大規模キャンパスネットワーク向けのODBCおよびISE DB（カスタム属性）を使用した簡素化されたアクセスポリシー

内容

概要

このドキュメントでは、機能とセキュリティの適用を損なわない大規模なキャンパス展開について説明します。シスコのエンドポイントセキュリティソリューションであるIdentity Services Engine(ISE)は、外部アイデンティティソースとの統合を通じてこの要件に対応します。

50以上の地域、4,000以上の異なるユーザプロファイル、600,000以上のエンドポイントを持つ大規模なネットワークでは、従来のIBNソリューションは、機能だけでなくすべての機能に対応できる拡張性など、さまざまな観点から検討する必要があります。今日の従来型の大規模ネットワークにおけるインテントベースネットワーク(IBN)ソリューションでは、機能だけでなく、スケーラビリティと管理の容易さにも重点が置かれています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Dot1x/MAB認証
- Cisco Identity Service Engine(CiscoISE)
- Cisco TrustSec（CTS）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

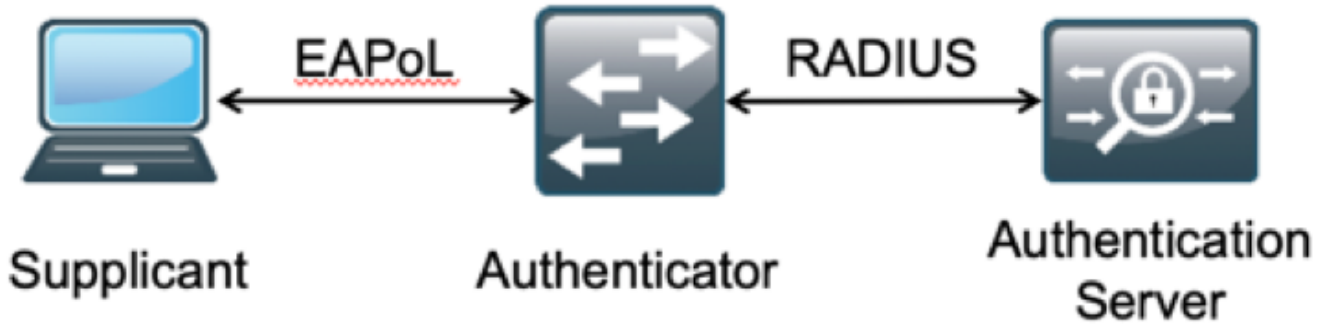
- Cisco Identity Services Engine(ISE)バージョン2.6パッチ2およびバージョン3.0
- Windows Active Directory(AD)Server 2008リリース2
- Microsoft SQL Server 2012

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定による潜在的な影響を理解してください。

背景説明

Identity Based Network(IBN)ソリューションでは、基本要素はサプリカント、オーセンティケータ、および認証(AAA)サーバです。サプリカントは、ネットワークアクセスが要求されたときにクレデンシャルを提供する、エンドポイント上のエージェントです。オーセンティケータまたはNAS（ネットワークアクセスサーバ）は、AAAサーバにクレデンシャルを伝送するネットワークスイッチとWLCで構成されるアクセスレイヤです。認証サーバは、ユーザ認証要求をIDストアに対して検証し、アクセス許可またはアクセス拒否のいずれかで認証を行います。IDストアは、AAAサーバ内または外部の専用サーバ上に配置できます。

次の図に、基本的なIBN要素を示します。



RADIUSはユーザデータグラムプロトコル(UDP)ベースのプロトコルで、認証と認可が組み合わされています。エンタープライズキャンパス向けのシスコのIBNソリューションでは、ISEのPolicy Service Node(PSN)ペルソナがAAAサーバとして機能し、エンドポイントをエンタープライズIDストアに対して認証し、条件に基づいて認可します。

Cisco ISEでは、これらの要件を満たすように認証および認可ポリシーが設定されます。認証ポリシーは、有線または無線のメディアタイプと、ユーザ検証のためのEAPプロトコルで構成されます。認可ポリシーは、照合する各種エンドポイントの条件と、ネットワークアクセスの結果(VLAN、ダウンロード可能ACL、またはSecure Group Tag(SGT)など)を定義する条件で構成されます。 これらは、ISEを設定できるポリシーの最大スケール数です。

次の表に、Cisco ISEポリシーのスケールを示します。

属性	**スケール番号**
認証ルールの最大数	1000（ポリシーセットモード） 3,000（ポリシーセットモード）
許可ルールの最大数	3200 Authzプロファイルを使用

技術トレンド

セグメンテーションは、実際のエッジネットワークを必要とせずに、今日の企業ネットワークの主要なセキュリティ要素の1つになっています。エンドポイントは、内部ネットワークと外部ネットワークの間をローミングできます。セグメンテーションは、特定のセグメントに対するセキュリティ攻撃を封じ込め、ネットワーク全体に拡大するのに役立ちます。Cisco ISEのTrustSecを使用した現在のソフトウェア定義型アクセス(SDA)ソリューションでは、お客様のビジネスモデルに基づいてセグメント化を行い、VLANやIPサブネットなどのネットワーク要素への依存を回避できます。

問題

ISEポリシーの設定500を超える異なるエンドポイントプロファイルを持つ大規模な企業ネットワークでは、認証ポリシーの数が管理不能なポイントに増加する可能性があります。Cisco ISEがこのような大量のユーザプロファイルに対応するために専用の認可条件をサポートしている場合でも、管理者がこのような多数のポリシーを管理することは困難です。

さらに、お客様は専用ポリシーの代わりに共通の認証ポリシーを必要とすることがあります。これにより、管理オーバーヘッドを回避し、エンドポイントのネットワークアクセスを基準に基づいて差別化することができます。

たとえば、Active Directory(AD)を**真実のソース**とし、エンドポイントの一意の差別化要因がADの属性の1つであるエンタープライズネットワークについて考えます。このような場合、従来のポリシー設定の方法では、一意のエンドポイントプロファイルごとに許可ポリシーが多くなります。

この方法では、各エンドポイントプロファイルはdomain.comの下のAD属性によって区別されます。したがって、専用の認可ポリシーを設定する必要があります。

次の表に、従来のAuthZポリシーを示します。

ABCポリシー	AnyConnectがUser-AND-Machine-Both-Passedと等しい場合 AND ADグループがdomain.com/groups/ABCと等しい場合 THEN SGT:C2S-ABCおよびVLAN:1021

DEFポリシー	AnyConnectがUser-AND-Machine-Both-Passedと等しい場合 AND ADグループがdomain.com/groups/DEFと等しい場合 THEN SGT:C2S-DEFおよびVLAN:1022
GHIポリシー	AnyConnectがUser-AND-Machine-Both-Passedと等しい場合 AND ADグループがdomain.com/groups/GHIと等しい場合 THEN SGT:C2S-GHIおよびVLAN:1023
XYZポリシー	AnyConnectがUser-AND-Machine-Both-Passedと等しい場合 AND ADグループがdomain.com/groups/XYZと等しい場合 THEN SGT:C2S-XYZおよびVLAN:1024

提案するソリューション

Cisco ISEでサポートされる許可ポリシーの最大数に対する違反を回避するために、提案するソリューションは、属性から取得された認可結果を使用して各エンドポイントを認可する外部DBを使用することです。たとえば、ADが認可の外部DBとして使用される場合、未使用のユーザ属性（DepartmentやPinコードなど）を参照して、SGTまたはVLANにマッピングされた認可された結果を提供できます。

これは、Cisco ISEと外部DBの統合、またはカスタム属性を設定したISEの内部DB内で実現されます。このセクションでは、次の2つのシナリオの導入について説明します。

> **注：**どちらのオプションでも、DBにはDOT1Xエンドポイントの**ユーザID**が含まれますが、**パスワード**は含まれません。DBは**認証**ポイントとしてのみ使用されます。認証は、ほとんどの場合Active Directory(AD)サーバに存在する顧客のIDストアのままにすることができます。

外部DBを使用した設定

Cisco ISEは外部DBと統合され、エンドポイントのクレデンシャルを検証します。

次の表に、検証済みの外部アイデンティティ・ソースを示します。

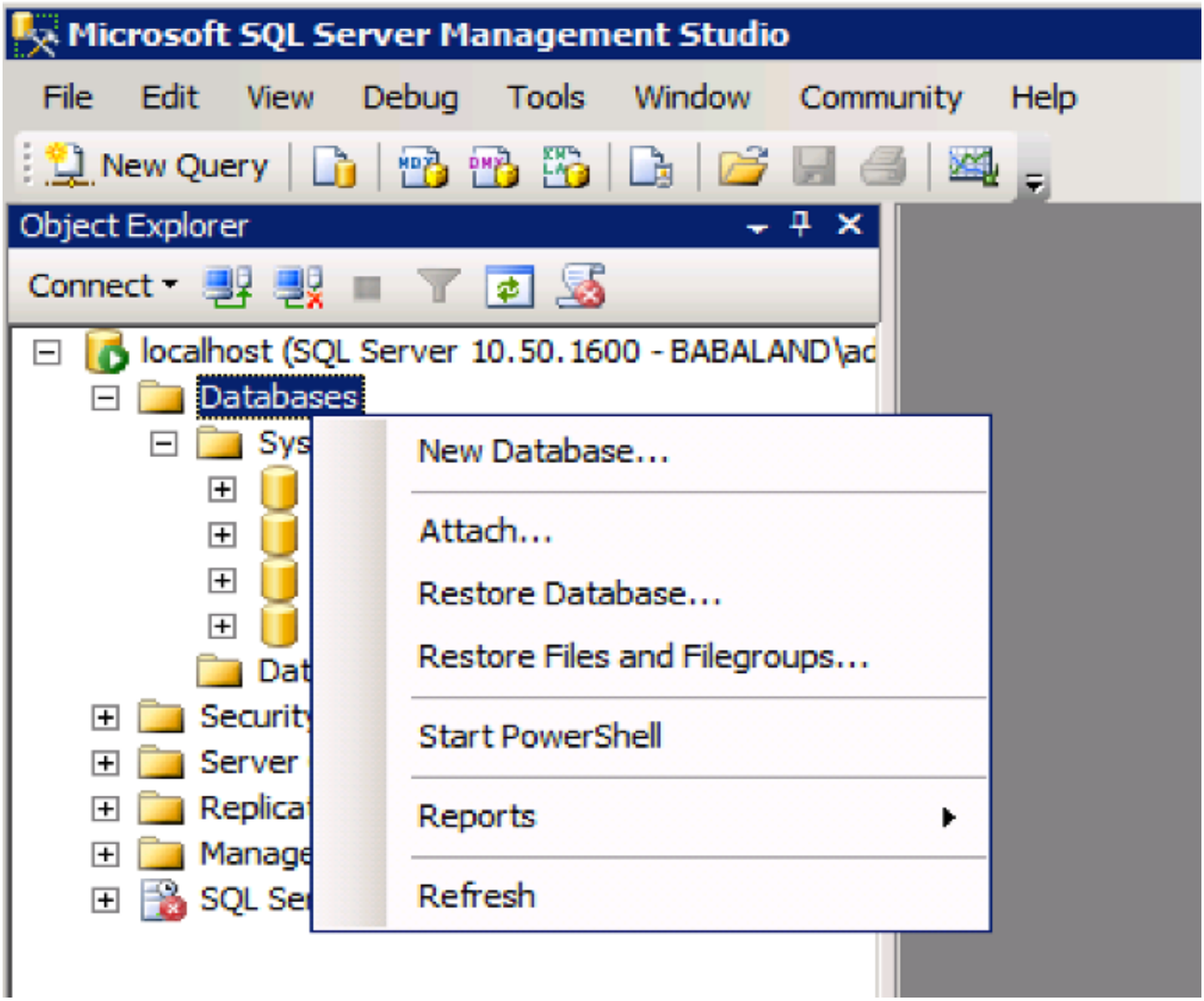
外部アイデンティティソース	OS/バージョン
Active Directory	
Microsoft Windows Active Directory 2003	-
Microsoft Windows Active Directory 2003 R2	-
Microsoft Windows Active Directory 2008	-
Microsoft Windows Active Directory 2008 R2	-
Microsoft Windows Active Directory 2012	-
Microsoft Windows Active Directory 2012 R2	-
Microsoft Windows Active Directory 2016	-
LDAPサーバ	
SunONE LDAPディレクトリサーバ	バージョン 5.2
OpenLDAPディレクトリサーバ	Version 2.4.23
任意のLDAP v3準拠サーバ	-

トークンサーバ	
RSA ACE/サーバ	6.xシリーズ
RSA Authentication Manager	7.xおよび8.xシリーズ
任意のRADIUS RFC 2865準拠トークンサーバ	-
Security Assertion Markup Language(SAML)シングルサインオン(SSO)	
Microsoft Azure	-
Oracle Access Manager(OAM)	Version 11.1.2.2.0
Oracle Identity Federation(OIF)	Version 11.1.1.2.0
PingFederateサーバ	Version 6.10.0.4
PingOne Cloud	-
セキュア認証	8.1.1
SAMLv2準拠のアイデンティティプロバイダー	-
Open Database Connectivity (ODBC)アイデンティティ・ソース	
Microsoft SQL Server(MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Editionリリース 12.1.0.2.0
PostgreSQL	9 ミリ秒
Sybase	16
MySQL	6.3
ソーシャルログイン (ゲストユーザアカウント用)	
Facebook	-

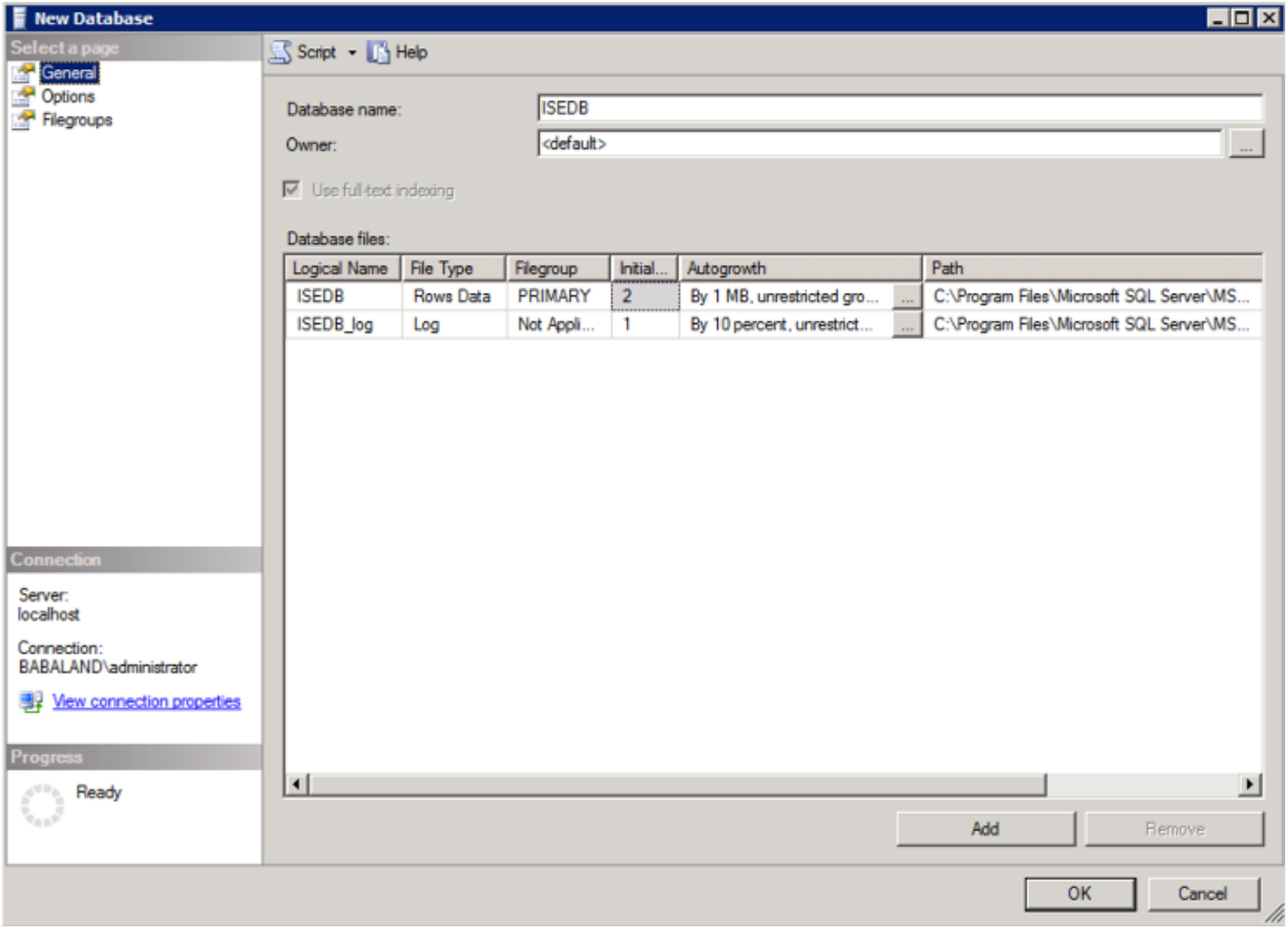
ODBC設定例

この設定は、ソリューションを構築するためにMicrosoft SQLで行われます。

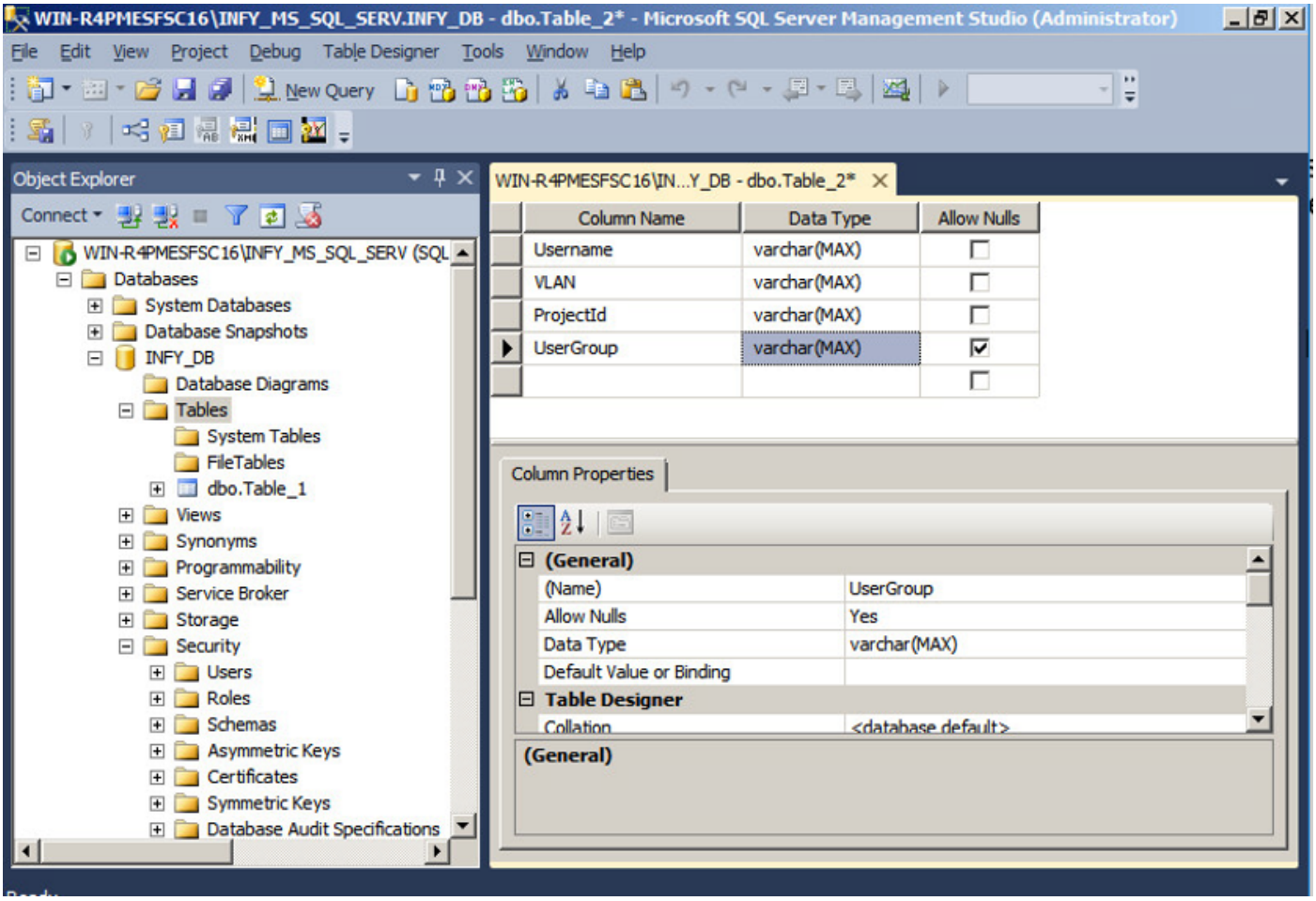
ステップ1:SQL Server Management Studioを開き([Start]メニュー> [Microsoft SQL Server])、データベースを作成します。



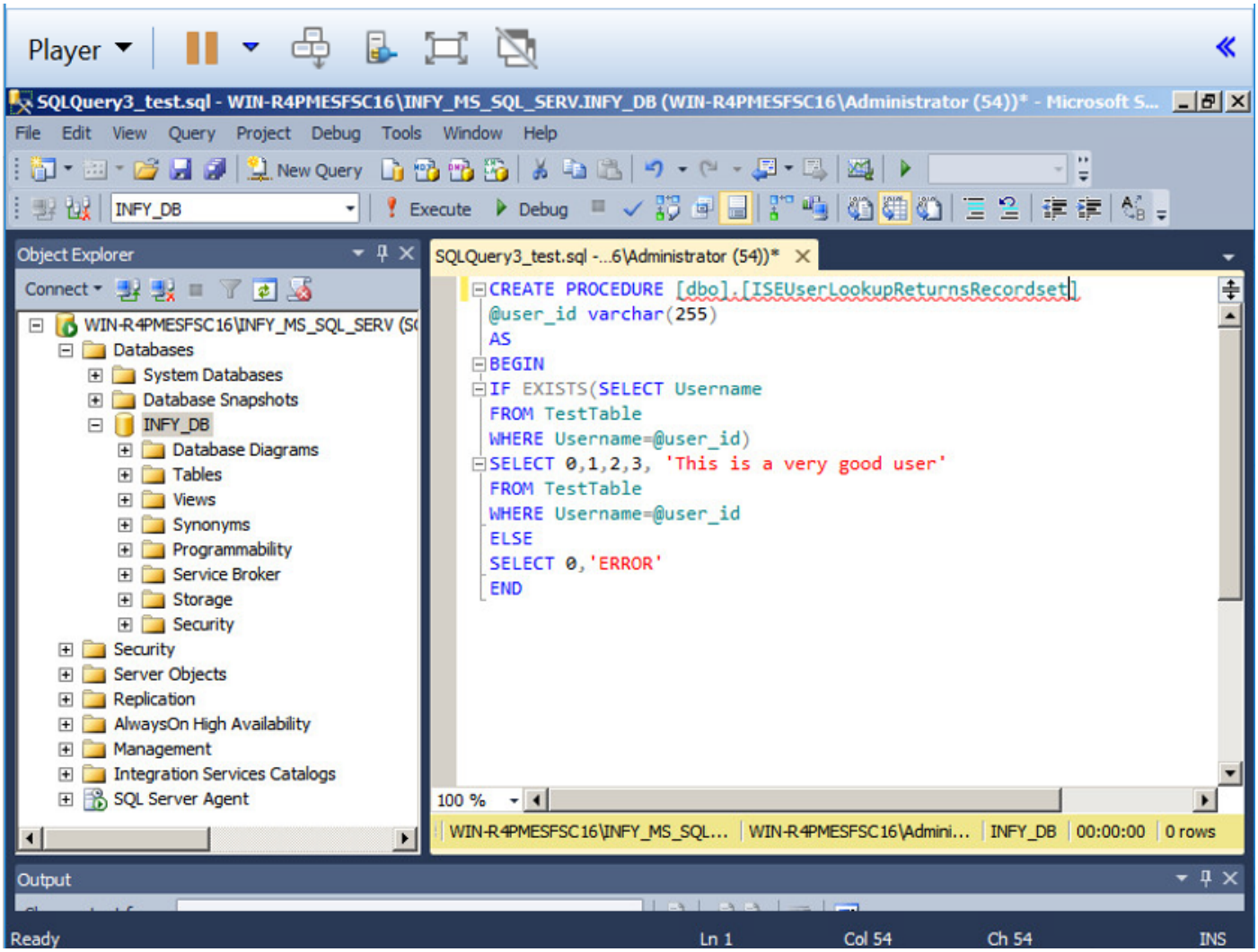
ステップ2：名前を指定し、データベースを作成します。



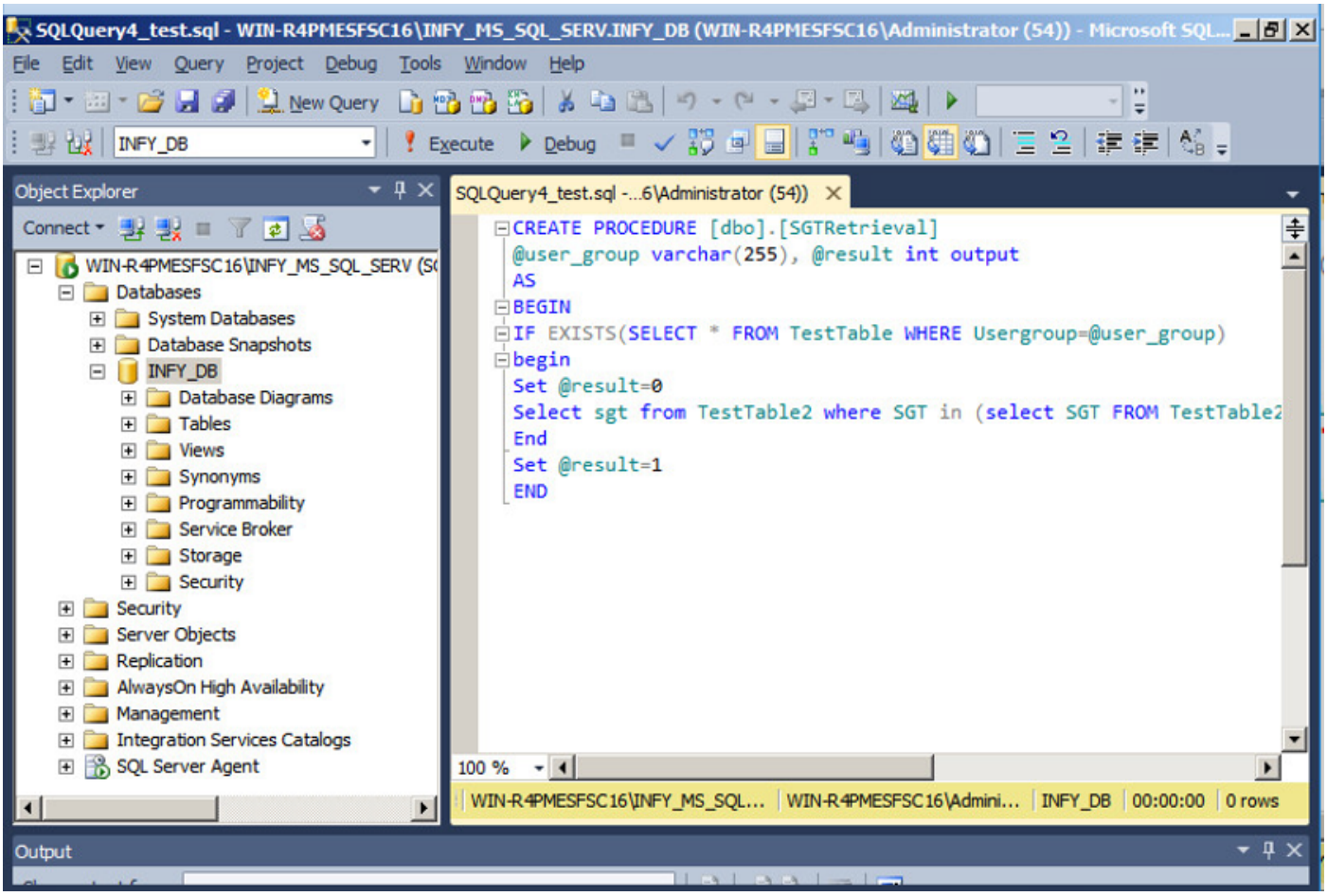
ステップ3：承認を受けるエンドポイントのパラメータとして必要な列を含む新しいテーブルを作成します。



ステップ4：ユーザ名が存在するかどうかを確認するプロシージャを作成します。



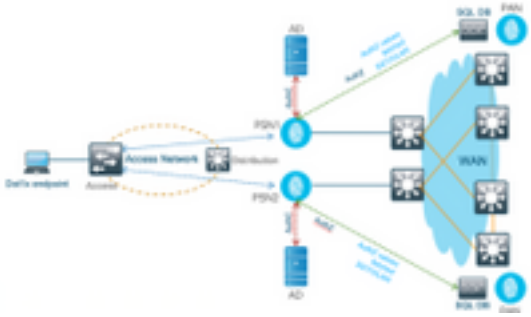
ステップ5:テーブルから属性(SGT)をフェッチするプロシージャを作成します。

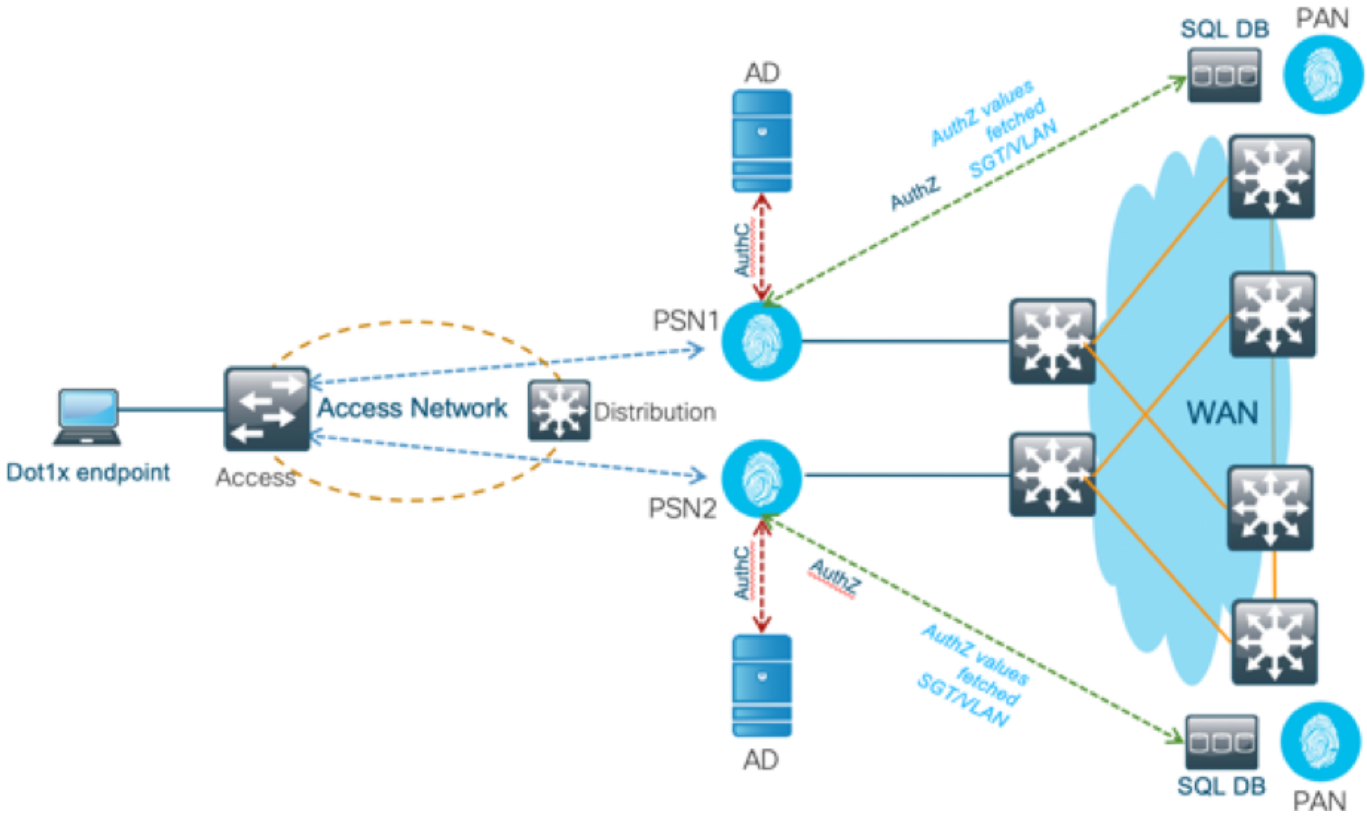


このドキュメントでは、Cisco ISEをMicrosoft SQLソリューションと統合して、大規模な企業ネットワークの認可規模の要件を満たします。

ソリューションワークフロー（ISE 2.7以前）

このソリューションでは、Cisco ISEはActive Directory(AD)およびMicrosoft SQLと統合されています。ADは認証IDストアとして使用され、MS SQLは認証に使用されます。認証プロセス中、ネットワークアクセスデバイス(NAD)はユーザクレデンシャルをPSN（IBNソリューションのAAAサーバ）に転送します。PSNは、Active Directory IDストアでエンドポイントのクレデンシャルを検証し、ユーザを認証します。認可ポリシーはMS SQL DBを参照して、**user-id**が参照として使用されるSGT/VLANなどの認可された結果をフェッチします。





長所

このソリューションには次のような利点があり、柔軟性があります。

- Cisco ISEは、外部DBが提供するすべての追加機能を活用できます。
- このソリューションは、Cisco ISEのスケール制限には依存しません。

デメリット

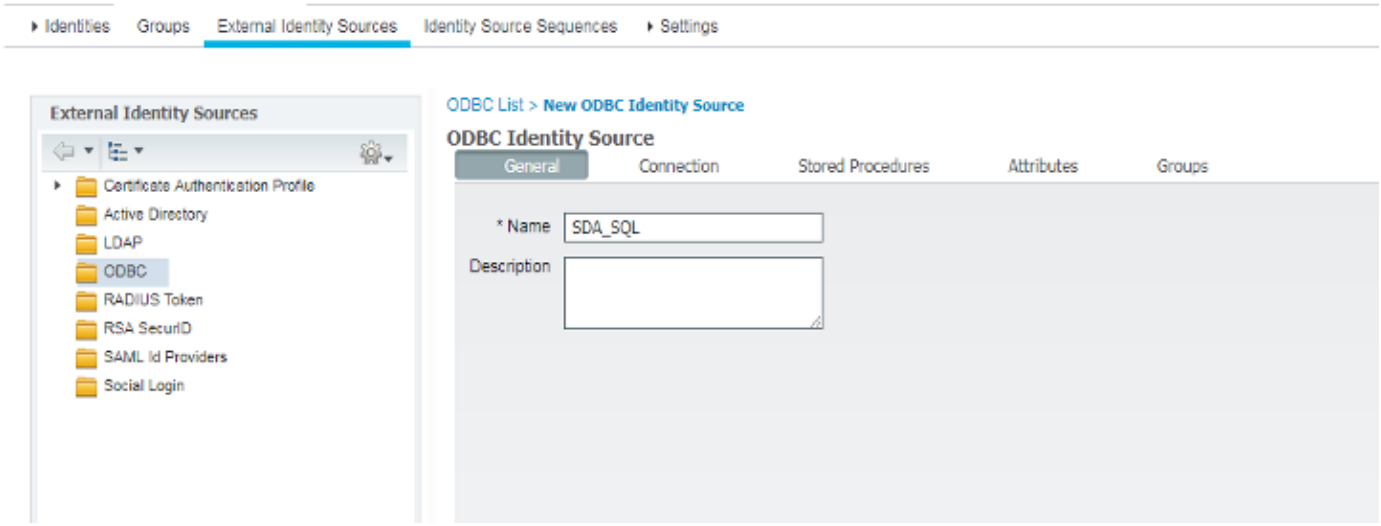
このソリューションには、次の短所があります。

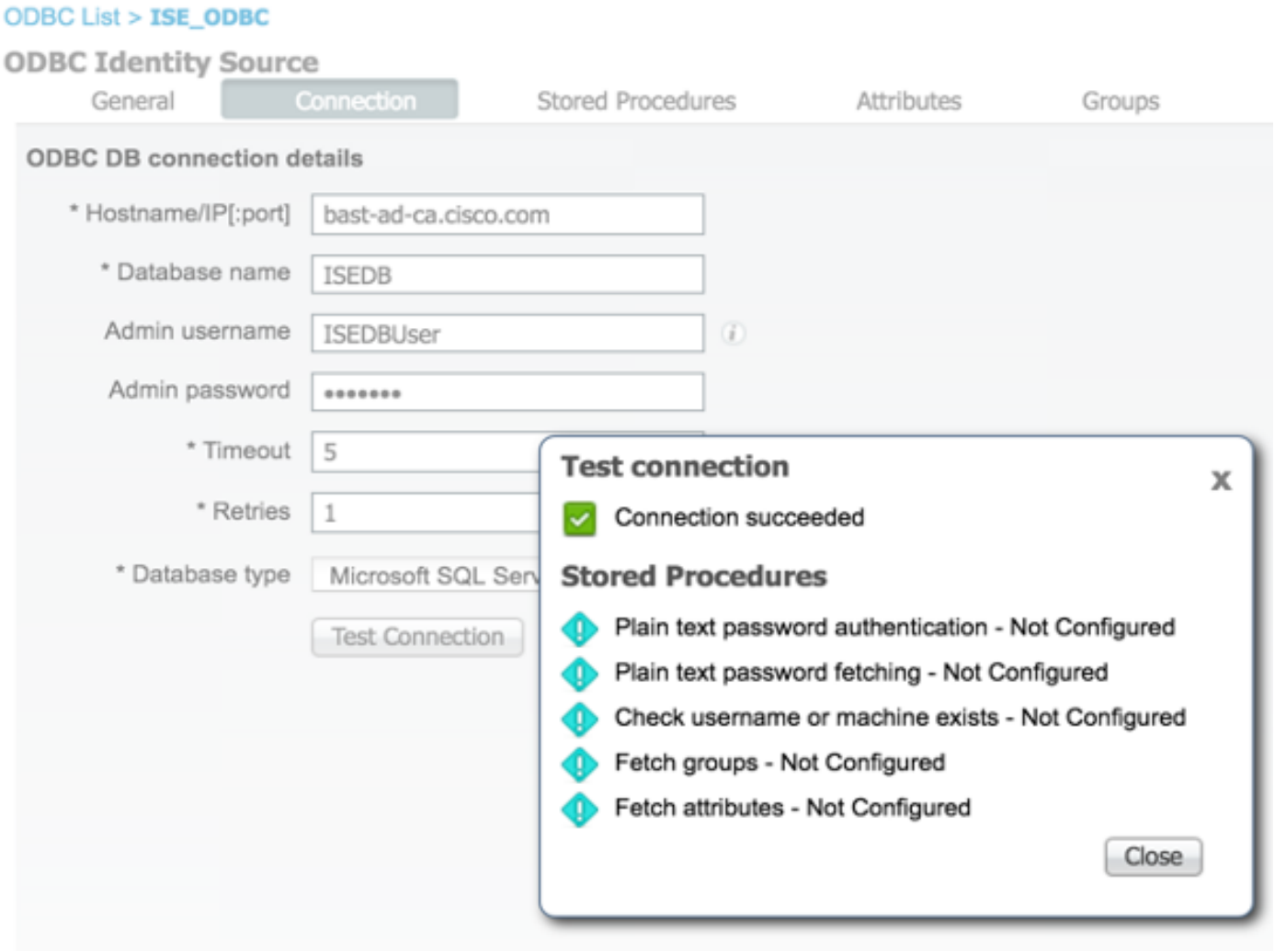
- 外部DBにエンドポイントクレデンシャルを入力するには、追加のプログラミングが必要です。
- 外部DBがPSNのようにローカルに存在しない場合、このソリューションはWANに依存し、エンドポイントAAAデータフローの障害の3rdポイントになります。
- 外部データベースのプロセスと手順を維持するために追加の知識が必要です。
- ユーザIDをDBに手動で設定した場合に発生するエラーを考慮する必要があります。

外部DBの設定例

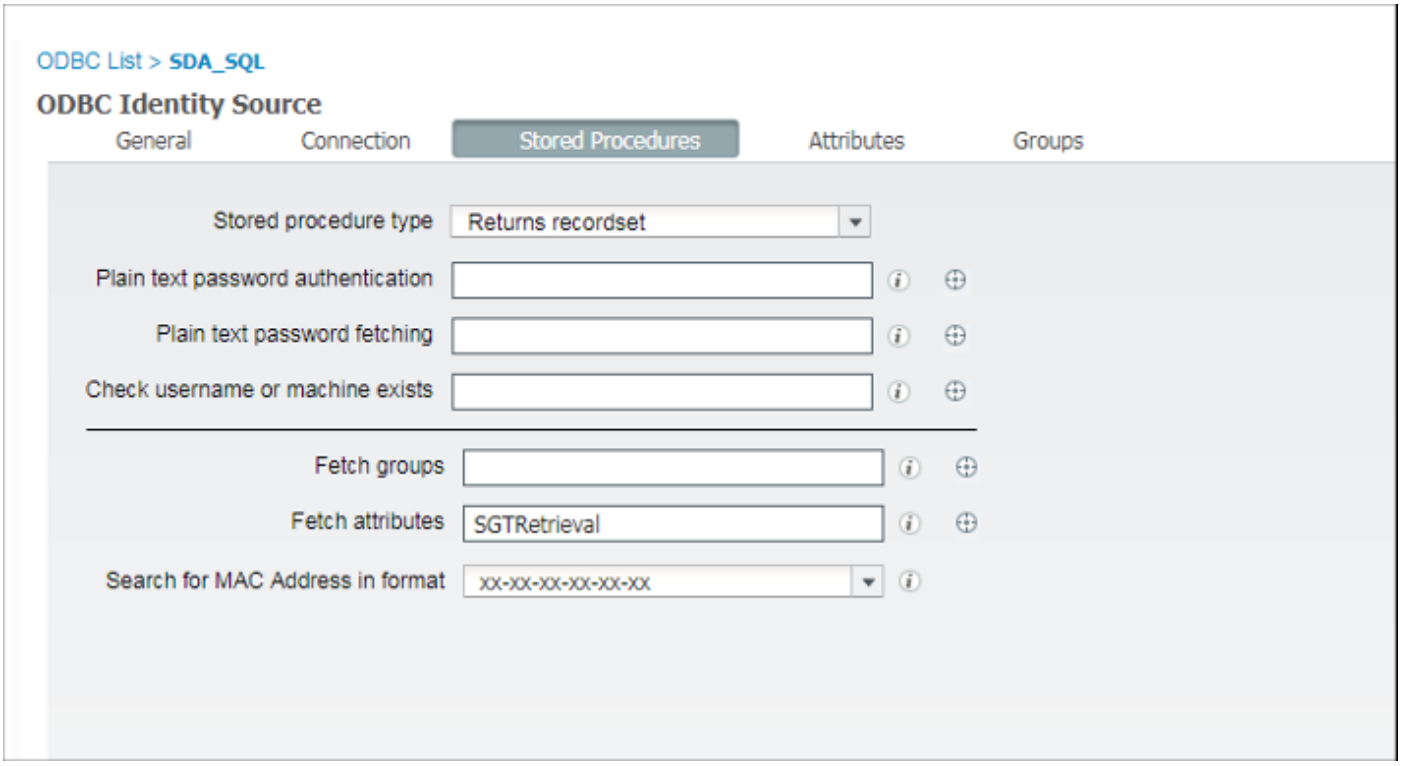
このドキュメントでは、認可ポイントとして使用される外部DBとしてMicrosoft SQLを示します。

ステップ1:Cisco ISEで[Administration] > [External Identity Source] > [ODBC] の順に選択してODBCアイデンティティストアを作成し、接続をテストします。

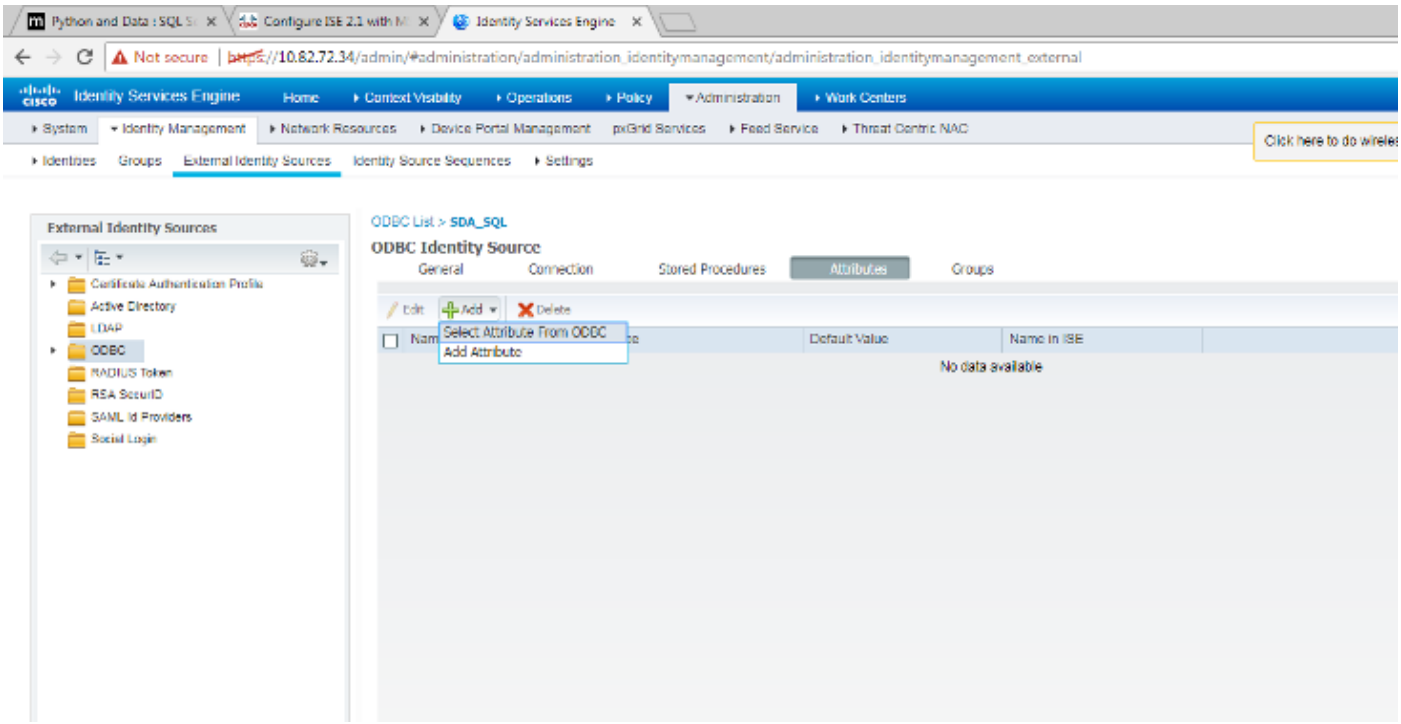


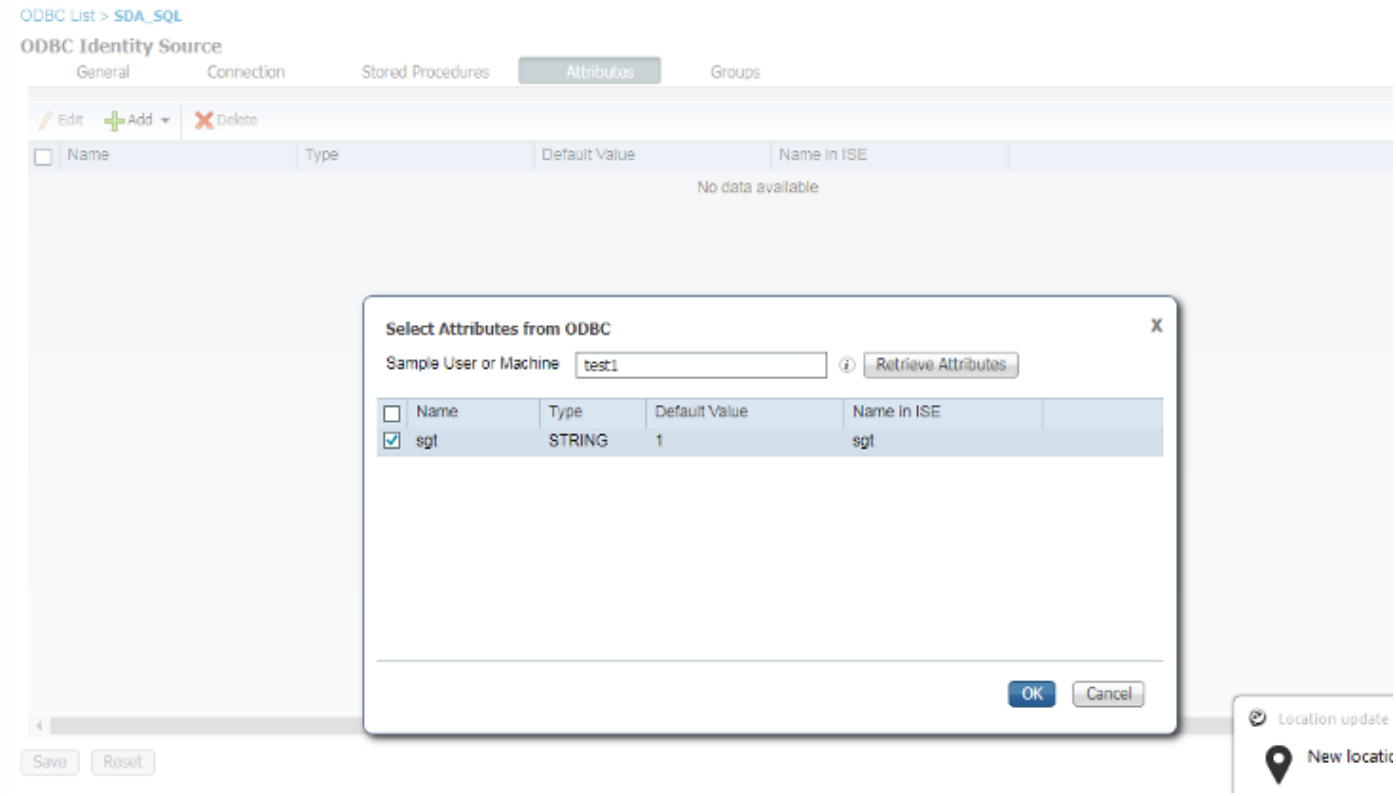


ステップ2:[ODBC]ページの[Stored Procedures]タブに移動し、Cisco ISEで作成したプロシージャを設定します。

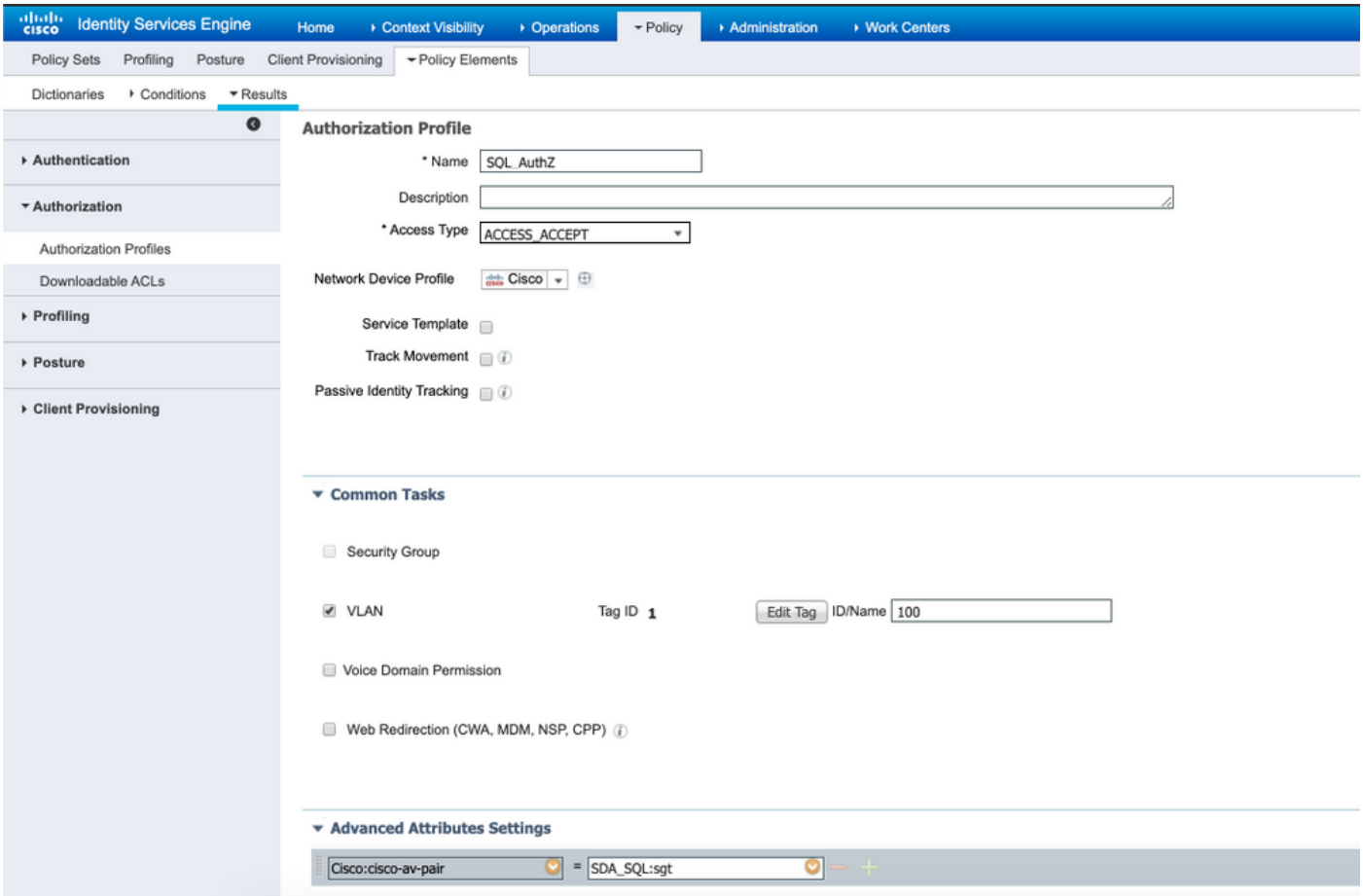


ステップ3：確認のためにODBC IDソースからユーザIDの属性を取得します。

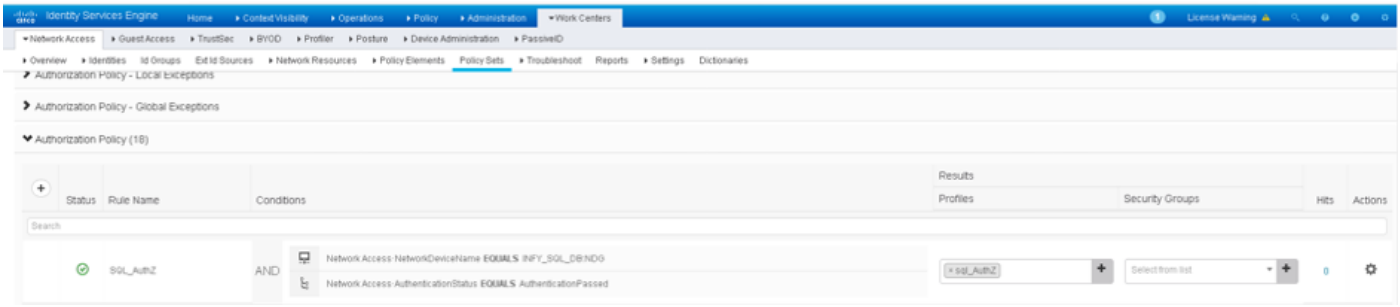




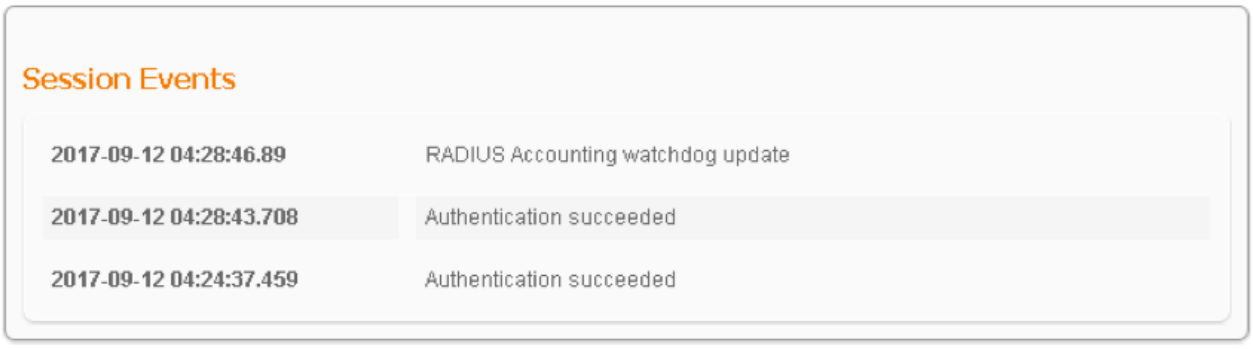
ステップ4:**認可プロファイル**を作成して設定します。Cisco ISEで、[Policy] > [Results] > [Authorization profile] > [Advance Attributes Settings] に移動し、属性として[Cisco:cisco-av-pair]を選択します。<name of ODBC database>:sgtとして値を選択し、保存します。



ステップ5:**認可ポリシー**を作成して設定します。Cisco ISEで、[Policy] > [Policy sets] > [Authorization Policy] > [Add] に移動します。[Identity Source]はSQLサーバなので、条件を入力します。前に作成した認可プロファイルとして結果プロファイルを選択します。



ステップ6：ユーザが認証および許可されると、確認のためにユーザに割り当てられたsgtがログに含まれます。

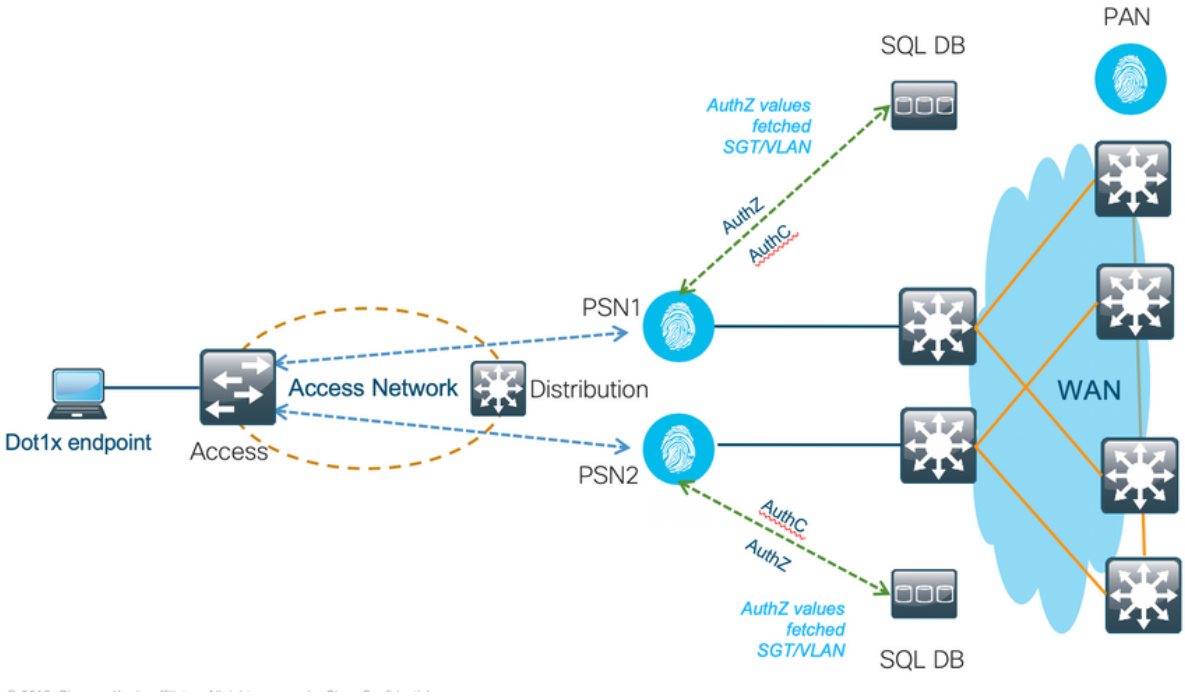


ソリューションワークフロー（ISE 2.7以降）

ISE 2.7以降では、Vlan、SGT、ACLなどのODBCから認可の属性をフェッチでき、これらの属性をポリシーで使用できます。

このソリューションでは、Cisco ISEはMicrosoft SQLと統合されています。MS SQLは、認証と認可のIDストアとして使用されます。エンドポイントからのクレデンシャルがPSNに提供されると、MS SQL DBに対してクレデンシャルが検証されます。認可ポリシーはMS SQL DBを参照して

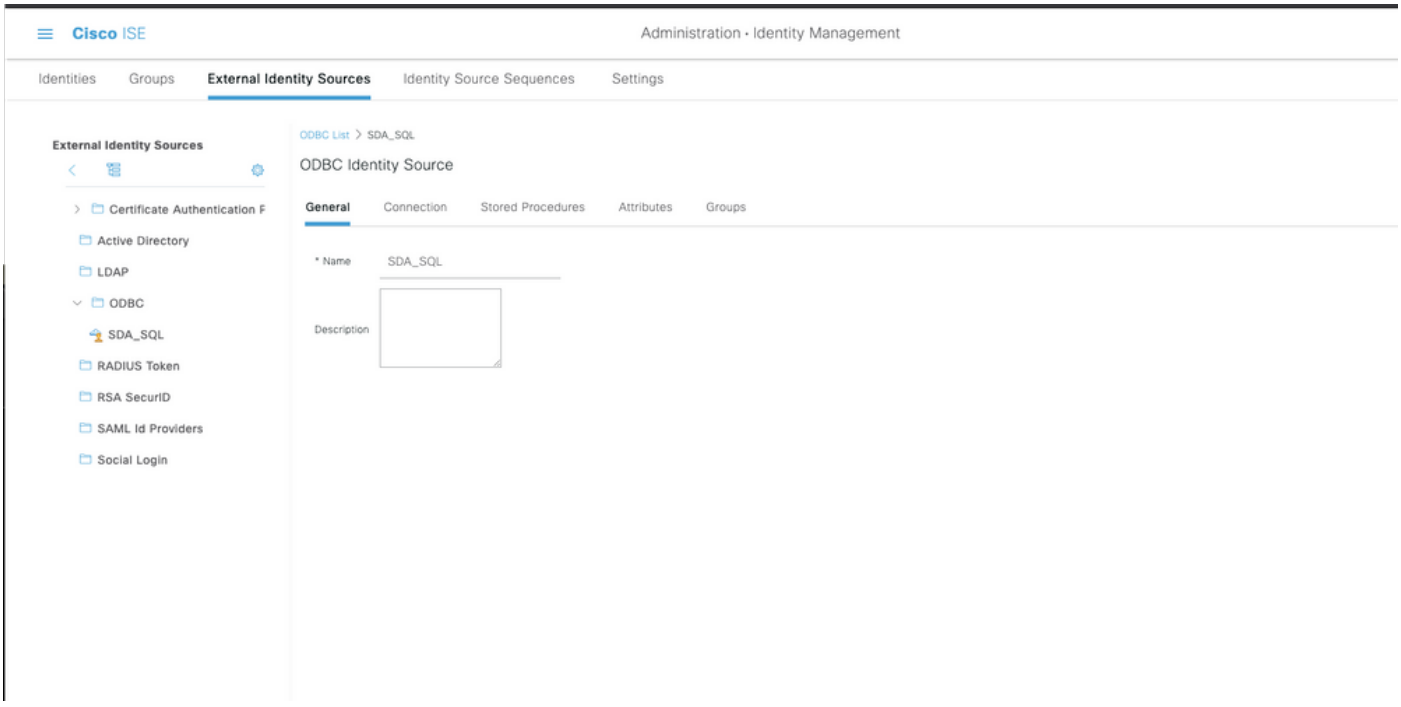
、**user-id**が参照として使用されるSGT/VLANなどの認可された結果をフェッチします。



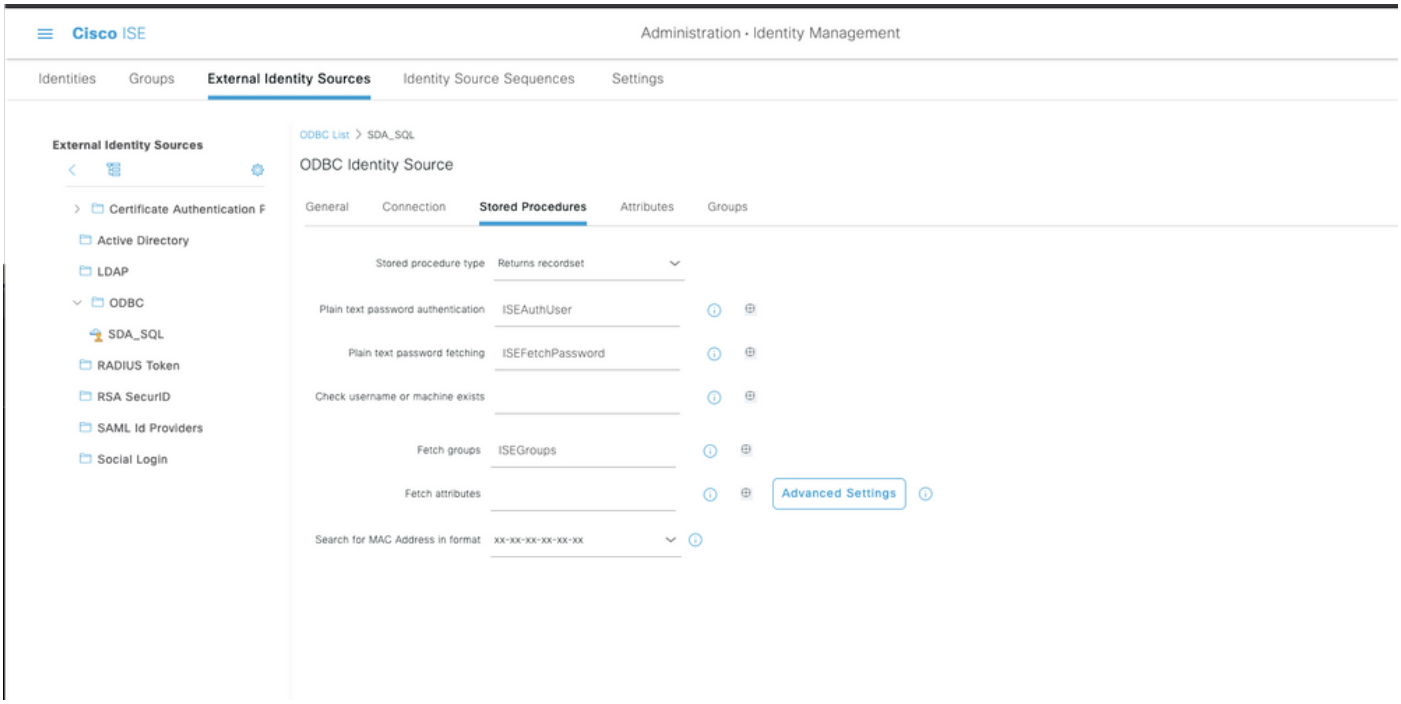
外部DBの設定例

ユーザ名、パスワード、VLAN ID、およびSGTとともにMS SQL DBを作成するには、このドキュメントで前述した手順に従います。

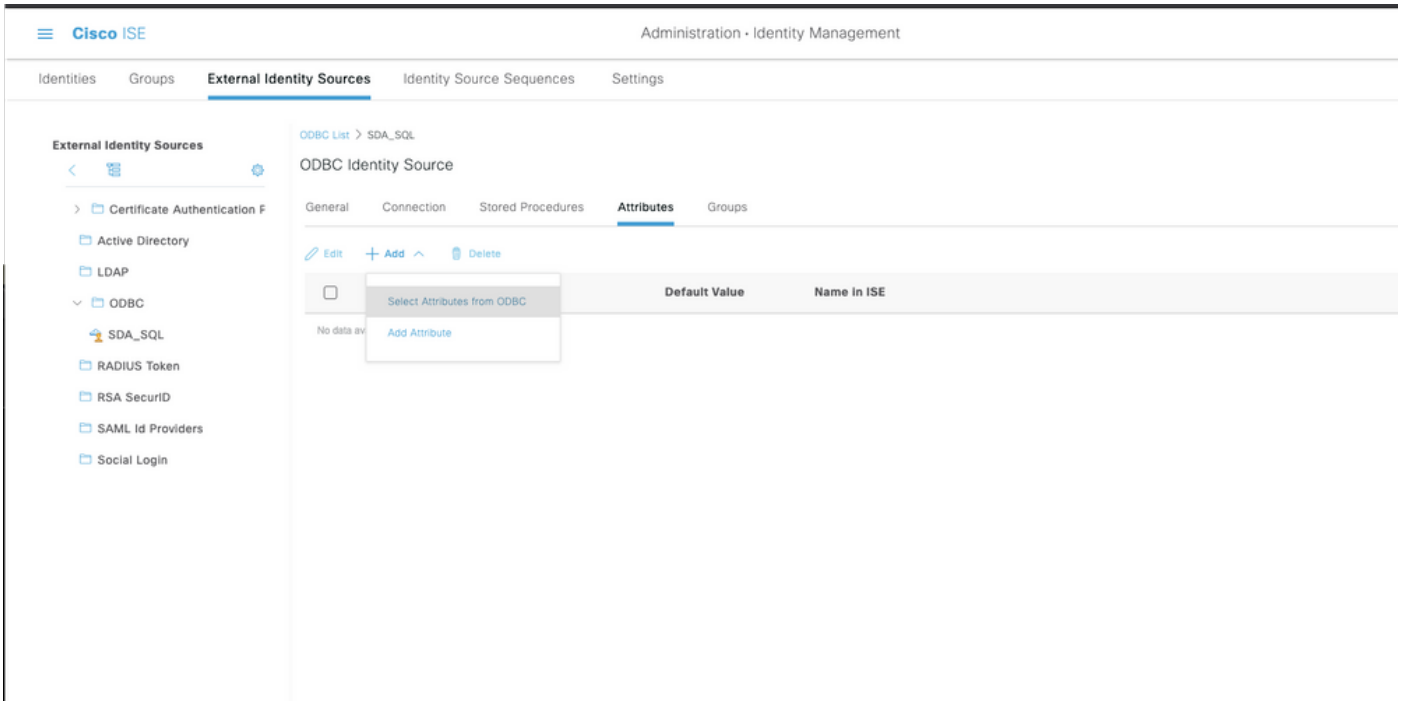
ステップ1:Cisco ISEで[Administration] > [External Identity Source] > [ODBC] の順に選択してODBCアイデンティティストアを作成し、接続をテストします。

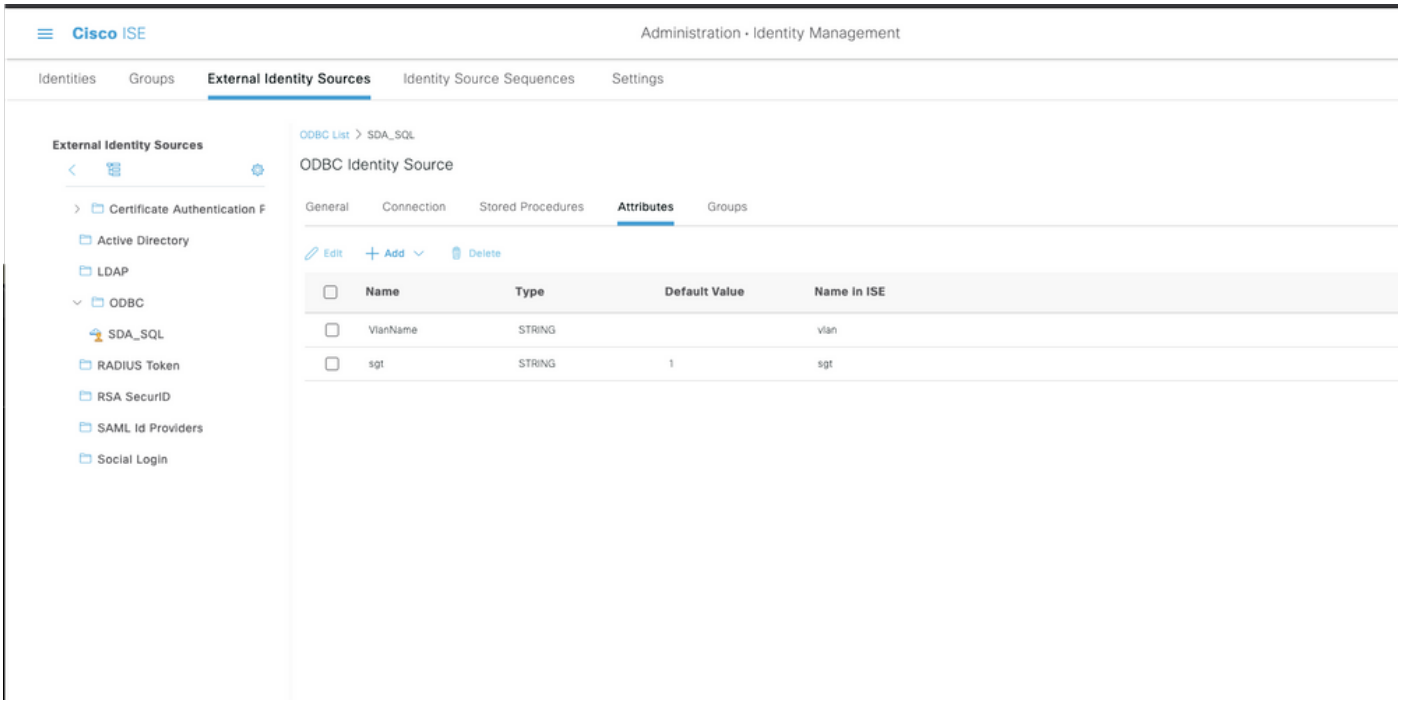


ステップ2:[ODBC]ページの[Stored Procedures]タブに移動し、Cisco ISEで作成したプロシージャを設定します。

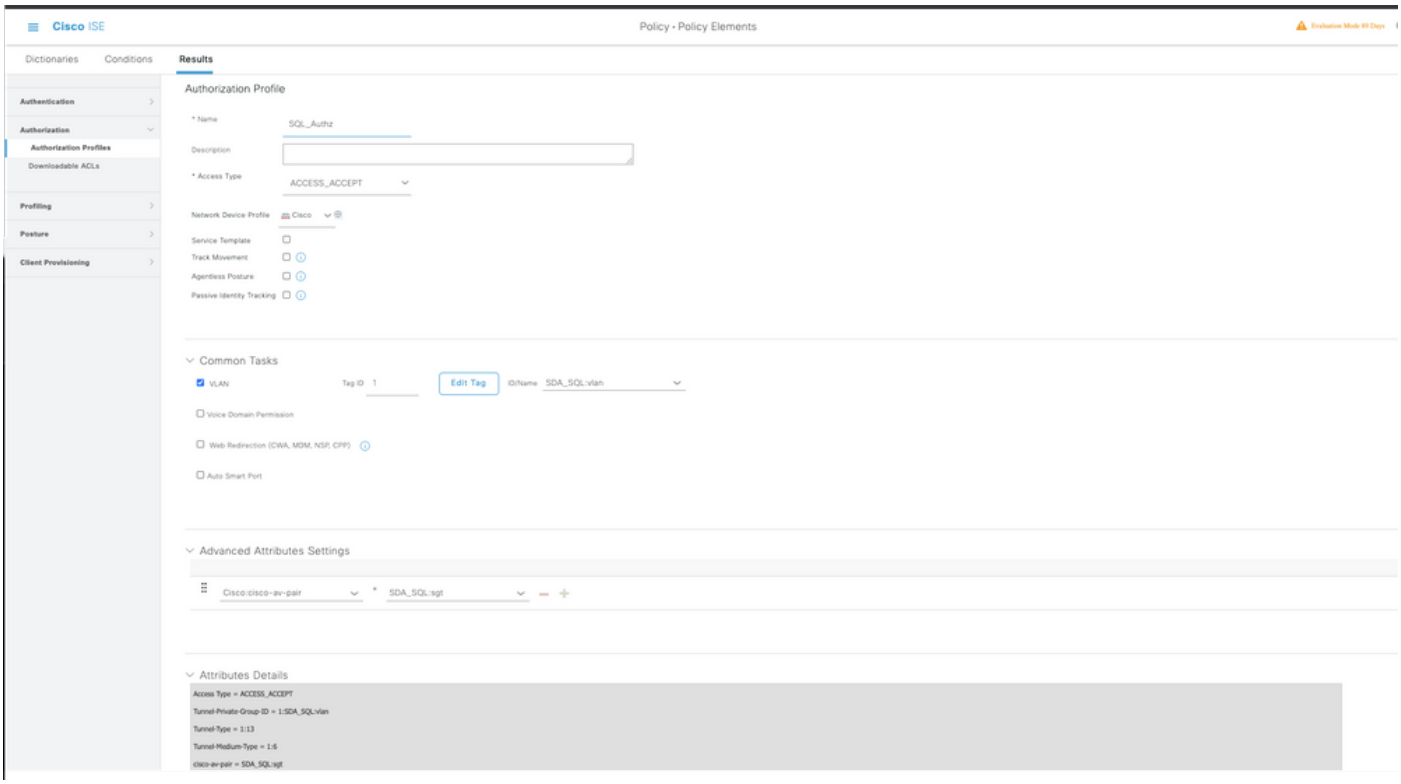


ステップ3：確認のためにODBC IDソースからユーザIDの属性を取得します。

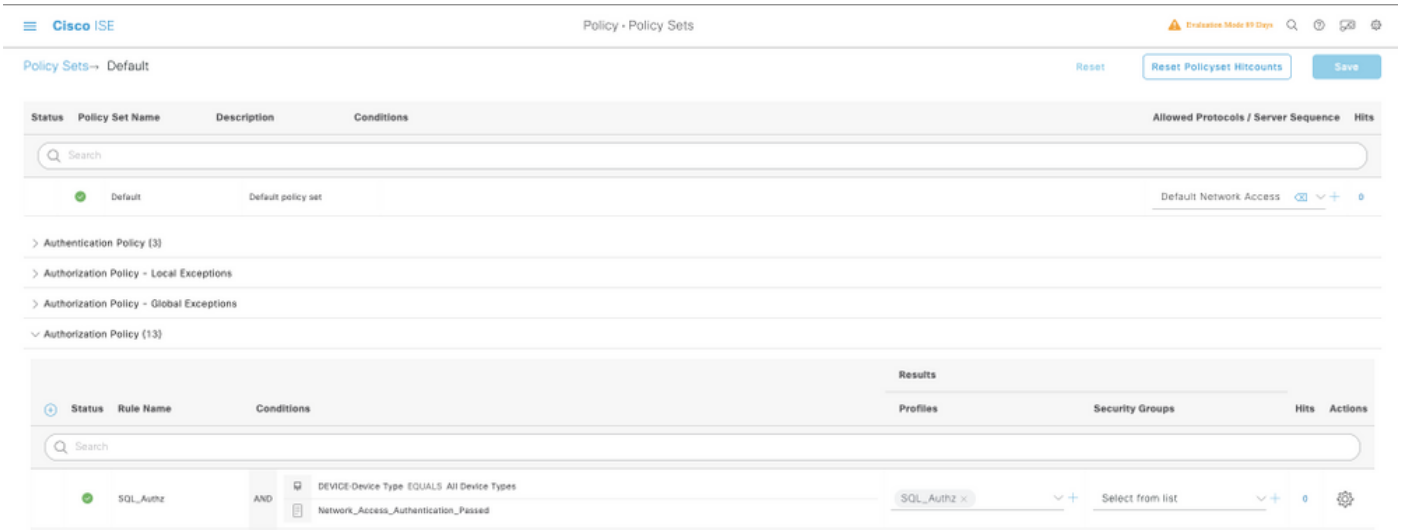




ステップ4:**認可プロファイル**を作成して設定します。Cisco ISEで、[Policy] > [Results] > [Authorization profile] > [Advance Attributes Settings] に移動し、属性として**Cisco:cisco-av-pair**を選択します。値として<name of ODBC database>:sgtを選択します。[Common Tasks]で、**VLAN** with ID/Name as <name of ODBC database>:vlanを選択して保存します



ステップ5:**認可ポリシー**を作成して設定します。Cisco ISEで、[Policy] > [Policy sets] > [Authorization Policy] > [Add] に移動します。[Identity Source]はSQLサーバなので、条件を入力します。前に作成した認可プロファイルとして結果プロファイルを選択します。

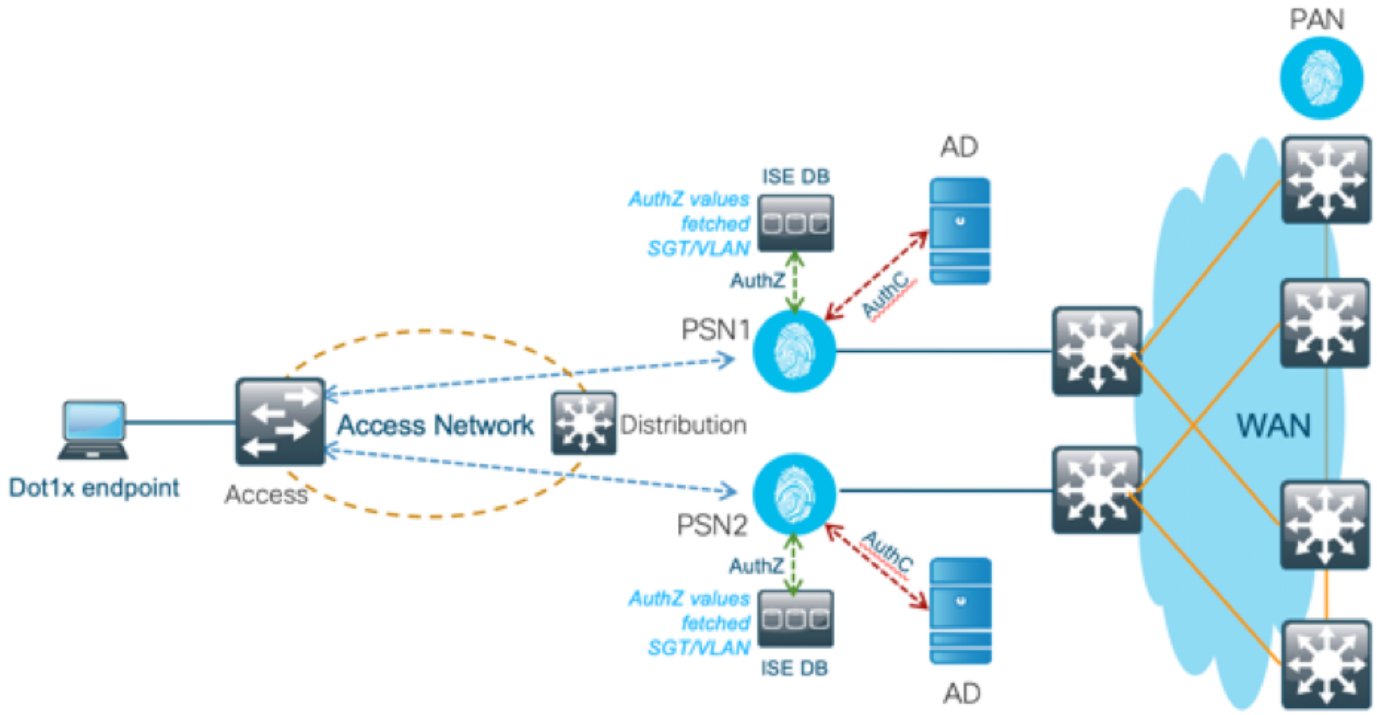


内部DBを使用

Cisco ISE自体には組み込みのDBがあり、これを使用してユーザIDを認証に使用できます。

ソリューションワークフロー

このソリューションでは、Active Directory(AD)が引き続き認証ソースである間、Cisco ISEの内部DBが認証ポイントとして使用されます。エンドポイントのユーザIDは、SGTやVLANなどの承認済みの結果を返す**カスタム属性**とともにCisco ISE DBに含まれます。エンドポイントからのクレデンシャルがPSNに提供されると、エンドポイントのクレデンシャルの有効性がActive Directory IDストアでチェックされ、エンドポイントが認証されます。認可ポリシーは、ISE DBを参照して、ユーザIDが参照として使用されるSGT/VLANなどの認可された結果を取得します。



長所

このソリューションには次のような利点があり、柔軟なソリューションとなっています。

- Cisco ISE DBは組み込み型のソリューションであるため、外部DBソリューションとは異なり、障害の3番目のポイントはありません。
- Cisco ISEクラスタは、すべてのペルソナ間のリアルタイムの同期を保証するため、PSNにはPANからリアルタイムでプッシュされるすべてのユーザIDとカスタム属性が含まれているため、WANの依存関係はありません。
- Cisco ISEは、外部DBが提供するすべての追加機能を活用できます。
- このソリューションは、Cisco ISEのスケール制限には依存しません。

デメリット

このソリューションには、次の短所があります。

- Cisco ISE DBが保留できるユーザIDの最大数は300,000です。
- ユーザIDをDBに手動で設定した場合に発生するエラーを考慮する必要があります。

内部DBの設定例

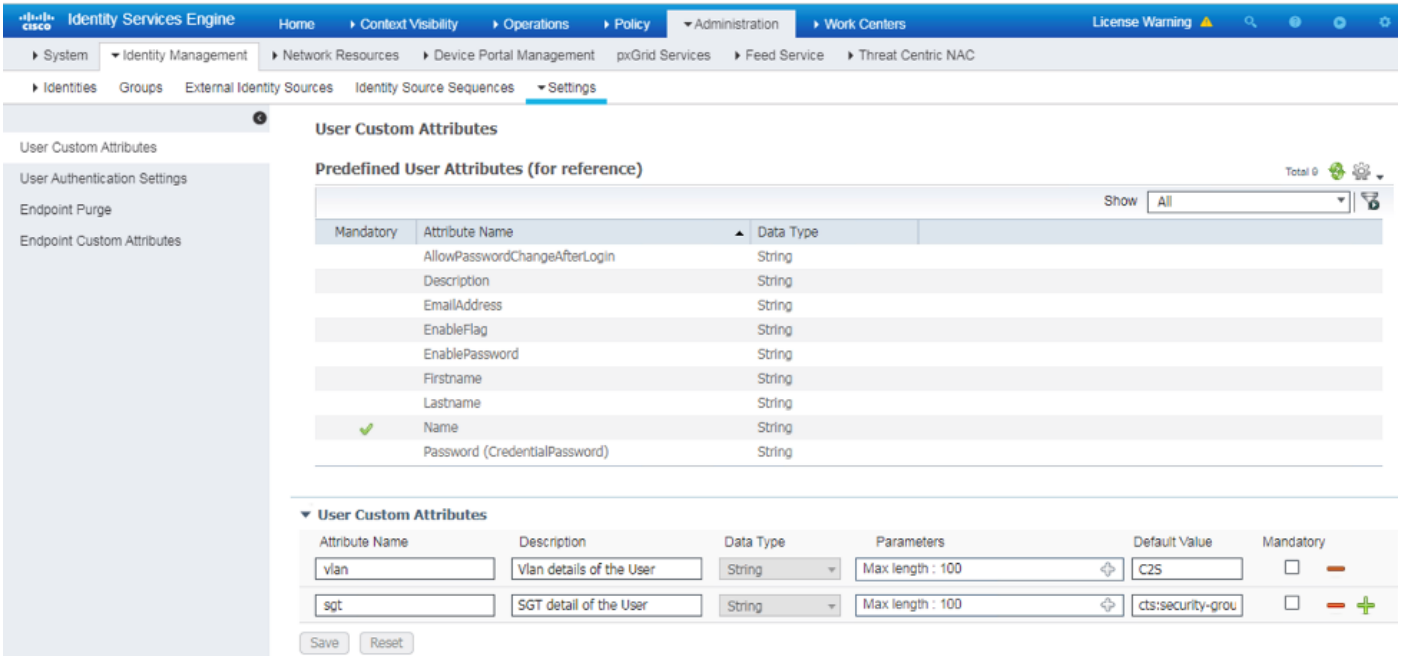
ユーザ単位のVLANおよびSGTは、内部IDストア内の任意のユーザに対して、カスタムユーザ属性を使用して設定できます。

ステップ1:各ユーザのVLANおよびSGT値を表す新しいユーザカスタム属性を作成します。[Administration] > [Identity Management] > [Settings] > [User Custom Attributes] に移動します。次の表に示すように、新しいユーザカスタム属性を作成します。

ここでは、ISE DBテーブルがカスタム属性とともに表示されます。

属性名	データタイプ	パラメータ（長さ）	デフォルト値
VLAN	String	100	C2S（デフォルトのVlan名）
sgt	String	100	cts:security-group-tag=0003-0（デフォルトのSGT値）

- このシナリオでは、VLAN値はVLAN名を表し、sgt値はSGTのcisco-av-pair属性を16進数で表します。

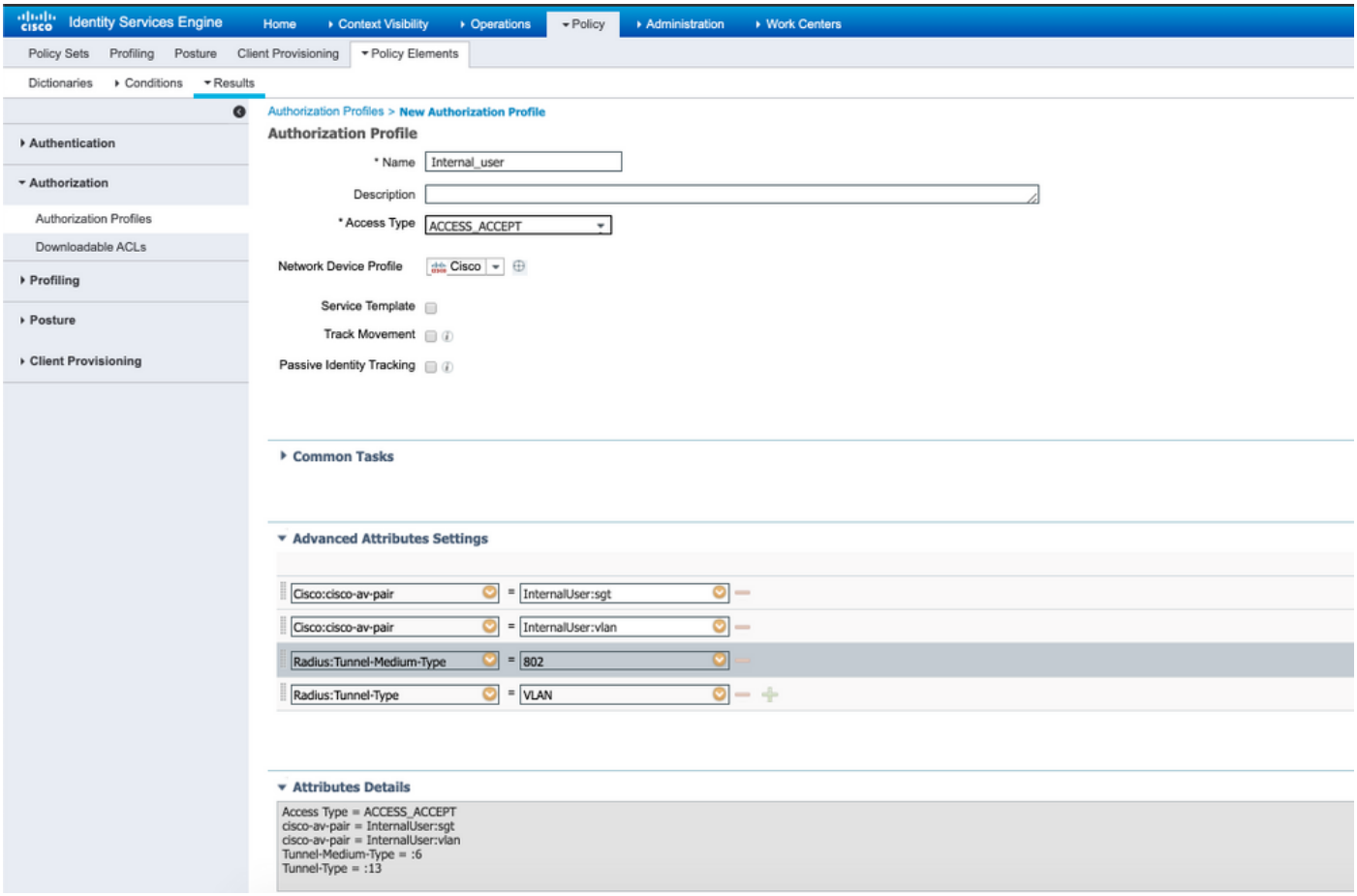


ステップ2:ユーザカスタム属性を使用して認可プロファイルを作成し、各ユーザのvlanおよびsgt値を示します。[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] > [Add] に移動します。[Advanced Attributes Settings]で以下の属性を追加します。

次の表に、内部ユーザのAuthZプロファイルを示します。

属性	**値**
Cisco:cisco-av-pair	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	InternalUser:vlan
Radius:Tunnel-Medium-Type	802
Radius：トンネルタイプ	VLAN

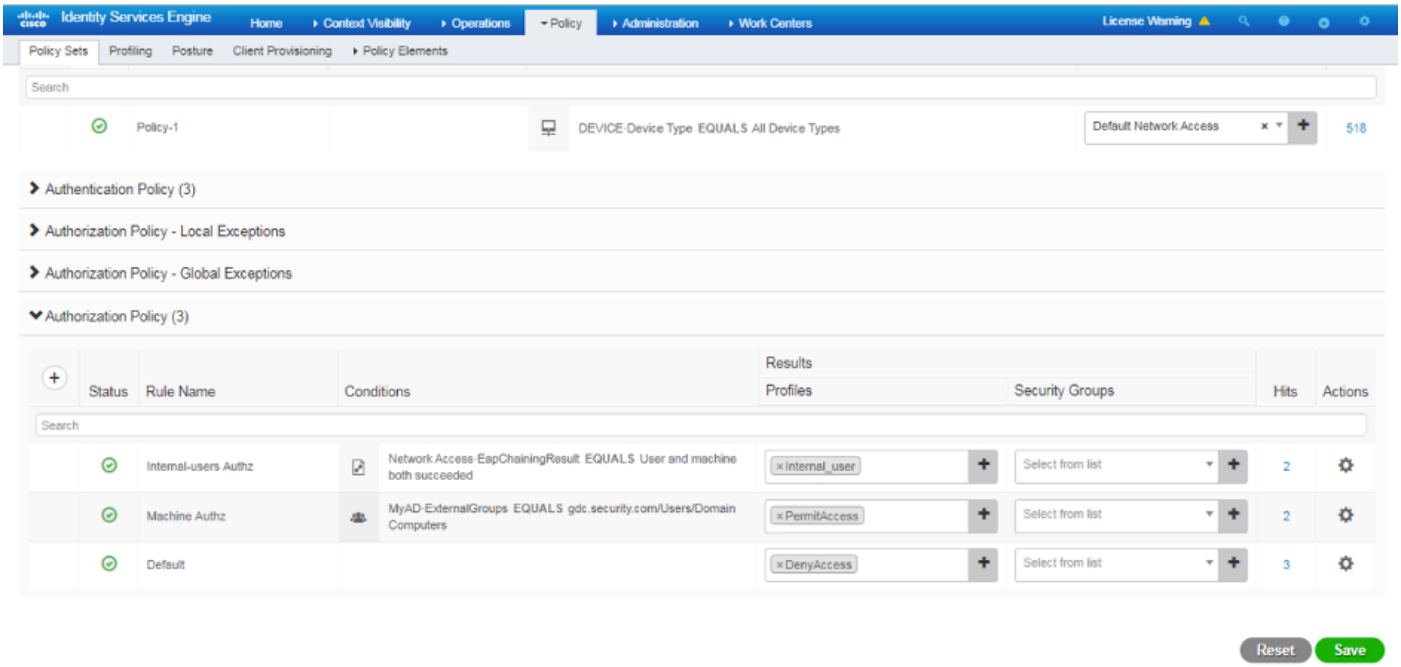
図に示すように、内部ユーザのプロファイル**Internal_user**は、SGTとVLANがそれぞれ**InternalUser:sgt**と**InternalUser:vlan**として設定されて設定されています。



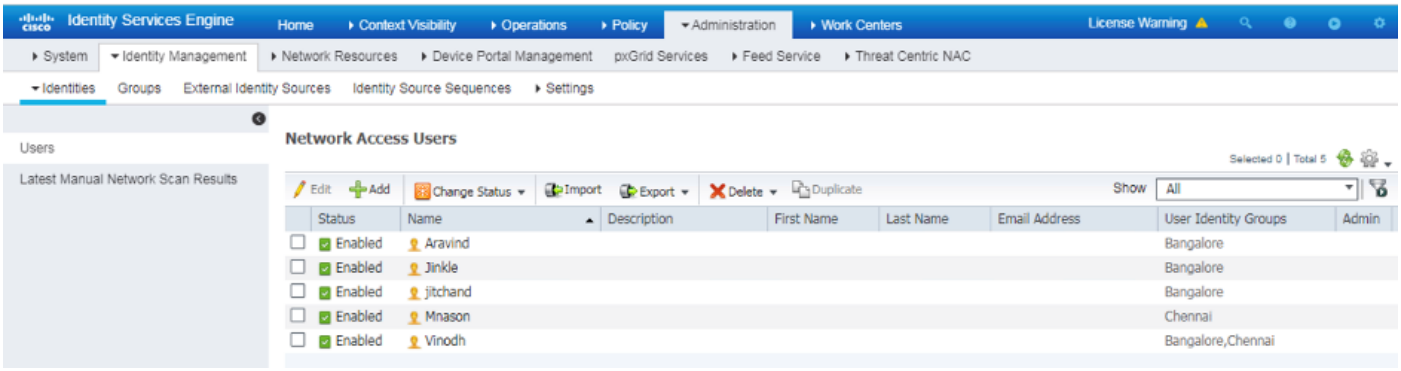
ステップ3:認可ポリシーを作成し、[Policy] > [Policy Sets] > [Policy-1] > [Authorization] に移動します。以下の条件で認可ポリシーを作成し、それぞれの認可プロファイルにマップします。

次の表に、内部ユーザのAuthZポリシーを示します。

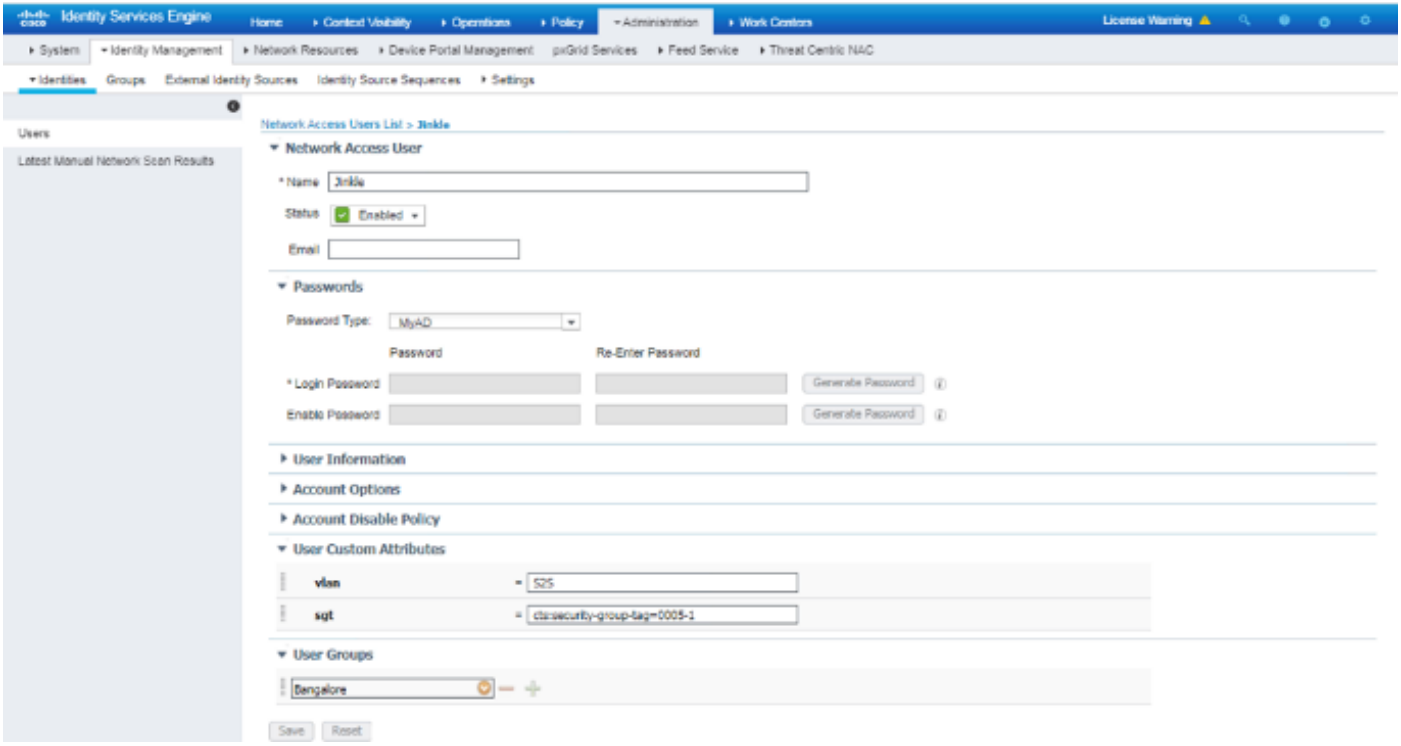
ルール名	条件	結果の認証プロファイル
Internal_User_Authz	Network Access.EapChainingResultsがUserとMachineの両方が成功した場合	Internal_user
Machine_Only_Authz	MyAD.ExternalGroupsがgdc.security.com/Users/Domainコンピュータと等しい場合	PermitAccess



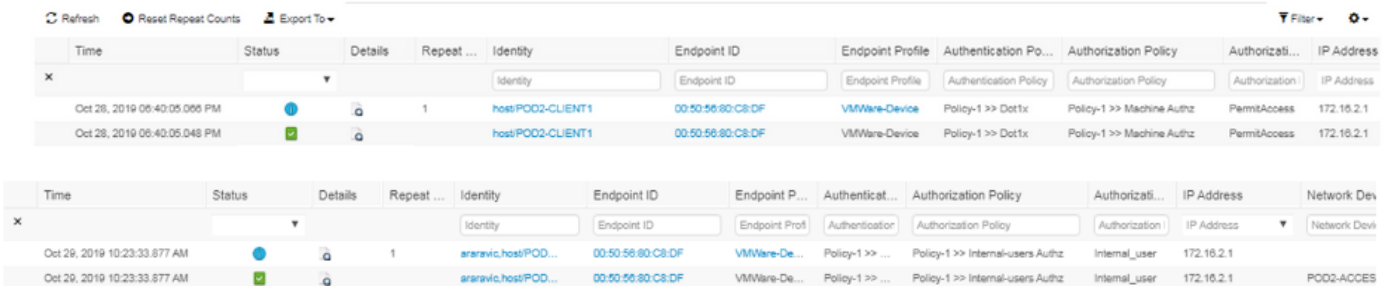
ステップ4：ユーザの詳細とそれぞれのカスタム属性を含むカスタム属性を使用して、一括ユーザIDをcsvテンプレートに作成します。 [Administration] > [Identity Management] > [Identities] > [Users] > [Import] > [Choose the file] > [Import] に移動して、csvをインポートします。



この図は、カスタム属性の詳細を持つサンプルユーザを示しています。ユーザを選択し、[edit]をクリックして、各ユーザにマップされたカスタム属性の詳細を表示します。



ステップ 5：ライブログを確認します。



[Result] セクションをチェックして、**Vlan**および**SGT**属性がAccess-Acceptの一部として送信されているかどうかを確認します。

結論

このソリューションにより、大企業のお客様の一部は、要件に合わせて拡張できます。ユーザIDの追加/削除には注意が必要です。エラーがトリガーされると、正規のユーザが不正アクセスを行ったり、逆の場合に不正アクセスを行う可能性があります。

関連情報

ODBCを介してMS SQLでCisco ISEを設定します。

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

用語集

[AAA]	認証認可アカウンティング
[AD]	Active Directory
認証	[Authentication]
認証Z	許可
DB	データベース
DOT1X	802.1X
IBN	IDベースネットワーク
ID	IDデータベース
ISE	Identity Services Engine
MnT	モニタリングとトラブルシューティング
MsSQL	Microsoft SQL

ODBC	Open DataBase Connectivity
パン	ポリシー管理ノード
PSN	ポリシーサービスノード
SGT	セキュアグループタグ
SQL	構造化照会言語(SQL)
VLAN	Virtual LAN（仮想 LAN）
WAN	ワイドエリアネットワーク

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。