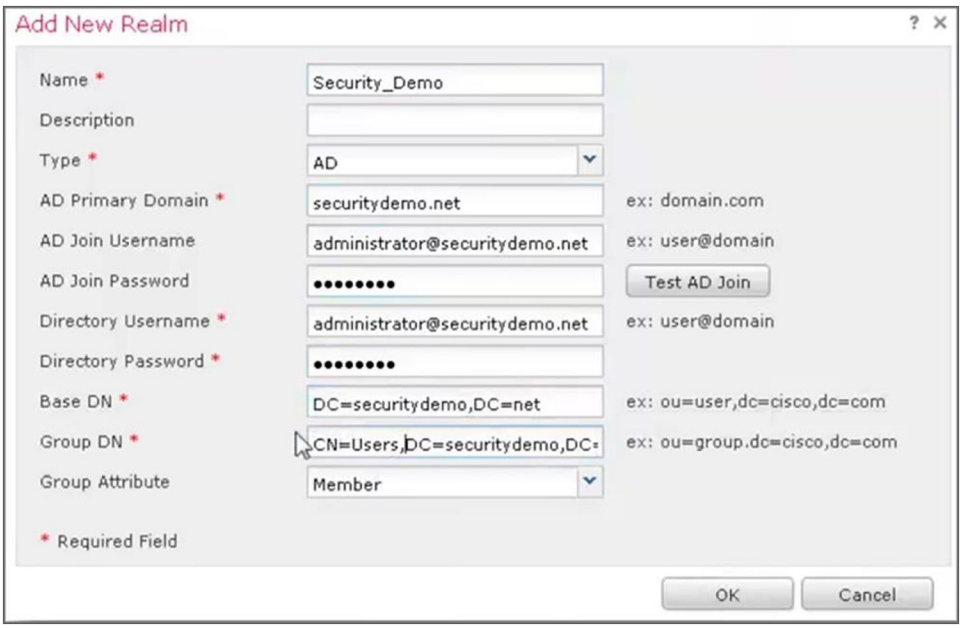

図 42.
新しい AD レルムの追加

4. [OK] をクリックします。
5. この時点で、AD ディレクトリ設定ページにリダイレクトされます。[ディレクトリの追加（Add directory）] をクリックします。
6. 次のフィールドに詳細情報を入力します。
   a) [ホスト名/IPアドレス（Hostname/IP Address）] フィールドには、Active Directory ドメインコントローラのホスト名または IP アドレスを入力します。暗号化方式を指定する場合は、このフィールドでホスト名を指定する必要があります。

   b) FMC と DC 間の接続に使用するポートを変更できます。暗号化されない接続の場合は、デフォルトで 389 に設定されます。

   c) FMC と DC 間の接続の暗号化プロトコルは、「STARTTLS」 または「LDAPS」に設定できます。暗号化しない場合は、「NONE」に設定します。

   d) 暗号化を使用する場合は、DC の SSL（セキュア ソケット レイヤ）証明書も指定できます。

   e) 接続をテストするには、[テスト（Test）] をクリックします。FMC は LDAP クエリをサーバに送信しようとします。これが成功すると、テストは成功です。

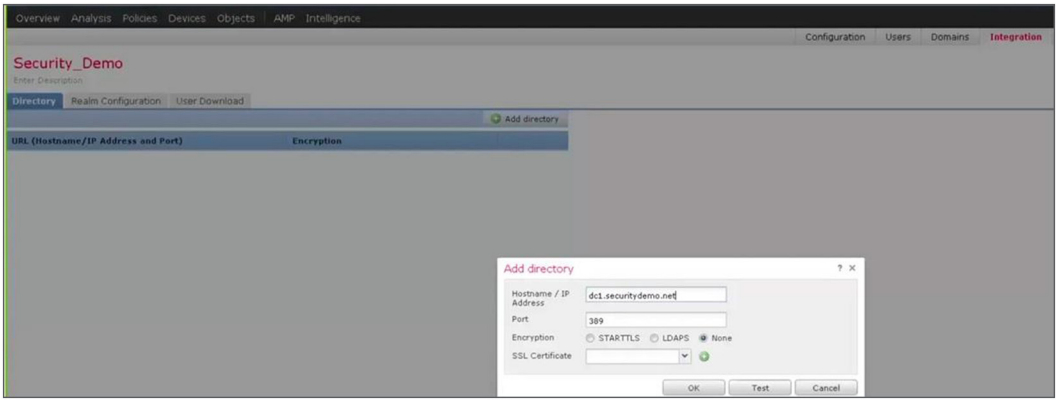

図 43.
DC の追加

7. [OK] をクリックします。
8. [保存（Save）] をクリックします。レルムタブページに戻ります。このページで、状態トグルをスライドしてレルムを有効にします。これにより、AD の参加およびユーザやユーザグループのダウンロードが可能になります。
9. レルムを編集し、[ユーザのダウンロード（User Download）] に移動します。 ここで、FMC によって AD ドメインからすべてのユーザとグループが自動的にダウンロードされたことを確認できます。ダウンロードの対象にするユーザとグループは指定できます。FMC のパフォーマンスを向上させるには、該当するユーザとグループをフィルタリングすることをお勧めします。

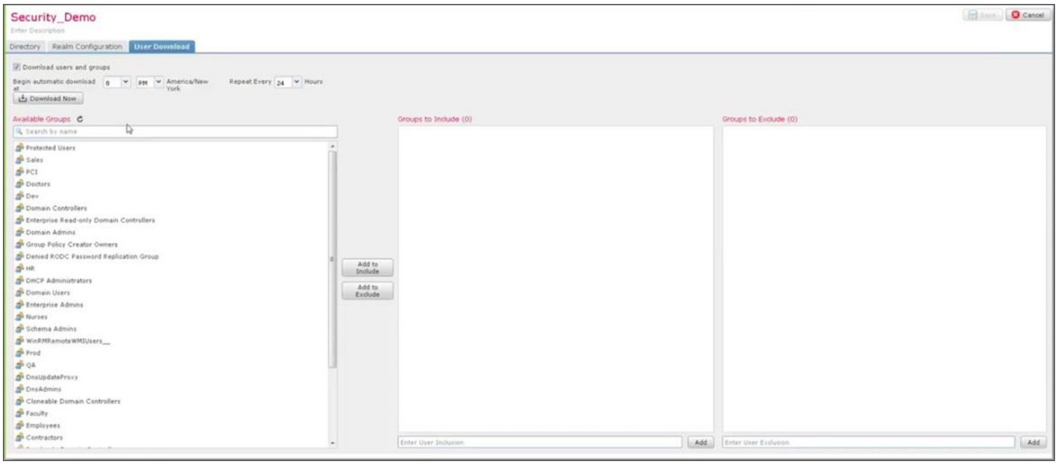

図 44.
AD ユーザとグループのフィルタリング

10. ダウンロードの開始時刻や間隔はカスタマイズできます。
11. [保存（Save）] をクリックします。

ISE を ID ソースとして設定

1. FMC が pxGrid を介して ISE/PIC と安全に通信できるようにする必要があります。そのためには、証明書の信頼関係を確立する必要があります。FMC 証明書の認証局（CA）として ISE/PIC を使用することで、簡単にこれを実行できます。
2. ISE/PIC で、[サブスクライバ（Subscribers）] -> [証明書（Certificates）] に移動して、次のフィールドに入力します。
   a) [処理の選択（I want to）] ドロップダウンで、[単一の証明書の生成（証明書署名要求なし）（Generate a single certificate (without a certificate signing request)）] オプションを選択します。
   b) FMC の証明書に割り当てる [共通名（CN）（Common Name (CN)）] を入力します。任意で説明を追加できます。FMC 用に生成された他の証明書と混同されるのを避けるために、CN の先頭に **pxgrid-** を付けることができます。
   c) 証明書のベースとなる pxGrid 証明書テンプレートを表示および編集できます。FMC 証明書には、**clientAuth** 拡張キーの使用値を含める必要があります。そうでない場合、他の拡張キーの使用値を含めることはできません。
   d) CN に FMC の FQDN が含まれていない場合、証明書に追加する [サブジェクト代替名（SAN）（Subject Alternative Name (SAN)）] を任意で指定できます。
   e) [証明書のダウンロード形式（Certificate Download Format）] ドロップダウンリストで、[Privacy Enhanced Electronic Mail（PEM）形式の証明書、PKSCB PEM 形式のキー（証明書チェーンを含む）（Certificate in Privacy Enhanced Electronic Mail (PEM) format, and key in the PKCS8 PEM format (including certificate chain)）] を選択します。
   f) 秘密キーの暗号化パスワードを入力します。
   g) [作成（Create）] をクリックします。

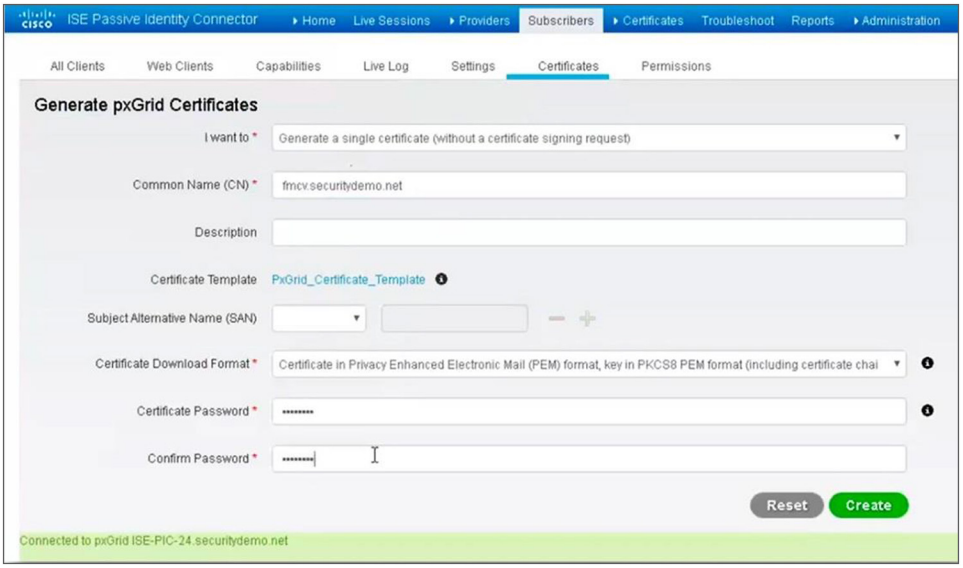

図 45.
FMC pxGrid 証明書の生成

3. 証明書バンドルの zip ファイルをダウンロードするためのポップアップが表示されます。このバンドルを保存して展開します。FMC に対して生成された証明書やキーと一緒に、ISE サービスで使用されるルート CA とサブ CA（認証局）の証明書を確認できます。

図 46.
証明書バンドルの内容

4. [サブスクライバ（Subscribers）] -> [設定（Settings）] の順に選択します。 [pxGrid 設定（pxGrid Settings）] で [新しい証明書ベースのアカウントを自動的に承認する（Automatically approve new certificate-based accounts）] のチェックボックスをオンにします。これにより、ISE/PIC サーバは FMC からの着信接続を自動的に承認できます。

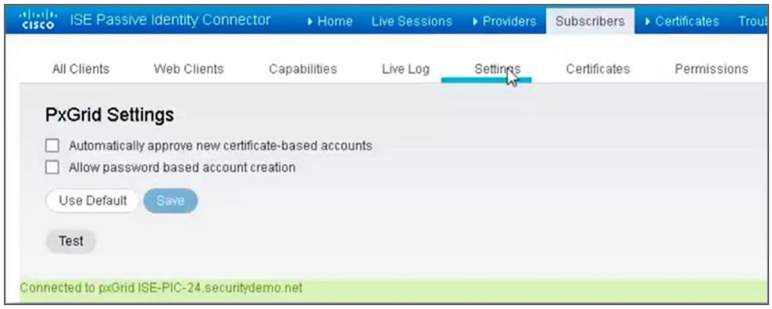

図 47.
pxGrid の設定

5. FMC で [システム（System）] -> [統合（Integration）] -> [アイデンティティ ソース（Identity Sources）] の順に選択します。[アイデンティティ サービス エンジン（Identity Services Engine）] をクリックします。
6. 表示されるフィールドに、次の詳細情報を入力します。
   a) pxGrid コントローラのプライマリホスト名/IP アドレスと、任意でセカンダリホスト名/IPアドレスを入力します
   b) pxGrid サーバの CA ドロップダウンで、[+] 記号をクリックして pxGrid コントローラのルート CA をインポートします。[参照（Browse）] をクリックして、ステップ 3 で抽出したフォルダに移動します。このフォルダで pxGrid ルート CA 証明書を選択して、この証明書の名前を入力します。

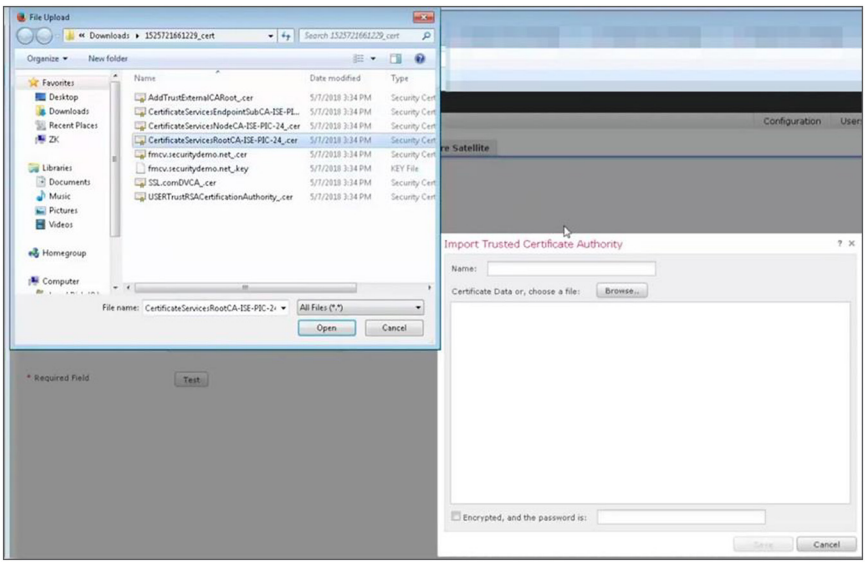

図 48.
pxGrid ルート証明書のインポート

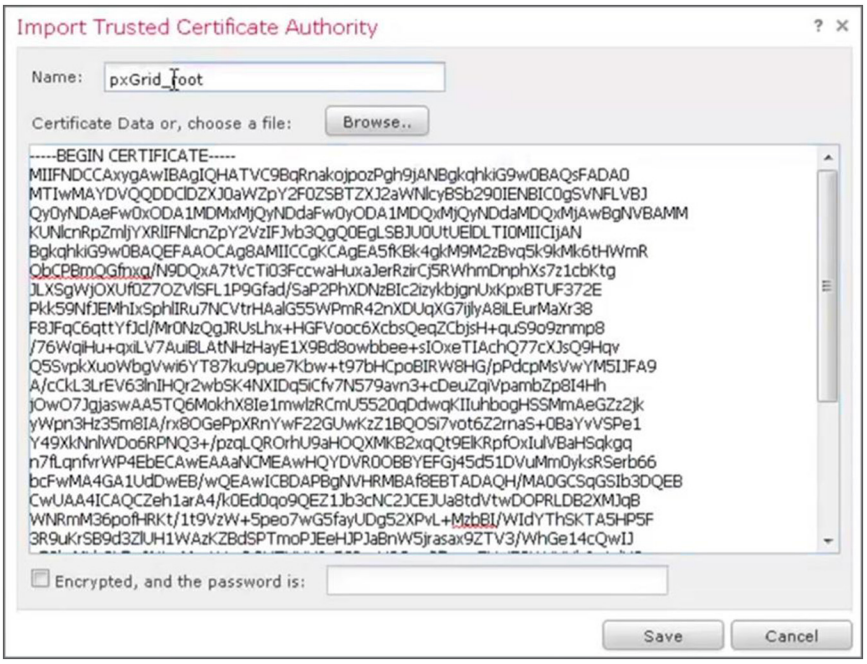

図 49.
pxGrid ルート証明書のインポート

c) ISE 2.2 以降、すべての pxGrid 通信はセキュアな pxGrid チャネル内で行われます。つまり、MnT ノードからの一括ダウンロードはすべて管理証明書ではなく **pxGrid 証明書を使用して**保護されます。次に、[MNT サーバ CA（MNT Server CA）] フィールドで上記の手順と同じ pxGrid 証明書を選択します。

d) [FMC サーバ証明書（FMC Server Certificate）] フィールドの横にある [+] 記号をクリックします。[証明書データ（Certificate Data）] の横にある [参照（Browse）] をクリックして、FMC PEM 証明書を選択します。[キー（Key）] の横にある [参照（Browse）] をクリックして、FMC PKCS＃8 キーを選択します。下のフィールドに秘密キーのパスワードを入力します。[保存（Save）] をクリックします。

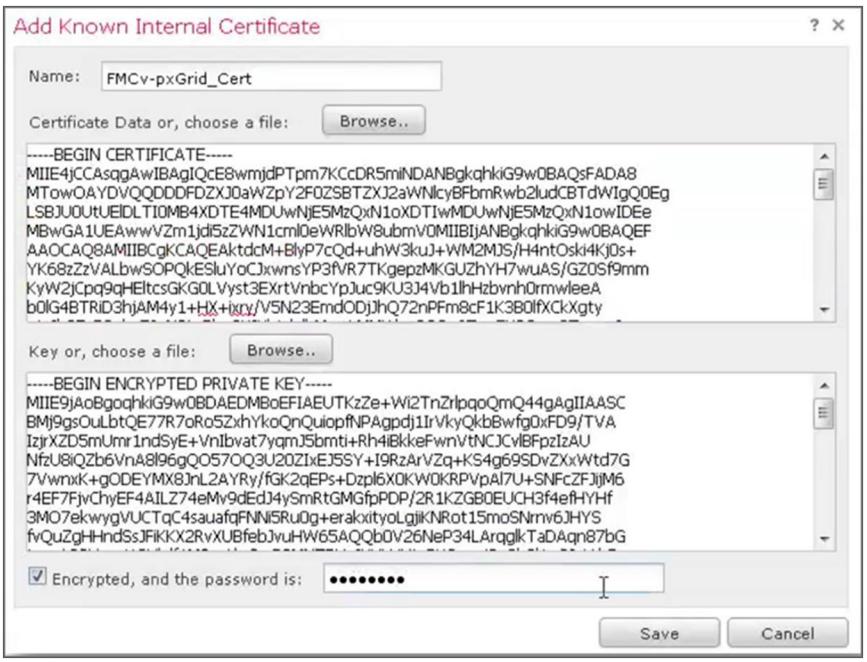

図 50.
pxGrid によって生成された FMC 証明書とキーのインポート

e) **ISE ネットワークフィルタ**は、指定された IPv4 アドレスブロックのユーザデータのみをダウンロードするように FMC に指示します。

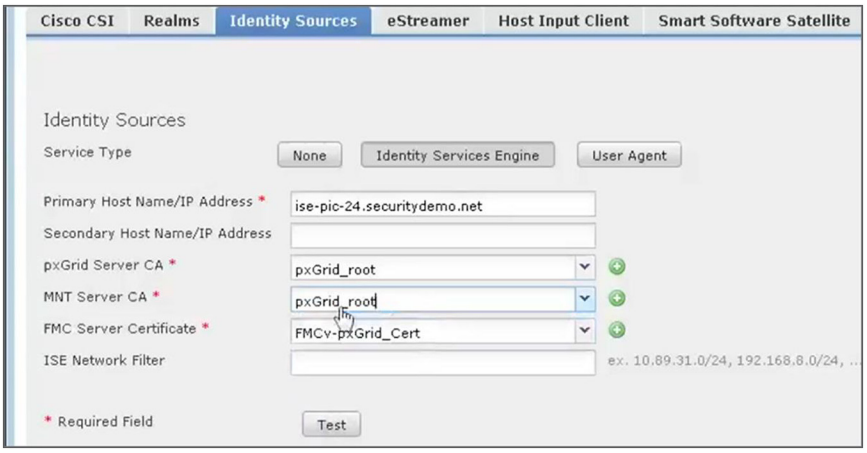

図 51.
FMC と ISE/PIC の統合の設定

f) [テスト（Test）] ボタンをクリックすると、ISE/PIC サーバへの接続をテストできます。

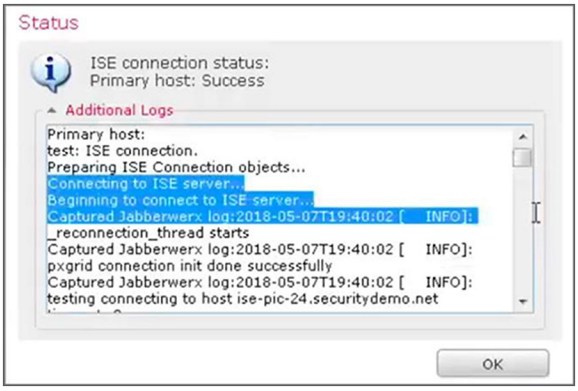

図 52.
ISE 統合テスト

g) テストが成功したら、[分析（Analysis）] -> [ユーザ（Users）] -> [アクティブセッション（Active Sessions）] の順に選択すると、ドメインのログオンイベントが表示されます。

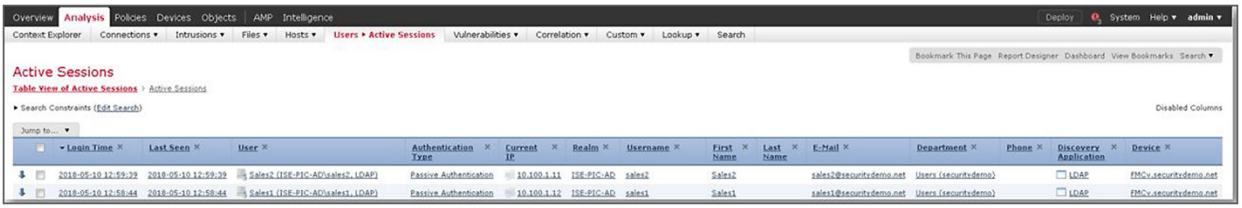

図 53.
FMC ユーザ アクティビティ イベント

コマンド root@firepower:~# **adi_cli session** を使用して、FMC CLI の Sudo モードからアクティブセッションを表示することもできます。

ユーザ ID を認識するようにアクセスポリシーを設定

1. [ポリシー（Policies）] -> [アクセス制御（Access Control）] -> [アイデンティティ（Identity）] に移動して、[新しいポリシー（New Policy）] をクリックします。
2. [名前（Name）] と任意で [説明（Description）] を入力してから、[保存（Save）] をクリックします。
3. [新規ルールの追加（Add New Rule）] をクリックして、アイデンティティルールを設定します。
4. [名前（Name）] を入力します。[有効（Enabled）] フィールドのチェックボックスをオンにしたままで、[アクション（Action）] を「パッシブ認証（Passive Authentication）」に設定します。
5. [レルムと設定（Realm & Settings）] に移動します。[レルム（Realm）] ドロップダウンリストから、[Security_Demo AD] レルムを選択します。[追加（Add）] をクリックします。

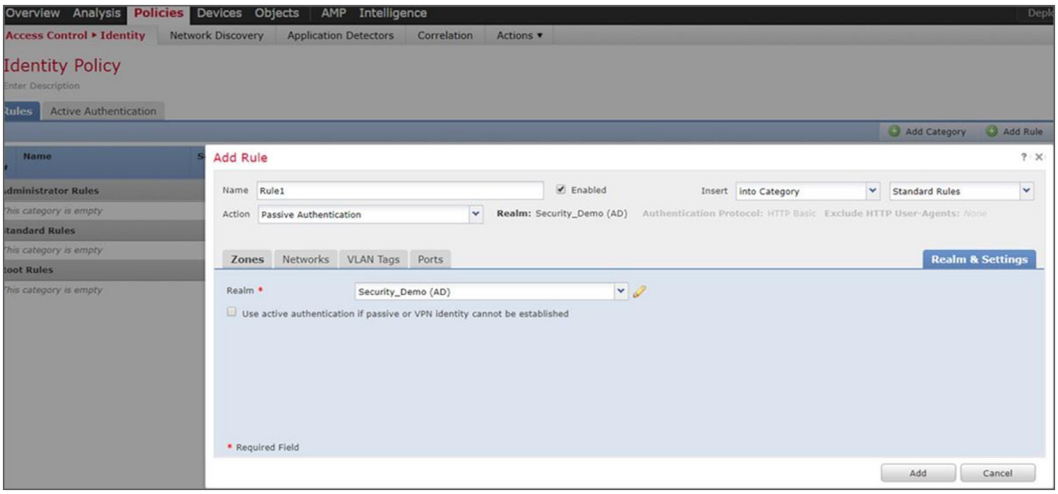

図 54.
アイデンティティルールの追加

6. [ポリシー（Policies）] -> [アクセス制御（Access Control）] -> [アクセス制御（Access Control）] に移動して、アクセス ポリシーを編集します。
7. [アイデンティティポリシー（Identity Policy）] をクリックして、ドロップダウンリストからポリシー名を選択します。[OK] をクリックします。

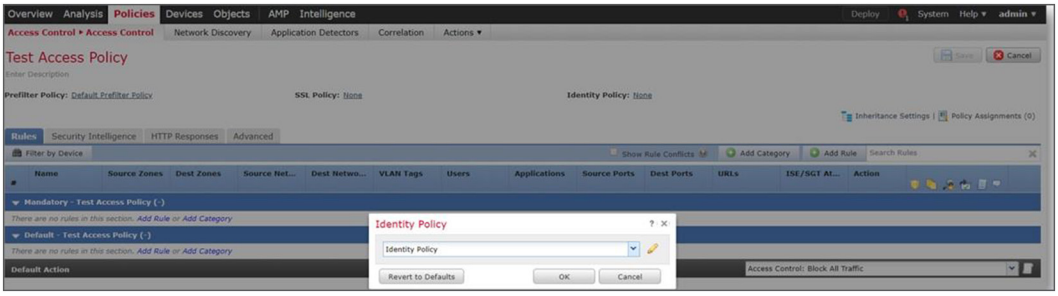

図 55.
ID ポリシーの追加

8. 同じアクセスポリシー内で、[ルールの追加（Add Rule）] をクリックします。 ダウンロードしたユーザとグループを使用できるようにするには、[ユーザ（Users）] に移動して、[使用可能なドメイン（Available Domains）] から [Security_Demo] を選択します。 これにより、[利用可能なユーザ（Available Users）] リストが表示され、そこから該当するユーザを選択できます。

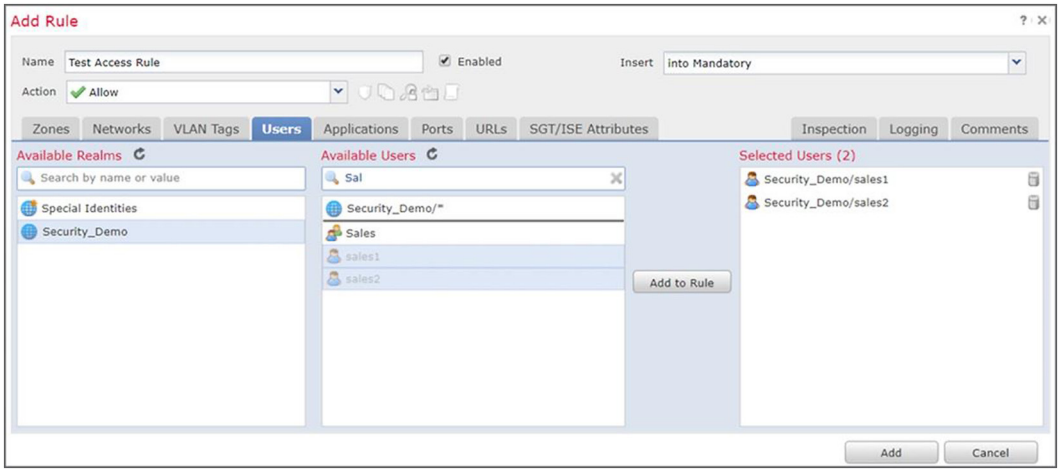

図 56.
アクセス ポリシーへのユーザアイデンティティの追加

9. [追加（Add）] をクリックします。
10. [保存（Save）] をクリックします。
11. この構成を FTD に展開します。

まとめ

上記のとおり、FMC-ISE pxGrid-AD を統合することで、ユーザコンテキストを認識して制御するための強力な機能が管理者に提供されます。また、このソリューションをカスタマイズすることで、小規模な環境から大規模な Active Directory ドメインやフォレスト環境にも対応することができます。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C07-742017-01JA 21.05