プローブおよびプロバイダとしての Active Directory

Active Directory（AD）は、ユーザー ID 情報（ユーザー名、IP アドレス、ドメイン名など）の取得元である安全性が高く正確なソースです。

AD プローブ（パッシブ ID サービス）は、WMI テクノロジーを使用して AD からユーザー ID 情報を収集しますが、その他のプローブはその他のテクノロジーや手法で AD をユーザー ID プロバイダとして使用します。ISE-PIC のその他のプローブとプロバイダ タイプの詳細については、プロバイダを参照してください。

Active Directory プローブを設定すると、次の（ソースとして Active Directory を使用する）その他のプローブも迅速に設定して有効にできます。

- Active Directory エージェント

（注） Active Directory エージェントは、Windows Server 2008 以降でのみサポートされます。

- SPAN
- エンドポイント プローブ

また、ユーザー情報の収集時に AD ユーザー グループを使用するために Active Directory プローブを設定します。AD、エージェント、SPAN、および syslog プローブで AD ユーザーグループを使用できます。AD グループの詳細については、Active Directory ユーザー グループの設定（7 ページ）を参照してください。

- Active Directory の使用 （1 ページ）
- Active Directory の設定 （12 ページ）

Active Directory の使用

パッシブ ID サービス 用の Active Directoryプローブを設定する前に、次のことを確認します。

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないこと。
- 参加操作用の 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）] を使用して設定されていないこと。
- DNS サーバーを適切に設定していることを確認します。これには、ISE-PIC からのクライアント マシンの逆引きの設定も含まれます。詳細については、DNS サーバーを参照してください。
- NTP サーバーのクロック設定を同期します。詳細については、システム時刻とネットワーク タイム プロトコル サーバー設定の指定を参照してください。

（注） Cisco ISE-PICが Active Directory に接続されているときに操作に関する問題がある場合は、[レポート（Reports）] の下にある [AD コネクタ操作レポート（AD Connector Operations Report ）] を参照してください。詳細については、使用可能なレポートを参照してください。

PassiveID セットアップの使用を開始する

ISE-PIC には、Active Directory からユーザー ID を受信するために、Active Directory を最初のユーザー ID プロバイダとして容易に設定できるウィザードがあります。ISE-PIC に Active Directory を設定することで、後でその他のプロバイダ タイプを設定するプロセスも簡素化されます。Active Directory を設定したら、ユーザーデータを受信するクライアントを定義するため、サブスクライバ（Cisco Firepower Management Center（FMC）や Stealthwatch など）を設定する必要があります。サブスクライバの詳細については、サブスクライバ を参照してください。

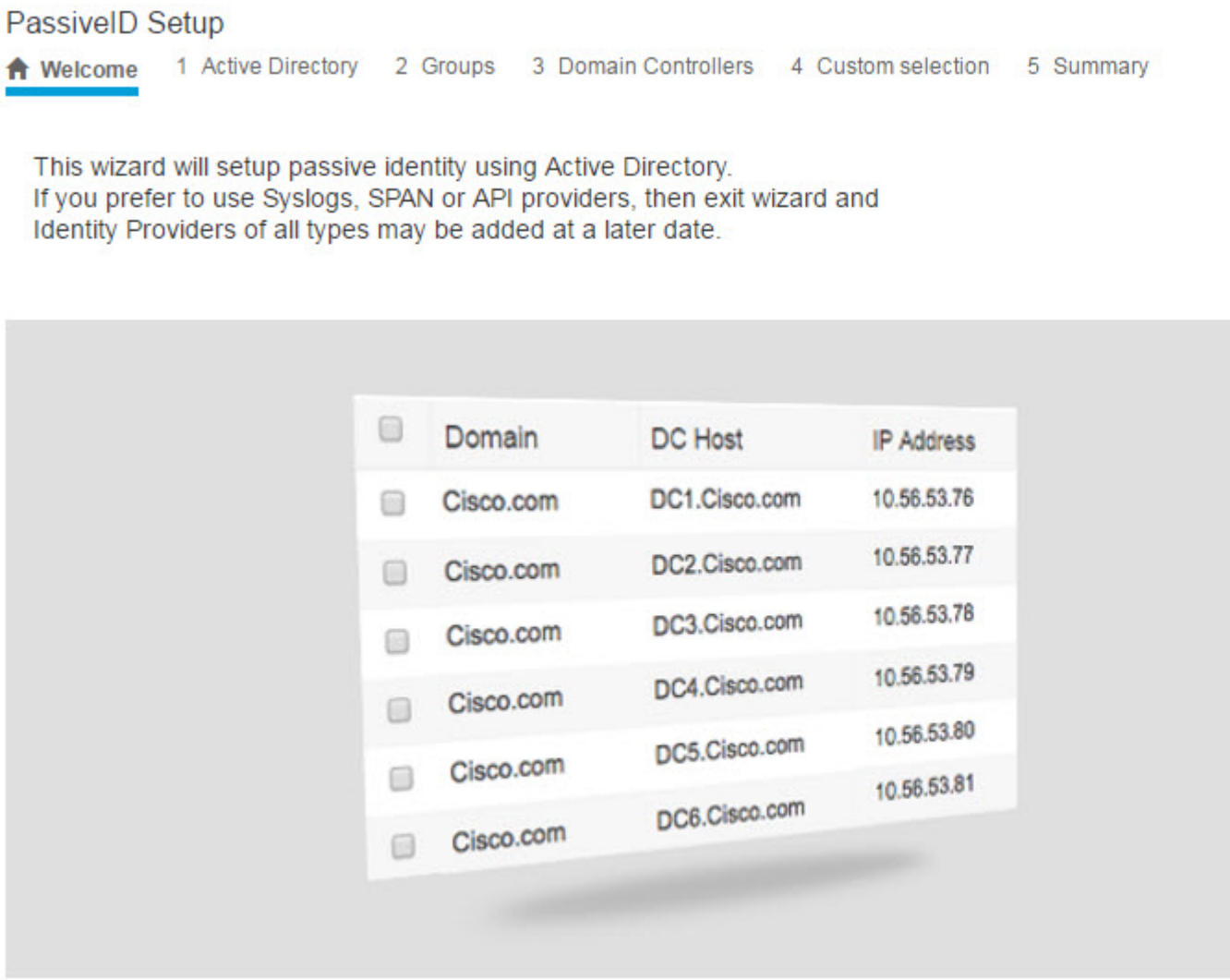
始める前に

- Microsoft Active Directory サーバーがネットワーク アドレス トランスレータの背後にないこと、およびネットワーク アドレス変換（NAT）アドレスを持たないことを確認します。
- 参加操作用の 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）] を使用して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 サーバー（DNS）にあることを確認します。ISE-PIC からのクライアント 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。詳細については、DNS サーバーを参照してください。

ステップ 1 **[ホーム（Home）] > [概要（Introduction）]** を選択します。[パッシブ ID コネクタの概要（Passive Identity Connector Overview）] 画面で [パッシブ ID ウィザード（Passive Identity Wizard）] をクリックします。

[PassiveID セットアップ（PassiveID Setup）] が表示されます。

図 *1 : [PassiveID セットアップ（PassiveID Setup）]*



ステップ 2 [次へ（Next）] をクリックしてウィザードを開始します。

ステップ 3 この Active Directory の参加ポイントの一意の名前を入力します。このノードが接続されている Active Directory ドメインのドメイン名を入力し、Active Directory 管理者のユーザー名とパスワードを入力します。

管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

ステップ 4 [次へ（Next）] をクリックし、Active Directory グループを定義し、追加してモニターするユーザー グループをすべてオンにします。

前のステップで設定した Active Directory 参加ポイントに基づいて Active Directory ユーザー グループが自動的に表示されます。

ステップ 5 [次へ（Next）] をクリックします。モニターする DC を選択します。[カスタム（Custom）] を選択した場合は、次の画面でモニターする特定の DC を選択します。完了したら、[次へ（Next）] をクリックします。

ステップ 6 [終了（Exit）] をクリックして、ウィザードを終了します。

次のタスク

最初のプロバイダとして Active Directory の設定を完了したら、追加のプロバイダ タイプも容易に設定できます。詳細については、プロバイダを参照してください。さらに、定義したいずれかのプロバイダが収集したユーザー ID 情報を受信するためのサブスクライバも設定できるようになりました。詳細については、サブスクライバを参照してください。

Active Directory（WMI）プローブの段階的なセットアップ

パッシブ ID サービス に Active Directory とWMI を設定するには、PassiveID セットアップの使用を開始する （2 ページ）を使用するか、この章の次の手順を実行します。

1. Active Directory プローブを設定します。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 （4 ページ）を参照してください。
2. AD ログイン イベントを受信する 1 つ以上の WMI 設定ノードの Active Directory ドメインコントローラのリストを作成します。
3. Active Directory を ISE-PIC と統合するため Active Directory を設定します。
4. （オプション）Active Directory プロバイダの管理 （8 ページ）。

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

始める前に

Cisco ISE-PIC ノードが、NTP サーバー、DNS サーバー、ドメインコントローラ、グローバルカタログサーバーが配置されているネットワークと通信できることを確認します。

Active Directory と、エージェント、syslog、SPAN、およびエンドポイントの各プローブを使用するには、参加ポイントを作成する必要があります。

Active Directory と統合する際に IPv6 を使用する場合は、関連する ISE-PIC ノードで IPv6 アドレスが設定されていることを確認する必要があります。

Google Chrome ブラウザを使用し、広告ブロックソフトウェアを有効にしている場合は、広告ブロッカーを無効にする必要があります。このタスクには、広告ブロッカーの影響を受ける Cisco ISE GUI 要素が含まれています。または、Google Chrome シークレットブラウザでこのタスクを実行できます。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 [追加（Add）] をクリックして、[Active Directory 参加ポイント名（Active Directory Join Point Name）] の設定のドメイン名と ID ストア名を入力します。

ステップ 3 [送信（Submit）] をクリックします。

新しく作成された参加ポイントをドメインに参加させるかどうかを確認するポップアップ ウィンドウが表示されます。すぐに参加させる場合は [はい（Yes）] をクリックします。

[いいえ（No）] をクリックした場合、設定を保存すると、Active Directory ドメインの設定がグローバルに保存されますが、いずれの Cisco ISE-PIC ノードもまだドメインに参加しません。

ステップ 4 作成した新しい Active Directory 参加ポイントの横にあるチェックボックスをオンにして [編集（Edit）] をクリックします。展開の参加/脱退テーブルに、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスが表示されます。

ステップ 5 参加ポイントがステップ 3 の間にドメインに参加しなかった場合は、関連する Cisco ISE-PIC ノードの横にあるチェックボックスをオンにし、[参加（Join）] をクリックして Active Directory ドメインに Cisco ISE-PIC ノードを参加させます。

設定を保存した場合も、これを明示的に実行する必要があります。1 回の操作で複数の Cisco ISE-PIC ノードをドメインに参加させるには、使用するアカウントのユーザー名とパスワードがすべての参加操作で同じである必要があります。各 Cisco ISE-PIC ノードを追加するために異なるユーザー名とパスワードが必要な場合は、Cisco ISE-PIC ノードごとに参加操作を個別に実行する必要があります。

ステップ 6 [ドメインへの参加（Join Domain）] ダイアログボックスで Active Directory のユーザー名とパスワードを入力します。

管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。

参加操作に使用するユーザーは、ドメイン自体に存在する必要があります。ユーザーが異なるドメインまたはサブドメインに存在する場合、ユーザー名は jdoe@acme.com のように、UPN 表記で表記する必要があります。

ステップ 7 （任意） [組織ユニットの指定（Specify Organizational Unit）] 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は、Cisco ISE-PIC ノードのマシンアカウントを CN=Computers,DC=someDomain,DC=someTLD 以外の特定の組織ユニットに配置する場合に、オンにする必要があります。Cisco ISE-PIC は、指定された組織ユニットの下にマシン アカウントを作成するか、またはマシン アカウントがすでにある場合は、この場所に移動します。組織ユニットが指定されない場合、Cisco ISE-PIC はデフォルトの場所を使用します。値は完全識別名（DN）形式で指定する必要があります。構文は、Microsoft のガイドラインに準拠する必要があります。特別な予約文字（/'+,;=<> など）、改行、スペース、およびキャリッジリターンは、バックスラッシュ（\）によってエスケープする必要があります。たとえば、OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ や Workstations,DC=someDomain,DC=someTLD のようにします。マシン アカウントがすでに作成されている場合、このチェックボックスをオンにする必要はありません。Active Directory ドメインに参加したマシン アカウントのロケーションを後で変更することもできます。

ステップ 8 [OK] をクリックします。

Active Directory ドメインに参加する複数のノードを選択できます。

参加操作に失敗した場合、失敗メッセージが表示されます。各ノードの失敗メッセージをクリックして、そのノードの詳細なログを表示します。

（注） 参加が完了すると、Cisco ISE-PIC によりその AD グループと対応するセキュリティ識別子（SID）が更新されます。Cisco ISE-PIC は自動的に SID の更新プロセスを開始します。このプロセスを完了できるようにする必要があります。

（注） DNS サービス（SRV）レコードが欠落している（参加しようとしているドメインに対し、ドメインコントローラが SRV レコードをアドバタイズしない）場合は、Active Directory ドメインに Cisco ISE-PIC を参加させることができない可能性があります。トラブルシューティング情報については、次の Microsoft Active Directory のマニュアルを参照してください。

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

（注） ISE には最大 200 のドメイン コントローラのみを追加できます。制限を超えると、「エラー発生 <DC FQDN> - DC の数が最大許容数である 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）」というエラーが表示されます。

ドメイン コントローラの追加

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 （注） パッシブ ID サービスの新しいドメイン コントローラ（DC）を追加するには、その DC のログイン クレデンシャルが必要です。

[PassiveID] タブに移動し、[DC の追加（Add DCs）] をクリックします。

ステップ 4 モニター対象として参加ポイントに追加するドメイン コントローラの隣にあるチェックボックスをオンにし、[OK] をクリックします。
ドメイン コントローラが [PassiveID] タブの [ドメイン コントローラ（Domain Controllers）] リストに表示されます。

ステップ 5 ドメイン コントローラを設定します。

a) ドメイン コントローラをオンにし、[編集（Edit）] をクリックします。[アイテムの編集（Edit Item）] 画面が表示されます。

b) 必要に応じて、各種ドメイン コントローラ フィールドを編集します。

c) WMI プロトコルを選択した場合は、[設定（Configure）] をクリックして WMI を自動的に設定するか、または [テスト（Test）] をクリックして接続をテストします。

DC フェールオーバー メカニズムは DC 優先順位リストに基づいて管理されます。このリストは、フェールオーバーの発生時に DC が選択される順序を決定します。ある DC がオフラインであるか、何らかのエラーのため到達不能な場合には、優先順位リストにおける優先順位が下がります。DC がオンラインに戻ると、優先順位リストにおけるその優先順位が適宜調整されます（上がります）。

Active Directory ユーザー グループの設定

Active Directory からユーザー ID 情報を収集するさまざまなプローブを使用する場合に、Active Directory ユーザー グループを使用できるようにするため、Active Directory ユーザー グループを設定します。内部的には、Cisco ISE はグループ名のあいまいさの問題を解決し、グループ マッピングを向上させるためにセキュリティ ID（SID）を使用します。SID により、グループ割り当てが正確に一致します。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。グループを追加する参加ポイントをクリックします。

ステップ 2 [グループ（Groups）] タブをクリックします。

ステップ 3 次のいずれかを実行します。

a) **[追加（Add）]** > **[ディレクトリからグループを選択（Select Groups From Directory）]** を選択して、既存のグループを選択します。

b) **[追加（Add）]** > **[グループの追加（Add Group）]** を選択して、グループを手動で追加します。グループ名と SID の両方を指定するか、またはグループ名のみを指定し、[SID を取得（Fetch SID）] を押します。

ユーザー インターフェイス ログインのグループ名に二重引用符（"）を使用しないでください。

ステップ 4 グループを手動で選択する場合は、フィルタを使用してグループを検索できます。たとえば、**admin*** をフィルタ基準として入力し、[グループの取得（Retrieve Groups）] をクリックすると、admin で始まるユーザー グループが表示されます。アスタリスク（*）ワイルドカード文字を入力して、結果をフィルタリングすることもできます。一度に取得できるのは 500 グループのみです。

ステップ 5 許可ポリシーで使用可能にするグループの隣にあるチェックボックスをオンにし、[OK] をクリックします。

ステップ 6 グループを手動で追加する場合は、新しいグループの名前と SID を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [保存（Save）] をクリックします。

（注） グループを削除し、そのグループと同じ名前で新しいグループを作成する場合は、[SID 値の更新（Update SID Values）] をクリックして、新しく作成したグループに新しい SID を割り当てる必要があります。アップグレードすると、最初の参加の後に SID が自動的に更新されます。

パッシブ ID 用の WMI の設定

始める前に

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。[管理（Administration）] > [システム（System）] > [展開（Deployment）] で、このノードのパッシブ ID が有効になっていることを確認します。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 [パッシブ ID（Passive ID）] タブに移動し、該当するドメイン コントローラの隣にあるチェックボックスをオンにし、[WMI の設定（Config WMI）] をクリックして、選択したドメイン コントローラが ISE-PIC により自動的に設定されるようにします。
Active Directory とドメイン コントローラを手動で設定する場合、または設定の問題のトラブルシューティングを行う場合は、Active Directory と Cisco ISE-PIC の統合の前提条件を参照してください。

（注） Windows サプリカントでネットワークレベル認証（NLA）を無効にし、パッシブ ID で正しくマッピングされるようにすることを推奨します。これは、ユーザーが代替アカウントと Remote Desktop Protocol を使用してデバイスにアクセスしようとすると、その代替ユーザーアカウントが両方のマシンにマッピングされ、その結果、これらのユーザーアカウントのアクセス権限が不正になる可能性があるためです。

（注） エージェントが Windows システムで正確な DC の詳細を取得できない場合は、DC と Cisco ISE 間の通信を再確立する必要があります。再確立するには、Cisco ISE IP アドレスと Cisco ISE FQDN（たとえば、Cisco ISE IP アドレス：https://10.0.0.0/ および Cisco ISE FQDN：https://ise1.cisco.com/）を Windows システム（**[このPC（This PC）] > [ローカルディスク（C:）（Local Disk (C:)）] > [Windows] > [System32] > [drivers] > [etc]**）の *hosts* ファイルに追加します。

Active Directory プロバイダの管理

Active Directory 参加ポイントの作成と設定が完了したら、次の作業を行い Active Directory プローブを管理します。

- Active Directory グループのためのユーザーのテスト （9 ページ）
- ノードの Active Directory の参加の表示 （9 ページ）

Active Directory グループのためのユーザーのテスト

Active Directory からユーザー グループを検証するには、[ユーザーのテスト（Test User）] ツールを使用できます。単一の参加ポイントまたはスコープのテストを実行できます。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 次のいずれかのオプションを選択します。

- すべての参加ポイントのテストを実行するには、**[拡張ツール（Advanced Tools）] > [すべての参加ポイントのユーザーをテスト（Test User for All Join Points）]** を選択します。
- 特定の参加ポイントのテストを実行するには、参加ポイントを選択し、[編集（Edit）] をクリックします。Cisco ISE-PIC ノードを選択し、[ユーザーのテスト（Test User）] をクリックします。

ステップ 3 Active Directory のユーザー（またはホスト）のユーザー名とパスワードを入力します。

ステップ 4 認証タイプを選択します。ステップ 3 のパスワード入力は、ルックアップ オプションを選択する場合には必要ありません。

ステップ 5 すべての参加ポイントに対してこのテストを実行する場合は、このテストを実行する Cisco ISE-PIC ノードを選択します。

ステップ 6 Active Directory からグループを取得するには、[グループを取得（Retrieve Groups）] および [属性の取得（Retrieve Attributes）] チェック ボックスをオンにします。

ステップ 7 [テスト（Test）] をクリックします。
テスト操作の結果と手順が表示されます。手順で失敗の原因を特定し、トラブルシューティングできます。

また、Active Directory がそれぞれの処理手順を実行するのに要する時間（ミリ秒単位）を表示することもできます。操作にかかる時間がしきい値を超えると、Cisco ISE-PIC に警告メッセージが表示されます。

ノードの Active Directory の参加の表示

特定の Cisco ISE-PIC ノードのすべての Active Directory 参加ポイントのステータスまたはすべての Cisco ISE-PIC ノードのすべての参加ポイントのリストを表示するには、[Active Directory] ページの [ノード ビュー（Node View）] ボタンを使用できます。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 [ノード ビュー（Node View）] をクリックします。

ステップ 3 [ISE Node（ISE ノード）] ドロップダウン リストからノードを選択します。

テーブルに、Active Directory のステータスがノード別に一覧されます。展開に複数の参加ポイントと複数の Cisco ISE-PIC ノードがある場合、このテーブルが更新されるまでに数分かかる場合があります。

ステップ 4 その Active Directory 参加ポイントのページに移動し、その他の特定のアクションを実行するには、参加ポイントの [名前（Name）] リンクをクリックします。

ステップ 5 [診断ツール（Diagnostic Tools）] ページに移動して特定の問題のトラブルシューティングを行うには、[診断概要（Diagnostic Summary）] 列のリンクをクリックします。診断ツールでは、ノードごとに各参加ポイントの最新の診断結果が表示されます。

Active Directory の問題の診断

診断ツールは、各 Cisco ISE-PIC ノードで実行されるサービスです。診断ツールを使用して、Active Directory 展開を自動的にテストおよび診断したり、Cisco ISE-PIC によって Active Directory が使用される場合に機能やパフォーマンスの障害の原因となる可能性がある問題を検出するための一連のテストを実行したりすることができます。

Cisco ISE-PIC が Active Directory に参加できない、または Active Directory に対して認証できない理由は、複数あります。このツールは、Cisco ISE-PIC を Active Directory に接続するための前提条件が正しく設定されていることを確認するのに役立ちます。また、ネットワーク、ファイアウォール設定、クロック同期、ユーザー認証などの問題の検出に役立ちます。このツールは、手順をステップごとに説明したガイドとして機能し、必要に応じて、中間の各レイヤの問題の修正を支援します。

ステップ 1 **[プロバイダ（Providers）]** > **[Active Directory]** を選択します。

ステップ 2 [拡張ツール（Advanced Tools）] ドロップダウン リストをクリックし、[診断ツール（Diagnostic Tools）] を選択します。

ステップ 3 診断を実行する Cisco ISE-PIC ノードを選択します。

Cisco ISE-PIC ノードを選択しない場合は、すべてのノードでテストが実行されます。

ステップ 4 特定の Active Directory 参加ポイントを選択します。

Active Directory 参加ポイントを選択しない場合は、すべての参加ポイントでテストが実行されます。

ステップ 5 オンデマンドで、またはスケジュールに基づいて診断テストを実行できます。

- テストをすぐに実行するには、[テストを今すぐ実行（Run Tests Now）] を選択します。
- スケジュールした間隔でテストを実行するには、[スケジュールしたテストを実行する（Run Scheduled Tests）] チェックボックスをオンにし、開始時刻とテストの実行間隔（時、日、週単位）を指定します。このオプションを有効にすると、すべての診断テストがすべてのノードとインスタンスに対して実行され、[ホーム（Home）] ダッシュボードの [アラーム（Alarms）] ダッシュレットに障害が報告されます。

ステップ 6 警告ステータスまたは失敗ステータスのテストの詳細を確認するには、[テストの詳細の表示（View Test Details）] をクリックします。

このテーブルを使用して、特定のテストの再実行、実行中のテストの停止、特定のテストのレポートの表示を行うことができます。

Active Directory ドメインの脱退

この Active Directory ドメインまたはこの参加ポイントを使用してユーザー ID を収集する必要がない場合は、Active Directory ドメインを脱退できます。

コマンドライン インターフェイスから Cisco ISE-PIC アプリケーション設定をリセットする場合、またはバックアップやアップグレードの後に設定を復元する場合、脱退操作が実行され、Cisco ISE-PIC ノードがすでに参加している場合は、Active Directory ドメインから切断されます。ただし、Cisco ISE-PIC ノードのアカウントは、Active Directory ドメインから削除されません。脱退操作では Active Directory ドメインからノード アカウントも削除されるため、脱退操作は管理者ポータルから Active Directory クレデンシャルを使用して実行することを推奨します。これは、Cisco ISE-PIC ホスト名を変更する場合にも推奨されます。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 作成した Active Directory 参加ポイントの隣にあるチェックボックスをオンにし、[編集（Edit）] をクリックします。展開の参加/脱退テーブルが、すべての Cisco ISE-PIC ノード、ノードのロール、およびそのステータスとともに表示されます。

ステップ 3 Cisco ISE-PIC ノードの隣にあるチェックボックスをオンにして [脱退（Leave）] をクリックします。

ステップ 4 Active Directory のユーザー名とパスワードを入力し、[OK] をクリックしてドメインを脱退し、Cisco ISE-PIC データベースからマシン アカウントを削除します。

Active Directory クレデンシャルを入力すると、Cisco ISE-PIC ノードは Active Directory ドメインを脱退し、Active Directory データベースから Cisco ISE-PIC マシン アカウントが削除されます。

（注） Active Directory データベースから Cisco ISE-PIC マシン アカウントを削除するには、ここに入力する Active Directory クレデンシャルに、ドメインからマシン アカウントを削除する権限がなければなりません。

ステップ 5 Active Directory クレデンシャルがない場合は、[使用可能なクレデンシャルなし（No Credentials Available）] チェックボックスをオンにして、[OK] をクリックします。

[クレデンシャルなしでドメインを脱退（Leave domain without credentials）] チェックボックスをオンにすると、プライマリ Cisco ISE-PIC ノードが Active Directory ドメインから脱退します。参加時に Active Directory で作成されたマシン アカウントは、Active Directory 管理者が手動で削除する必要があります。

Active Directory の設定の削除

特定の Active Directory 設定をプローブとして使用しない場合は、Active Directory の設定を削除する必要があります。別の Active Directory ドメインに参加する場合は、設定を削除しないでく

ださい。現在参加しているドメインから脱退し、新しいドメインに参加できます。この設定は唯一の設定であるため、削除しないでください。 ISE-PIC

始める前に

Active Directory ドメインが残っていることを確認します。

ステップ 1 **[プロバイダ（Providers）] > [Active Directory]** を選択します。

ステップ 2 設定された Active Directory の横のチェックボックスをオンにします。

ステップ 3 [ローカル ノード ステータス（Local Node Status）] が [参加していない（Not Joined）] としてリストされていることを確認します。

ステップ 4 [削除（Delete）] をクリックします。

Active Directory データベースから設定を削除しました。後で Active Directory を使用する場合は、有効な Active Directory の設定を再送信できます。

Active Directory デバッグ ログの有効化

Active Directory デバッグ ログはデフォルトでは記録されません。Active Directory のデバッグ ログを有効にすると、ISE-PIC のパフォーマンスに影響する場合があります。

ステップ 1 **[管理（Administration）] > [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 Active Directory のデバッグ情報を取得する Cisco ISE-PIC ノードの隣のオプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 3 [Active Directory] オプション ボタンをクリックし、[編集（Edit）] をクリックします。

ステップ 4 [Active Directory] の隣にあるドロップダウン リストから [DEBUG] を選択します。これにはエラー、警告、および verbose ログが含まれます。完全なログを取得するには、[TRACE] を選択します。

ステップ 5 [保存（Save）] をクリックします。

Active Directory の設定

Active Directory（AD）は、安全性が高く正確なソースであり、ここからユーザー情報（ユーザー名、IP アドレスなど）が取得されます。

参加ポイントを作成、編集することで Active Directory プローブを作成、管理するには、**[プロバイダー（Providers）] > [Active Directory]** を選択します。

詳細については、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 （4 ページ）を参照してください。

[プロバイダー（Providers）] > [Active Directory] を選択し、編集する参加ポイントをオンにして、**[編集（Edit）]** をクリックします。[ドメインへの参加（Join Domain）] 画面で、**[プロバイダー（Providers）] > [Active Directory]** を選択し、編集する参加ポイントをオンにして **[参加（Join）]** をクリックします。

表 *1 : Active Directory* 参加ポイント名の設定と *[*ドメインへの参加（*Join Domain*）*]* ウィンドウ

フィールド名	説明
参加ポイント名（**Join Point Name**）	設定したこの参加ポイントを容易に区別できる一意の名前。
Active Directory ドメイン（**Active Directory Domain**）	このノードが接続している Active Directory ドメインのドメイン名。
ドメイン管理者（**Domain Administrator**）	管理者権限を持つ Active Directory ユーザーのユーザー プリンシパル名またはユーザー アカウント名。
パスワード（**Password**）	Active Directory で設定されているドメイン管理者のパスワード。
組織単位の指定（**Specifiy Organizational Unit**）	管理者の組織単位の情報を入力します。
クレデンシャルの保存（**Store Credentials**）	管理者のユーザー名とパスワードが保存され、モニター対象として設定されているすべてのドメイン コントローラ（DC）に使用されます。 エンドポイント プローブの場合は、[クレデンシャルの保存（Store Credentials）] を選択する必要があります。

[プロバイダ（Providers）] > [Active Directory] を選択します。

表 *2 : [Active Directory* 参加/脱退（*Active Directory Join/Leave*）*]* ウィンドウ

フィールド名	説明
ISEノード（**ISE Node**）	インストール環境での特定のノードの URL。
ISE ノードのロール（**ISE Node Role**）	インストール環境でそのノードがプライマリ ノードまたはセカンダリ ノードのいずれであるかを指定します。
ステータス（**Status**）	ノードが Active Directory ドメインにアクティブに参加しているかどうかを示します。

フィールド名	説明
ドメイン コントローラ（**Domain Controller**）	Active Directory に参加しているノードの場合、この列には Active Directory ドメインでノードが接続している特定のドメイン コントローラが示されます。
サイト（**Site**）	これは完全な ISE インストール環境にのみ関連します。詳細については、完全な ISE インストールへの ISE-PIC のアップグレードを参照してください。

表 *3 : [*パッシブ *ID* ドメイン コントローラ（*DC*）（*Passive ID Domain Controllers (DC)*）*]* リスト

フィールド	説明
ドメイン（**Domain**）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名。
DC ホスト（**DC Host**）	ドメインコントローラが存在しているホスト。
サイト（**Site**）	これは完全な ISE インストール環境にのみ関連します。詳細については、完全な ISE インストールへの ISE-PIC のアップグレードを参照してください。
IP アドレス（**IP Address**）	ドメイン コントローラの IP アドレス。
モニター方法（**Monitor Using**）	次のいずれかの方法で、ユーザー ID 情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント を参照してください。

表 *4 : [パッシブ ID ドメインコントローラ（DC）（Passive ID Domain Controllers (DC)）] 編集ウィンドウ*

フィールド名	説明
ホスト FQDN（**Host FQDN**）	ドメインコントローラが存在しているサーバーの完全修飾ドメイン名を入力します。
説明（**Description**）	このドメイン コントローラを容易に特定できるように、一意の説明を入力します。
ユーザー名（**User Name**）	Active Directory にアクセスするための管理者のユーザー名。
パスワード（**Password**）	Active Directory にアクセスするための管理者のパスワード。
プロトコル（**Protocol**）	次のいずれかの方法で、ユーザー ID 情報を取得するため Active Directory ドメイン コントローラをモニターします。 • [WMI]：WMI インフラストラクチャを使用して Active Directory を直接モニターします。 • [エージェント名（Agent name）]：ユーザー情報を取得するために Active Directory をモニターするエージェントを定義している場合は、Agent プロトコルを選択し、ドロップダウンリストから使用するエージェントを選択します。エージェントの詳細については、Active Directory エージェント を参照してください。

Active Directory グループは Active Directory から定義および管理されます。このノードに参加している Active Directory のグループは、このタブで確認できます。Active Directory の詳細については、https://msdn.microsoft.com/en-us/library/bb742437.aspxを参照してください。

[プロバイダー（Providers）] > **[Active Directory]** > **[詳細設定（Advanced Settings）]** を選択します。

表 *5 : Active Directory* の詳細設定

フィールド名	説明
履歴期間（**History interval**）	すでに発生したユーザー ログインの情報を パッシブ ID サービスが読み取る期間。これは、パッシブ ID サービスの起動時または再起動時に、このサービスが使用不可であった間に生成されたイベントを確認するために必要となります。エンドポイント プローブがアクティブな場合、この期間の頻度が維持されます。
ユーザーセッションのエージングタイム（**User session aging time**）	ユーザーがログインできる時間です。パッシブ ID サービスでは、DC からの新しいユーザー ログイン イベントが識別されますが、DC はユーザーがログオフする時点を報告しません。エージング タイムを使用すると、ISE-PIC で、ユーザーがログインする時間間隔を決定できます。
NTLM プロトコル設定（**NTLM Protocol settings**）	ISE-PIC と DC の間の通信プロトコルとして [NTLMv1] または [NTLMv2] を選択できます。推奨されるデフォルトは [NTLMv2] です。

フィールド名	説明
[認証フロー（Authorization Flow）]	

フィールド名	説明
	PassiveID ログインユーザーの認証ポリシーを設定するには、このチェックボックスをオンにします。 Active Directory グループメンバーシップに基づいて SGT をユーザーに割り当てる認証ポリシーを設定できます。設定すると、PassiveID 認証に対しても TrustSec ポリシールールを作成できるようになります。 [PassiveID] ディクショナリの [PassiveID_Provider]、[PassiveID_Username]、または [PassiveID_Groups] 属性を使用して、PassiveID ログインユーザーの認証ルールを作成できます。[PassiveID_Provider] 属性には、次の値を設定できます。 • **API** • エージェント • **SPAN** • **Syslog** • **WMI** • その他 PassiveID ログインユーザーの IP-SGT マッピングと Active Directory グループの詳細は、セッショントピックに含まれています。これらの詳細は、pxGrid、pxGrid クラウド、または SXP を使用して公開できます。 認証ポリシーのステータスと SGT の詳細は、[RADIUSライブログ（RADIUS Live Logs）] ウィンドウ（[操作（Operations）] > [RADIUS] > [ライブログ（Live Logs）]）および [RADIUSライブセッション（RADIUS Live Sessions）] ウィンドウ（[操作（Operations）] > [RADIUS] > [ライブセッション（Live Sessions）]）で表示できます。 （注） • PassiveID、pxGrid、pxGrid クラウド、および SXP サービスがノードで有効になっていることを確認します。これらのサービスを有効にするには、[管理（Administration）] > [システム（System）] > [展開（Deployment）] を選択します。 • [SXP設定（SXP Settings）] ウィンドウ（[ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [SXP設定（SXP Settings）]）で [SXP IP SGTマッピングテーブルにRADIUSおよびPassiveID

フィールド名	説明
	マッピングを追加する（Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping）]オプションを有効にして、SXP マッピングに PassiveID マッピングを含める必要があります。 • API プロバイダーを使用して認証された PassiveID ログインユーザーの SGT の詳細は、SXP を使用して公開することはできません。ただし、これらのユーザーの SGT の詳細は、pxGrid および pxGrid Cloud を介して公開できます。

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。