Politique d'accès simplifiée avec ODBC et base de données ISE (attribut personnalisé) pour les réseaux de campus à grande échelle

Contenu

Introduction

Ce document décrit le déploiement de campus à grande échelle sans compromettre ses fonctionnalités et l'application de la sécurité. La solution de sécurité des terminaux de Cisco, Identity Services Engine (ISE), répond à cette exigence en intégrant une source d'identité externe.

Pour les réseaux à grande échelle comportant plus de 50 géolocalisations, plus de 4 000 profils d'utilisateurs différents et 600 000 terminaux ou plus, les solutions IBN traditionnelles doivent être considérées sous un angle différent : plus que de simples fonctionnalités, qu'elles s'adaptent à toutes les fonctionnalités. La solution IBN (Intent-Based Network) dans les réseaux traditionnels à grande échelle d'aujourd'hui nécessite de se concentrer davantage sur l'évolutivité et la facilité de gestion, et pas seulement sur ses fonctionnalités.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

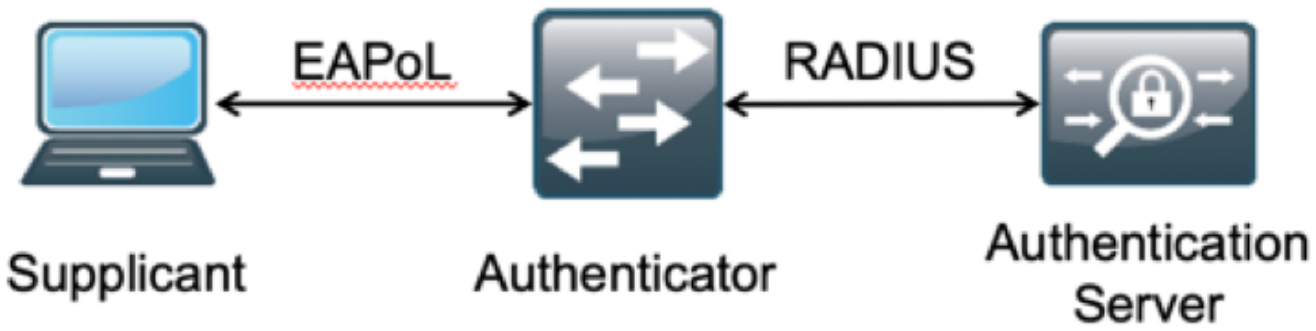
- Cisco Identity Services Engine (ISE) version 2.6, correctif 2 et version 3.0
- Windows Active Directory (AD) Server 2008 version 2
- Microsoft SQL Server 2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si le réseau est actif, assurez-vous de comprendre l'impact potentiel de toute configuration.

Informations générales

Dans une solution de réseau basé sur l'identité (IBN), les éléments de base sont le demandeur, l'authentificateur et le serveur d'authentification (AAA). Le demandeur est un agent sur le terminal qui fournit les informations d'identification lorsqu'il est sollicité pour l'accès au réseau. Authenticator ou NAS (Network Access Server) est la couche d'accès, qui comprend les commutateurs réseau et les WLC qui transportent les informations d'identification vers le serveur AAA. Le serveur d'authentification valide la demande d'authentification utilisateur par rapport à un magasin d'ID et l'autorise avec un access-accept ou un access-reject. Le magasin d'ID peut se trouver sur le serveur AAA ou sur un serveur dédié externe.

Cette image présente les éléments IBN de base.



RADIUS est un protocole basé sur le protocole UDP (User Datagram Protocol) avec authentification et autorisation couplées. Dans la solution IBN de Cisco pour campus d'entreprise, le personnage PSN (Policy Service Node) d'ISE agit en tant que serveur AAA qui authentifie les

terminaux par rapport à l'ID Store d'entreprise et autorise en fonction d'une condition.

Dans Cisco ISE, les stratégies d'authentification et d'autorisation sont configurées pour répondre à ces exigences. Les stratégies d'authentification comprennent le type de support, filaire ou sans fil, et les protocoles EAP pour la validation utilisateur. Les politiques d'autorisation sont constituées de conditions qui définissent les critères de correspondance des différents terminaux et les résultats d'accès au réseau, qui peuvent être un VLAN, une liste de contrôle d'accès téléchargeable ou une balise de groupe sécurisé (SGT). Il s'agit des valeurs d'échelle maximales pour les politiques avec lesquelles ISE peut être configuré.

Ce tableau présente l'échelle des politiques Cisco ISE.

Attribut	Numéro d'échelle
Nombre maximal de règles d'authentification	1000 (mode Jeu de stratégies)
Nombre maximal de règles d'autorisation	3 000 (mode Jeu de stratégies) avec 3 200 profils Authz

Tendances technologiques

La segmentation est devenue l'un des principaux éléments de sécurité pour les réseaux d'entreprise actuels, sans qu'il soit nécessaire de mettre en place un véritable réseau de périphérie. Les terminaux sont autorisés à circuler entre les réseaux internes et externes. La segmentation permet de contenir toute attaque de sécurité sur un segment particulier afin de l'étendre au réseau. La solution Software-Defined Access (SDA) d'aujourd'hui, avec l'aide de TrustSec de Cisco ISE, permet de segmenter en fonction du modèle commercial du client afin d'éviter les dépendances sur des éléments de réseau tels que les VLAN ou les sous-réseaux IP.

Problème

Configuration des politiques ISE pour les réseaux d'entreprise à grande échelle avec plus de 500 profils de terminaux différents, le nombre de politiques d'autorisation peut augmenter jusqu'à un point ingérable. Même si Cisco ISE prend en charge des conditions d'autorisation dédiées pour répondre à un tel volume de profils utilisateur, la gestion de ce grand nombre de politiques par les administrateurs pose un défi.

En outre, les clients peuvent avoir besoin de politiques d'autorisation communes plutôt que de politiques dédiées pour éviter les frais de gestion et disposer d'un accès réseau différencié pour les terminaux en fonction de leurs critères.

Par exemple, considérez un réseau d'entreprise avec Active Directory (AD) comme **source de vérité** et le différenciateur unique du terminal est l'un des attributs dans AD. Dans ce cas, la méthode traditionnelle de configuration des stratégies comporte davantage de stratégies d'autorisation pour chaque profil de point de terminaison unique.

Dans cette méthode, chaque profil de point de terminaison est distingué avec un attribut AD sous domain.com. Par conséquent, une stratégie d'autorisation dédiée doit être configurée.

Ce tableau présente les stratégies AuthZ traditionnelles.

Politique ABC	Si AnyConnect est égal à User-AND-Machine-Both-Passed ET Si Groupe AD EST ÉGAL À domain.com/groups/ABC ALORS SGT:C2S-ABC ET VLAN:1021
politique d'aide aux pays en développement	Si AnyConnect est égal à User-AND-Machine-Both-Passed ET Si Groupe AD EST ÉGAL À domain.com/groups/DEF ALORS SGT:C2S-DEF ET VLAN:1022
Politique GHI	Si AnyConnect est égal à User-AND-Machine-Both-Passed ET Si Groupe AD EST ÉGAL À domain.com/groups/GHI ALORS SGT:C2S-GHI ET VLAN:1023
Politique XYZ	Si AnyConnect est égal à User-AND-Machine-Both-Passed ET Si Groupe AD EST ÉGAL À domain.com/groups/XYZ ALORS SGT:C2S-XYZ ET VLAN:1024

Solution proposée

Pour contourner la violation du nombre maximal évolutif de politiques d'autorisation prises en charge sur Cisco ISE, la solution proposée consiste à utiliser une base de données externe qui autorise chaque terminal avec le résultat d'autorisation extrait de ses attributs. Par exemple, si AD est utilisé en tant que base de données externe pour l'autorisation, tous les attributs utilisateur inutilisés (comme le service ou le code PIN) peuvent être référencés pour fournir des résultats autorisés mappés avec SGT ou VLAN.

Cela est possible grâce à l'intégration de Cisco ISE avec une base de données externe ou dans la base de données interne d'ISE configurée avec des attributs personnalisés. Cette section explique le déploiement de ces 2 scénarios :

> **Note**: Dans les deux options, la base de données contient l'**ID utilisateur** mais pas le **mot de passe** des points d'extrémité DOT1X. La base de données est utilisée comme point d'**autorisation** uniquement. L'authentification peut toujours être le magasin d'ID du client qui, dans la plupart des cas, réside sur le serveur Active Directory (AD).

Configuration avec la base de données externe

Cisco ISE est intégré à une base de données externe pour la validation des identifiants de terminal :

Ce tableau présente les sources d'identité externe validées.

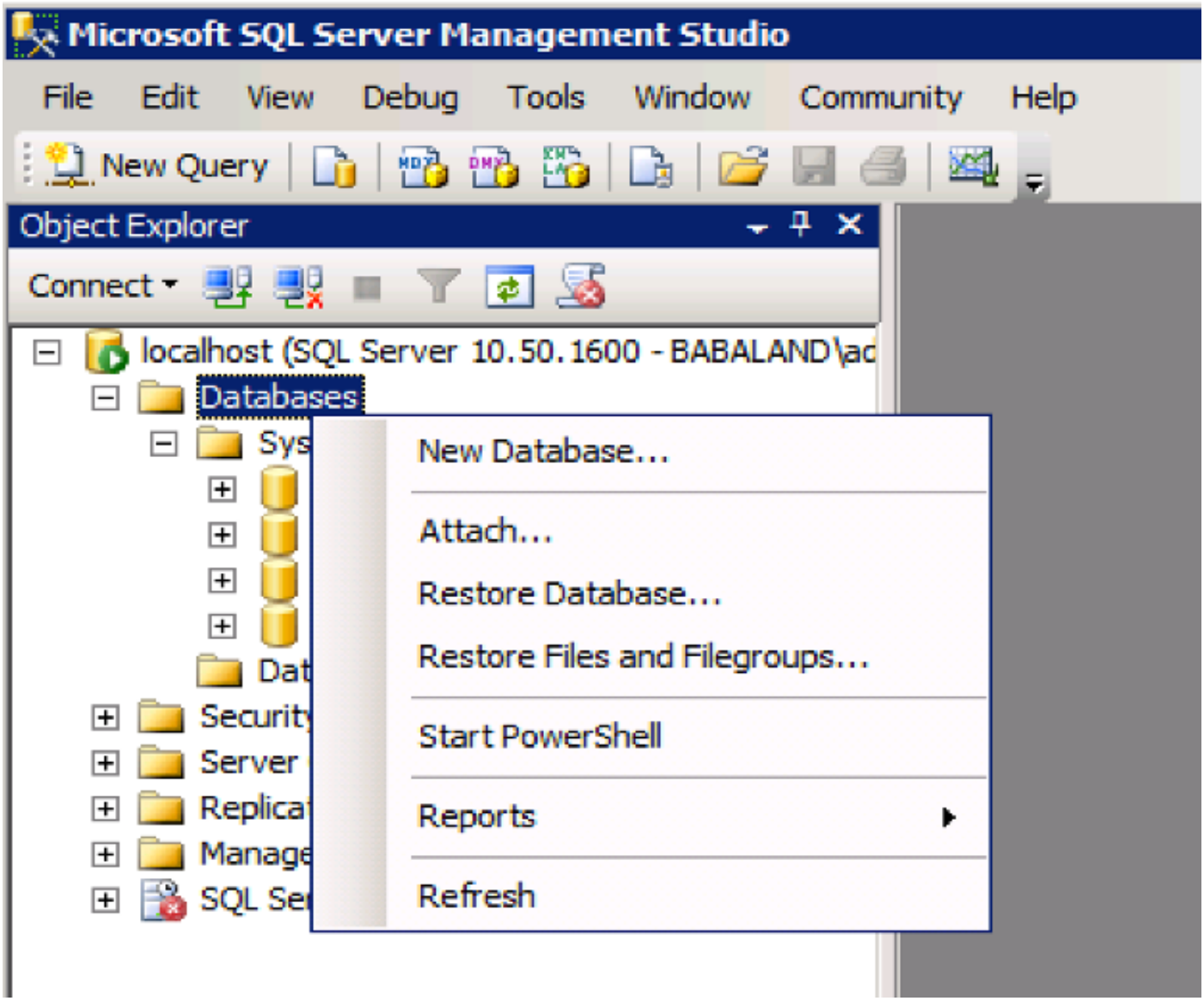
Source d'identité externe	OS/Version
Active Directory	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—

Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—
Serveurs LDAP	
Serveur d'annuaire LDAP SunONE	Version 5.2
Serveur d'annuaire OpenLDAP	Version 2.4.23
Tout serveur compatible LDAP v3	—
Serveurs de jetons	
RSA ACE/Server	Série 6.x
RSA Authentication Manager	Séries 7.x et 8.x
Tout serveur de jeton compatible RADIUS RFC 2865	—
Authentification unique (SSO) SAML (Security Assertion Markup Language)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
Serveur PingFederate	Version 6.10.0.4
Cloud PingOne	—
Authentification sécurisée	8.1.1
Tout fournisseur d'identité conforme à SAMLv2	—
Source d'identité ODBC (Open Database Connectivity)	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition version 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Connexion sociale (pour les comptes d'utilisateurs invités)	
Facebook	—

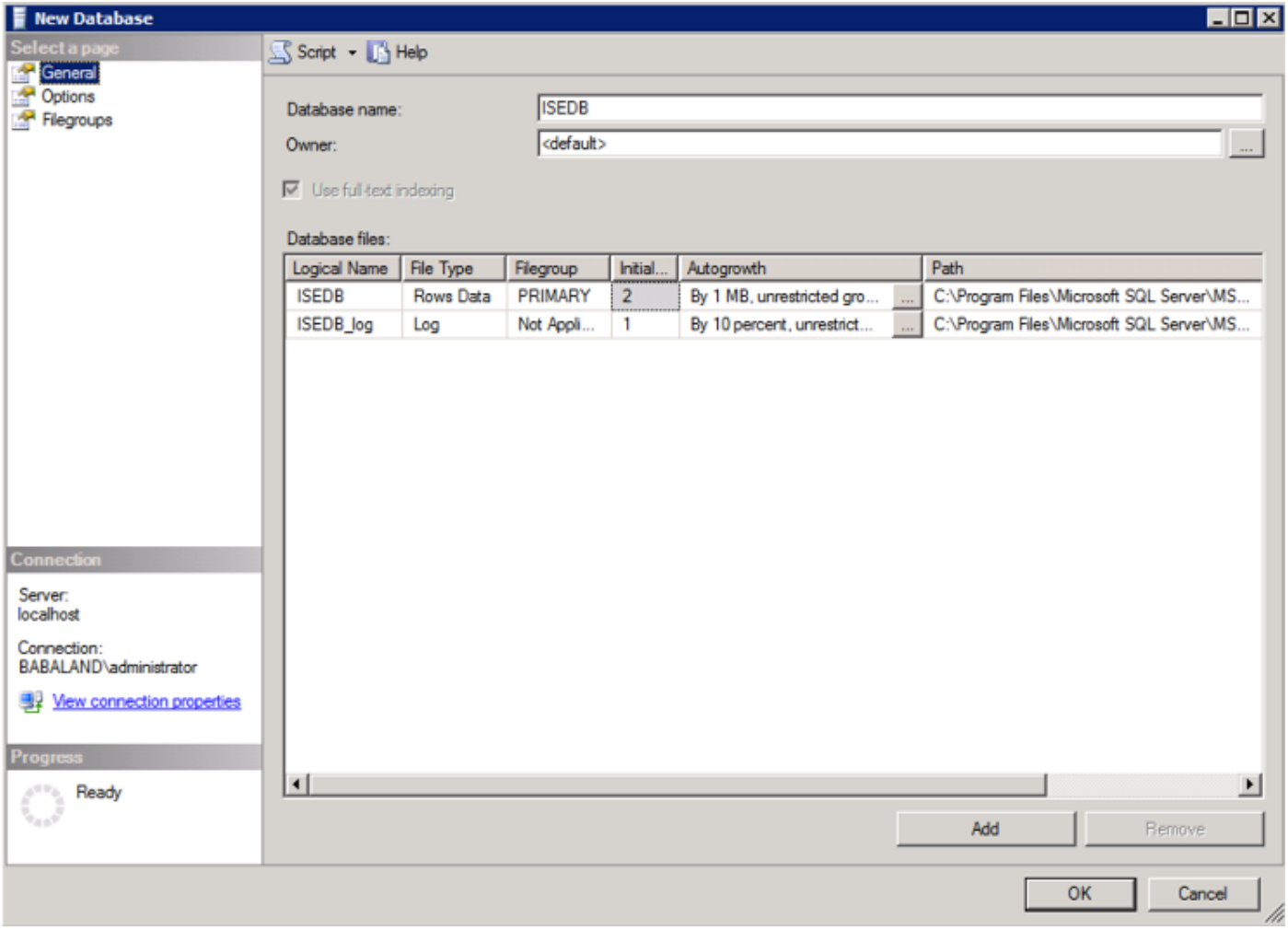
Exemples de configuration ODBC

Cette configuration est effectuée sur Microsoft SQL pour créer la solution :

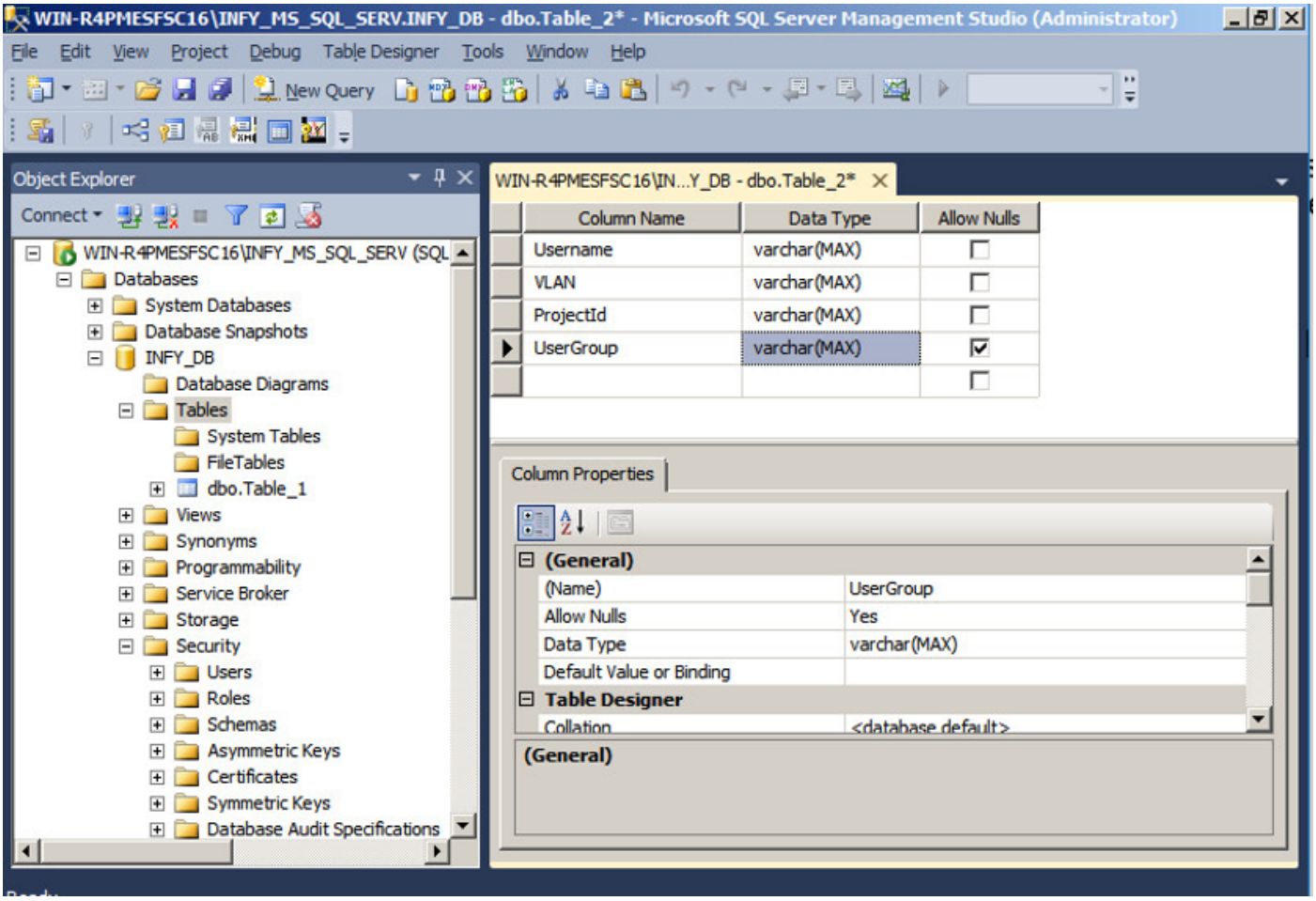
Étape 1. Ouvrez SQL Server Management Studio (**menu Démarrer > Microsoft SQL Server**) pour créer une base de données :



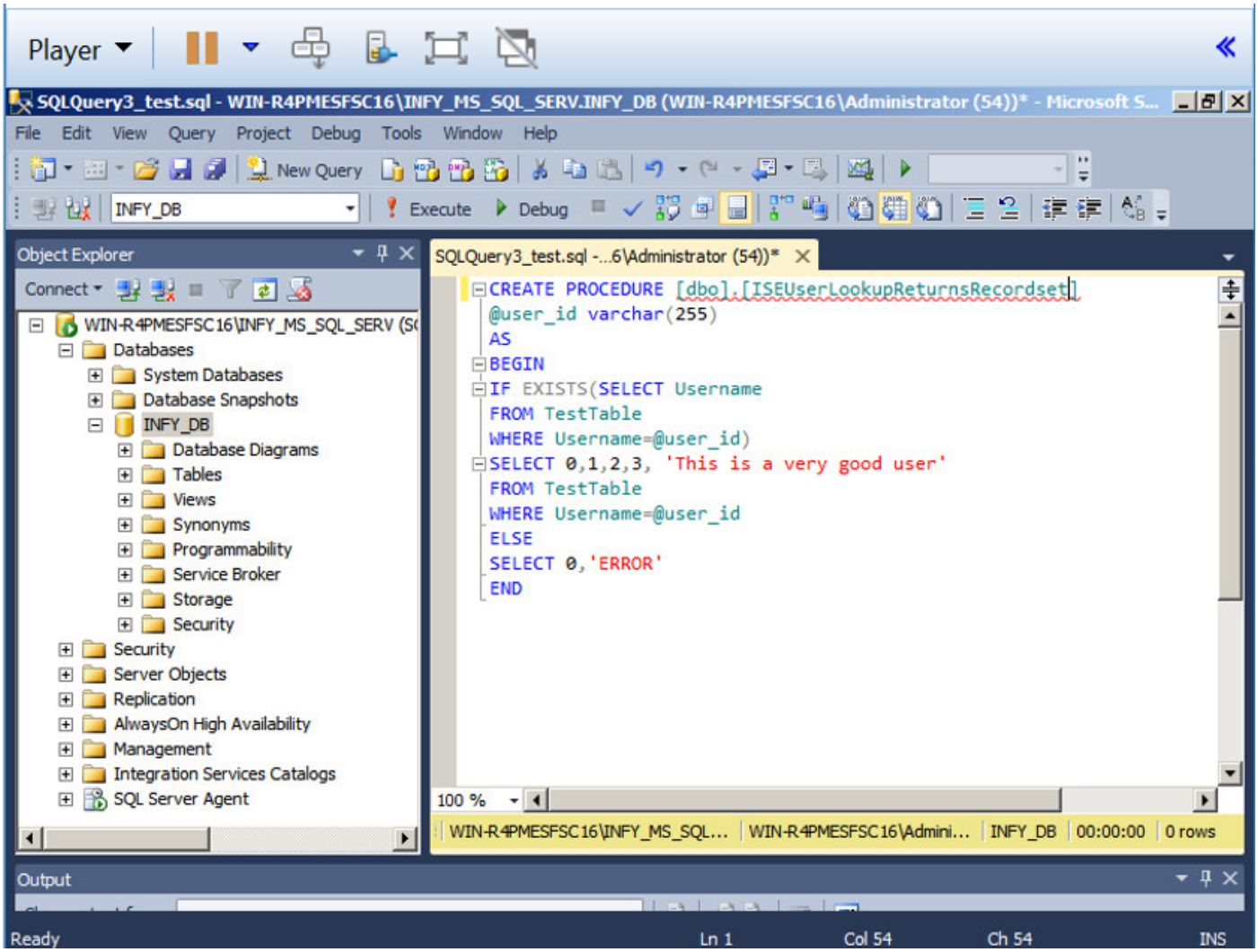
Étape 2. Entrez un nom et créez la base de données.



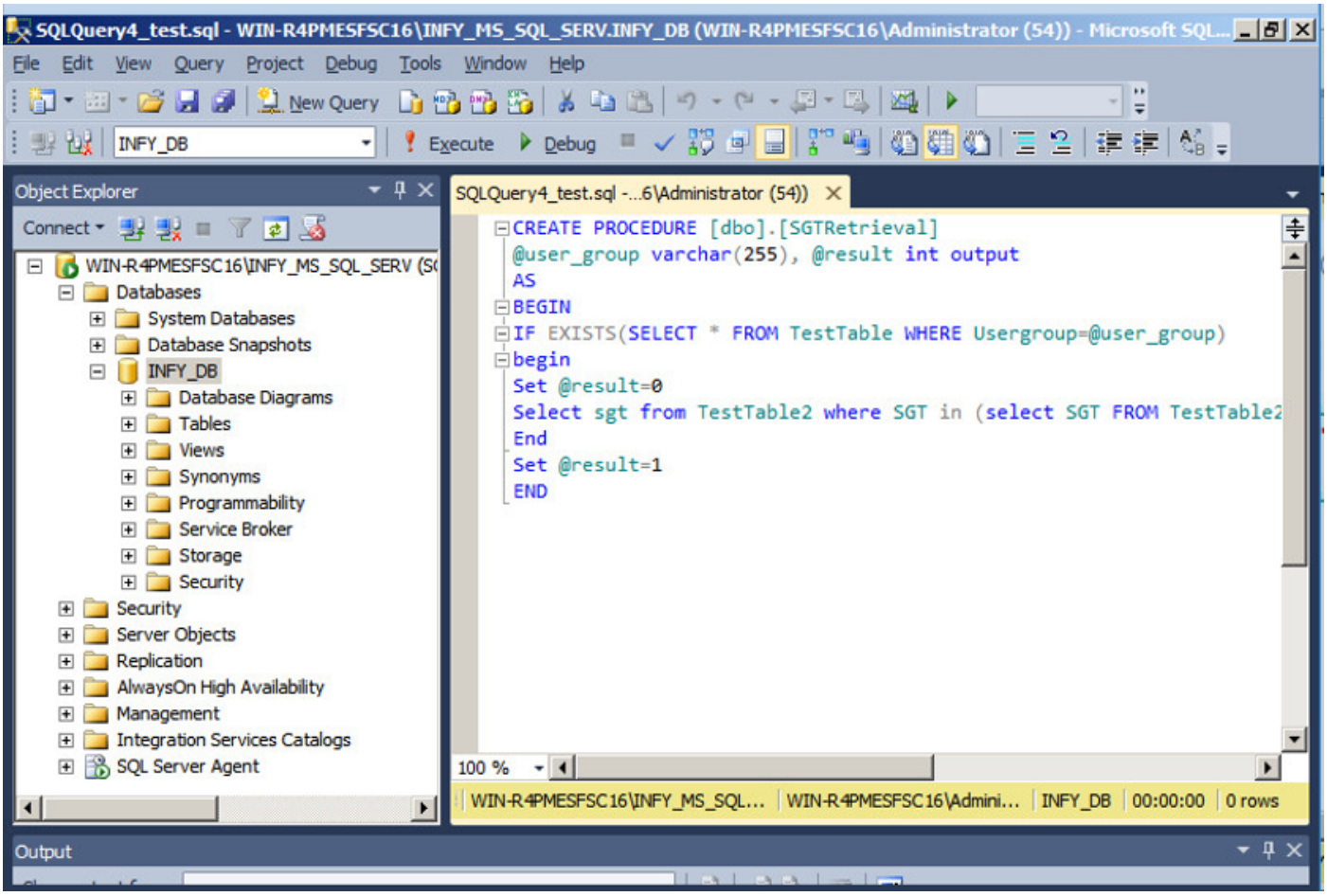
Étape 3 : création d’une table avec les colonnes requises comme paramètres pour les points de terminaison autorisés



Étape 4. Créez une **procédure** pour vérifier si le nom d'utilisateur existe.



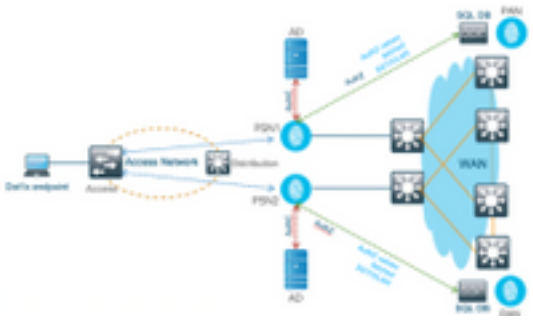
Étape 5. Créez une procédure pour extraire des attributs (SGT) de la table.

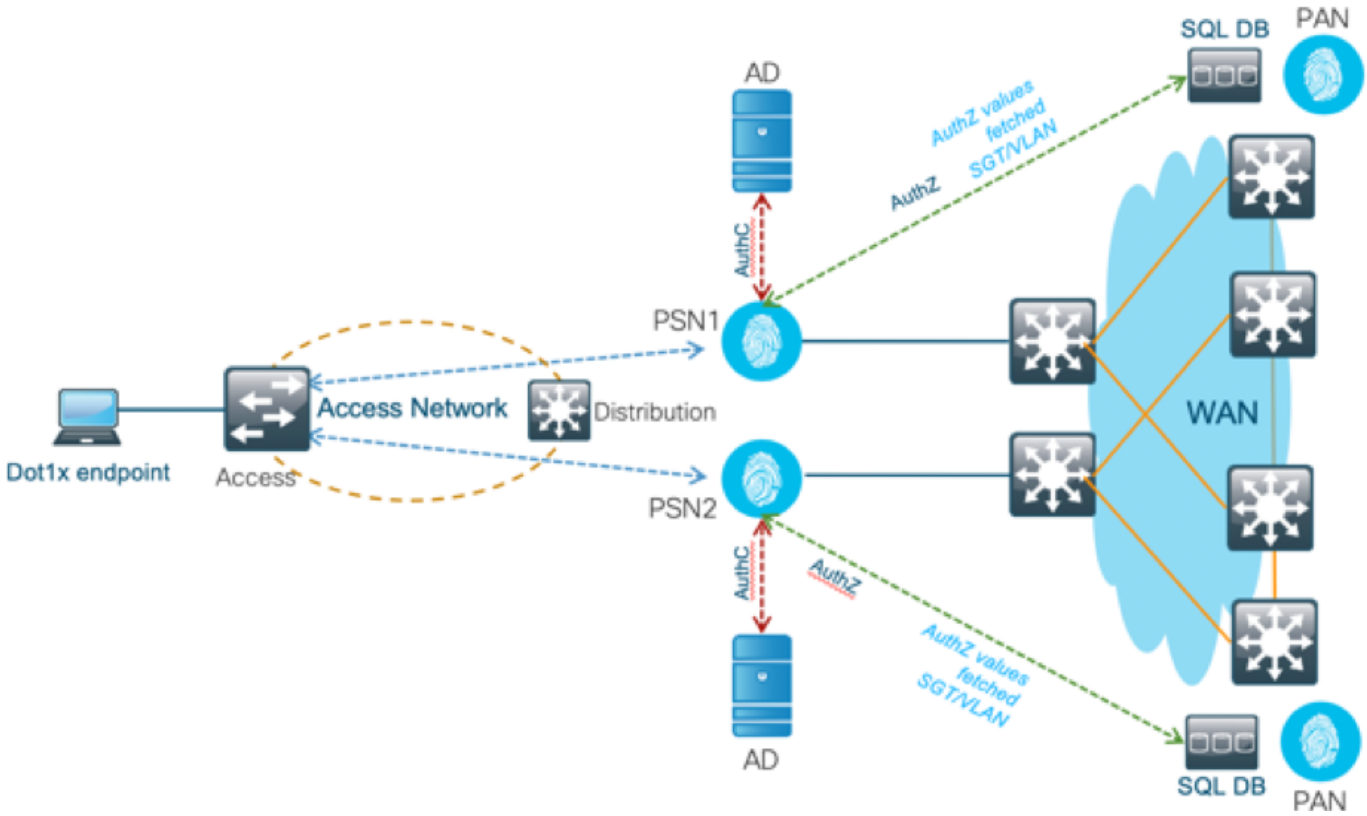


Dans ce document, Cisco ISE est intégré à la solution Microsoft SQL pour répondre aux exigences d'évolutivité des autorisations sur les réseaux de grandes entreprises.

Workflow de la solution (ISE 2.7 et versions antérieures)

Dans cette solution, Cisco ISE est intégré à Active Directory (AD) et Microsoft SQL. AD est utilisé comme magasin d'ID d'authentification et MS SQL pour l'autorisation. Au cours du processus d'authentification, le périphérique d'accès réseau (NAD) transmet les informations d'identification de l'utilisateur au PSN, le serveur AAA de la solution IBN. PSN valide les informations d'identification du point de terminaison avec le magasin d'ID Active Directory et authentifie l'utilisateur. La politique d'autorisation se réfère à la base de données MS SQL pour récupérer les résultats autorisés comme SGT / VLAN pour lequel **user-id** est utilisé comme référence.





Avantages

Cette solution présente les avantages suivants, ce qui la rend flexible :

- Cisco ISE peut tirer parti de toutes les fonctionnalités supplémentaires que la base de données externe peut offrir.
- Cette solution ne dépend d'aucune limite d'évolutivité Cisco ISE.

Inconvénients

Cette solution présente les inconvénients suivants :

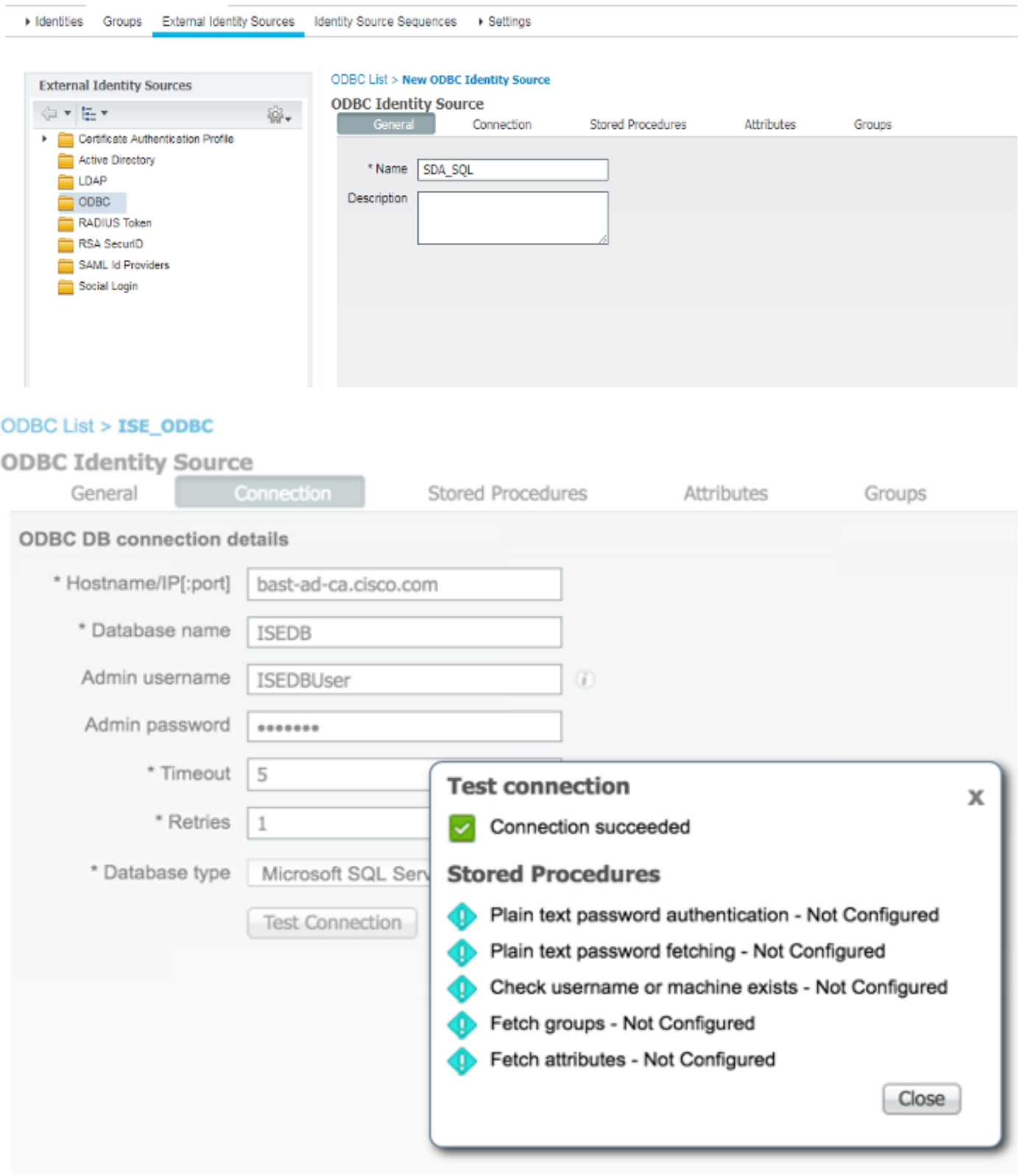
- Nécessite une programmation supplémentaire pour remplir la base de données externe avec des informations d'identification de point de terminaison.
- Si la base de données externe n'est pas présente localement comme les PSN, cette solution dépend du WAN, ce qui en fait le 3^{e} point de défaillance dans le flux de données AAA du point d'extrémité.
- Nécessite des connaissances supplémentaires pour gérer les processus et procédures de base de données externes.
- Les erreurs provoquées par la configuration manuelle de l'ID d'utilisateur dans la base de données doivent être prises en compte.

Exemples de configurations de base de données externe

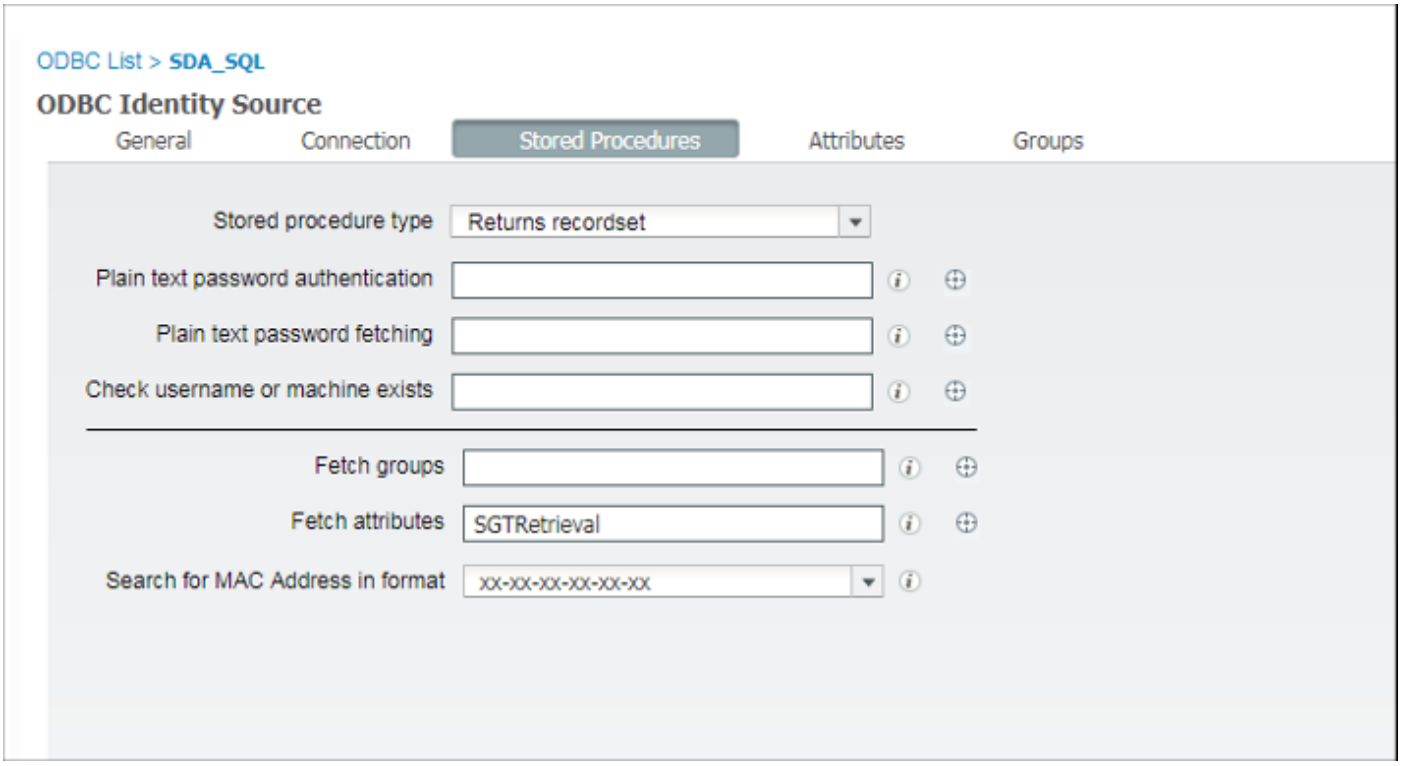
Dans ce document, Microsoft SQL apparaît comme la base de données externe utilisée comme point d'autorisation.

Étape 1 : création du magasin d’identités ODBC dans Cisco ISE à partir du menu **Administration >**

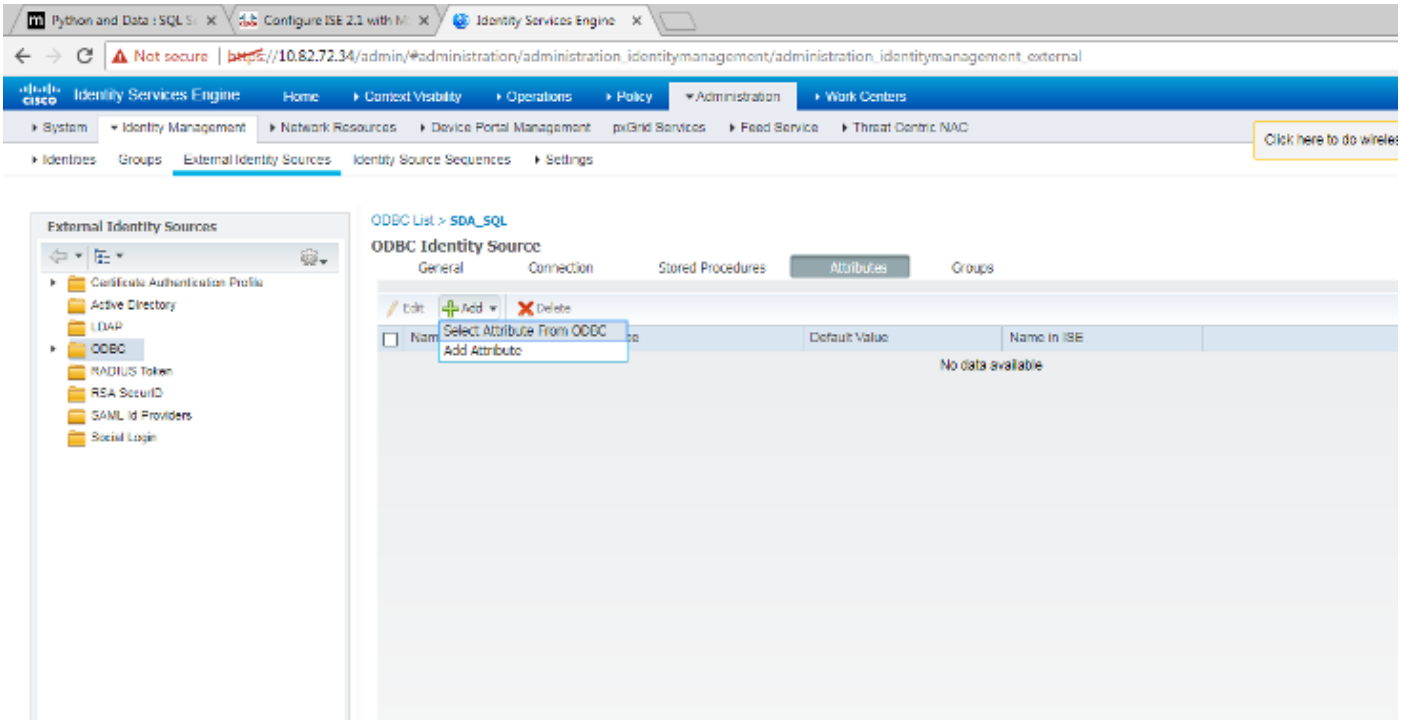
External Identity Source > ODBC et test des connexions

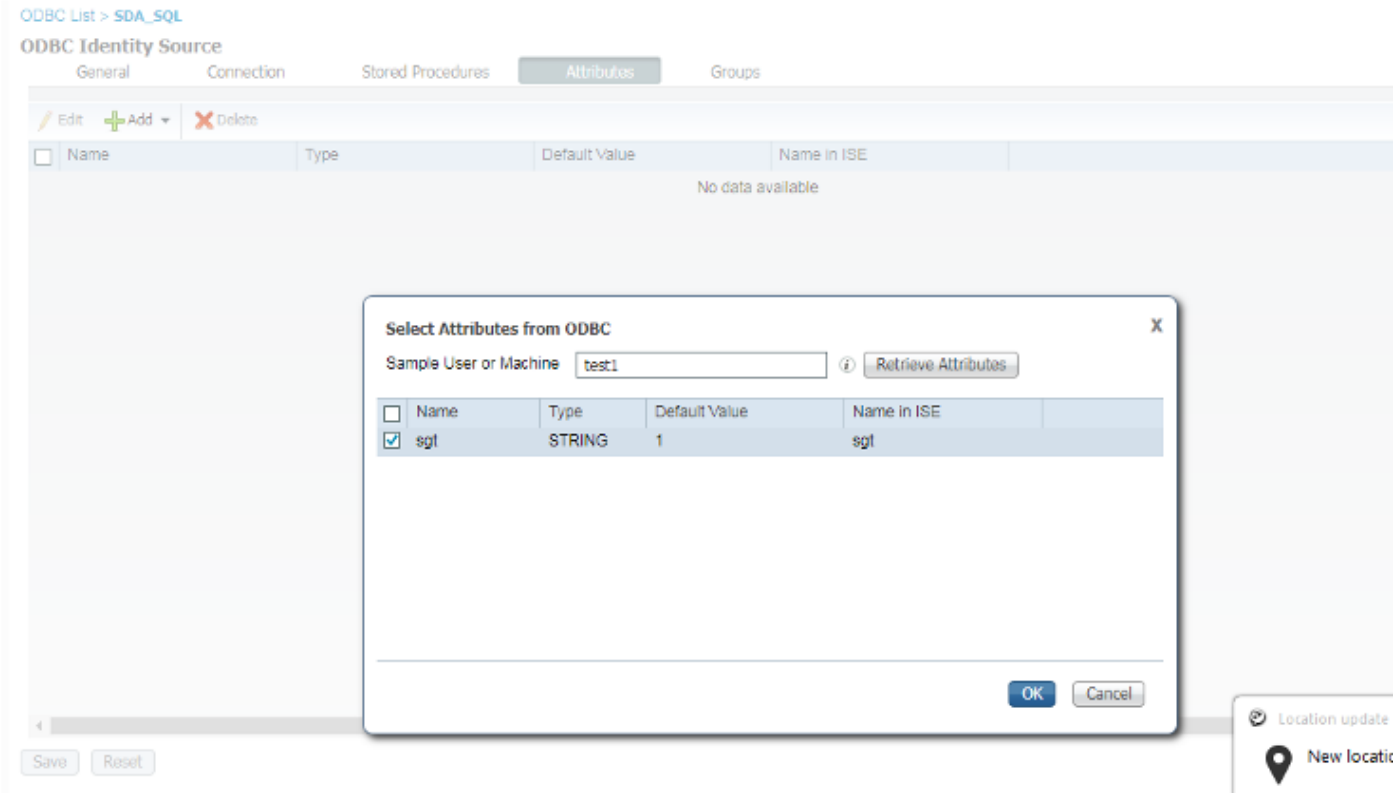


Étape 2. Accédez à l'onglet Procédures stockées de la page ODBC pour configurer les procédures créées dans Cisco ISE.

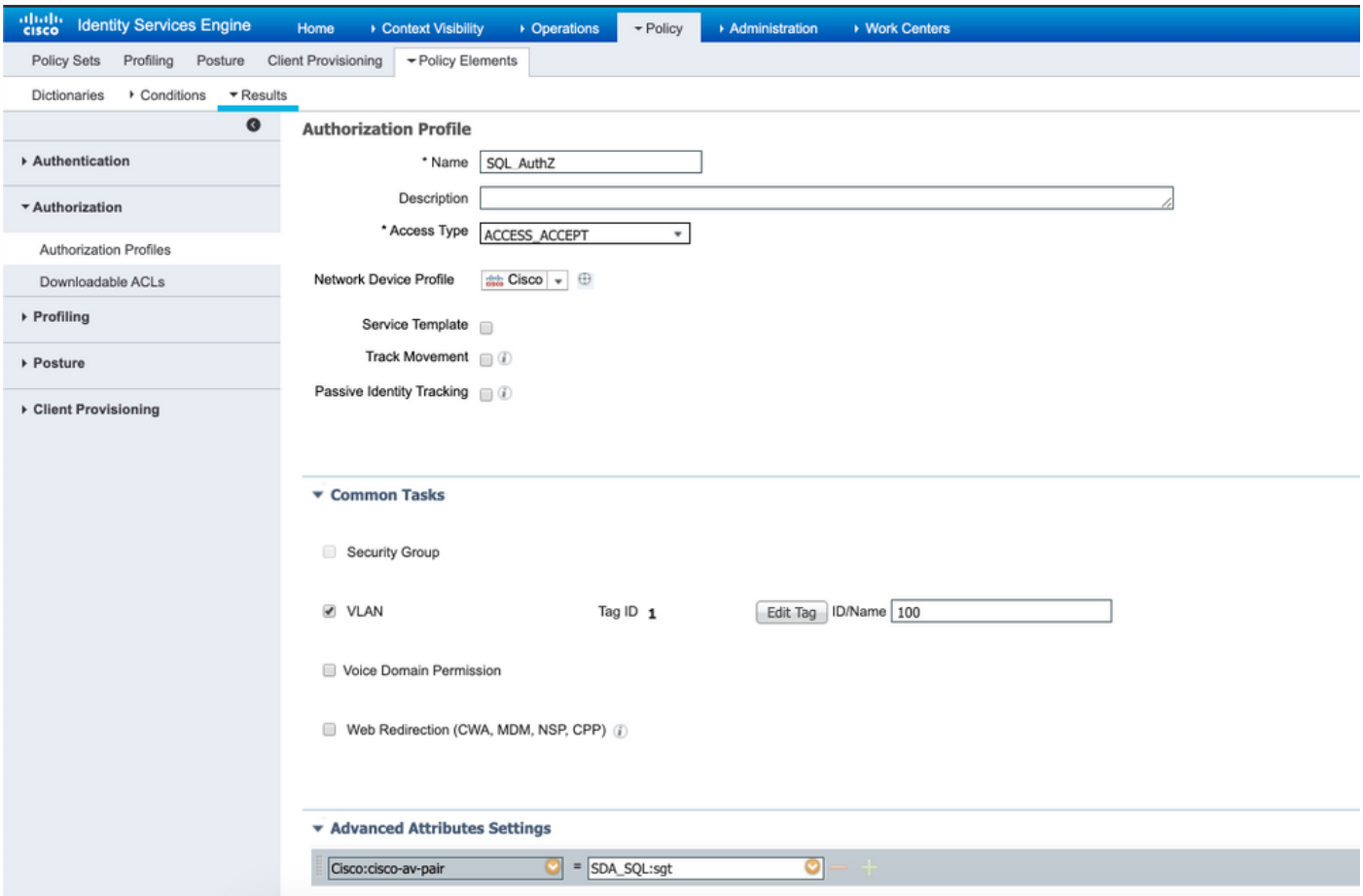


Étape 3. Récupérez les attributs de l'ID utilisateur à partir de la source d'ID ODBC pour vérification.



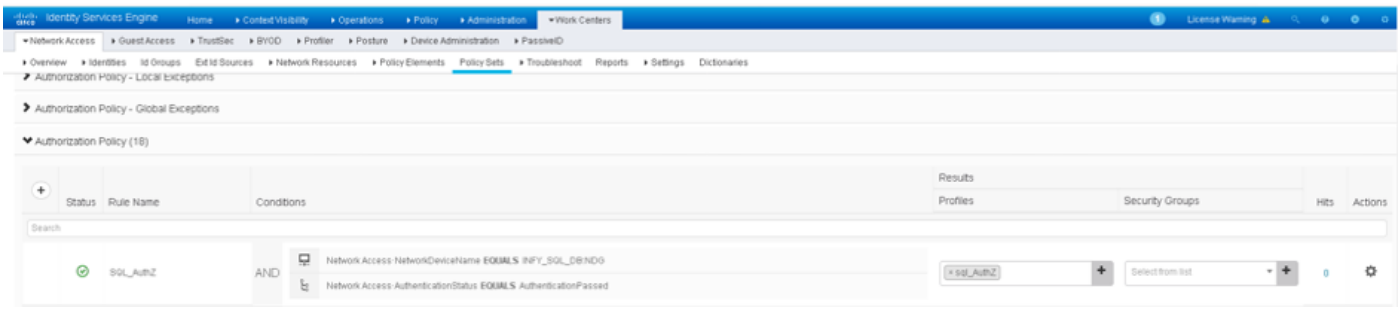


Étape 4 : création d'un **profil d'autorisation** et configuration Dans Cisco ISE, accédez à **Policy > Results > Authorization profile > Advance Attributes Settings** et sélectionnez l'attribut en tant que **Cisco : cisco-av-pair.** Sélectionnez les valeurs en tant que <nom de la base de données ODBC> : sgt, puis enregistrez-le.



Étape 5 : création d'une **stratégie d'autorisation** et configuration de celle-ci Dans Cisco ISE, accédez à **Policy > Policy sets > Authorization Policy > Add.** Placez la condition comme Identity

Source est le serveur SQL. Sélectionnez le profil Résultat comme profil d'autorisation créé précédemment.



Étape 6. Une fois que l'utilisateur est authentifié et autorisé, les journaux contiennent la sgt attribuée à l'utilisateur, pour vérification.

Result

State	ReauthSession:AC1004320000109702FD9BB4
Class	CACS:AC1004320000109702FD9BB4:POD4-ISE/293950587/330
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 400
EAP-Key-Name	19:59:b7:15:23:a2:2c:27:b1:56:12:9d:39:b9:64:32:fd:a4:b6:bf:33:f9:0e:46:16:da:8f:b7:17:37:13:73:d3:7e:19:50:8d:32:93:d9:6d:e4:0c:08:65:48:36:16:ec:ef:f7:31:5b:84:fe:5d:a4:1b:ba:64:80:d7:0a:ea:b2
cisco-av-pair	cts:security-group-tag=0011-0
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

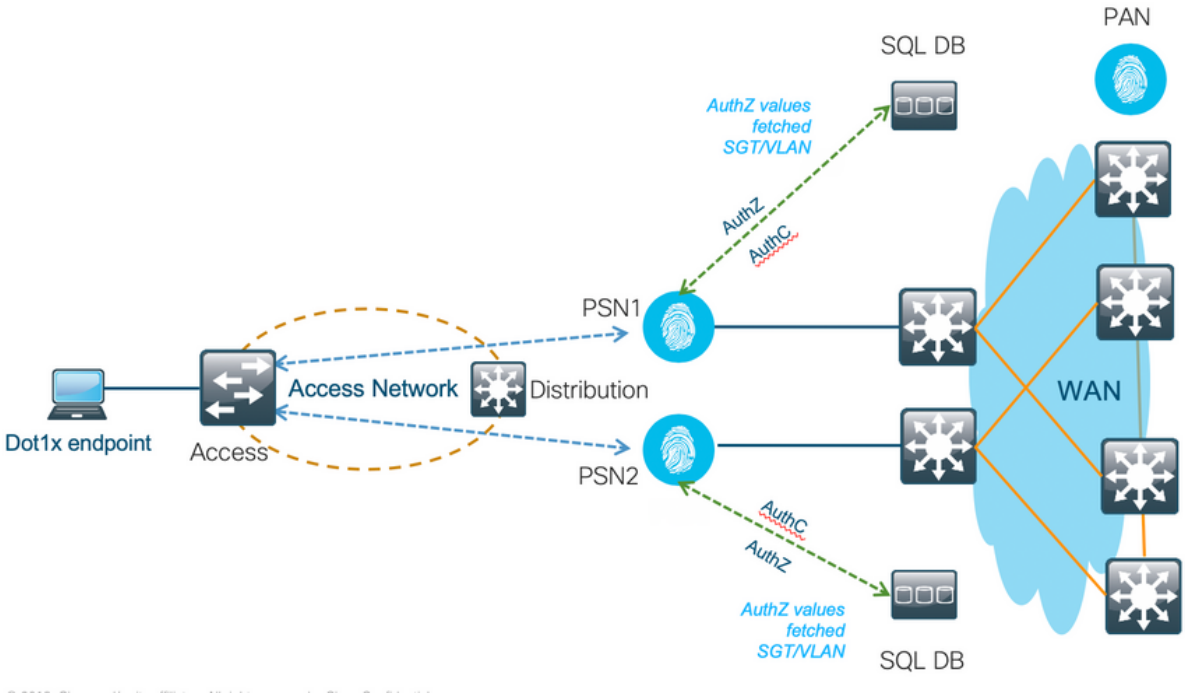
Session Events

2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

Workflow de la solution (après ISE 2.7)

Après ISE 2.7, les attributs d'autorisation peuvent être récupérés à partir d'ODBC tels que Vlan, SGT, ACL et ces attributs peuvent être utilisés dans les stratégies.

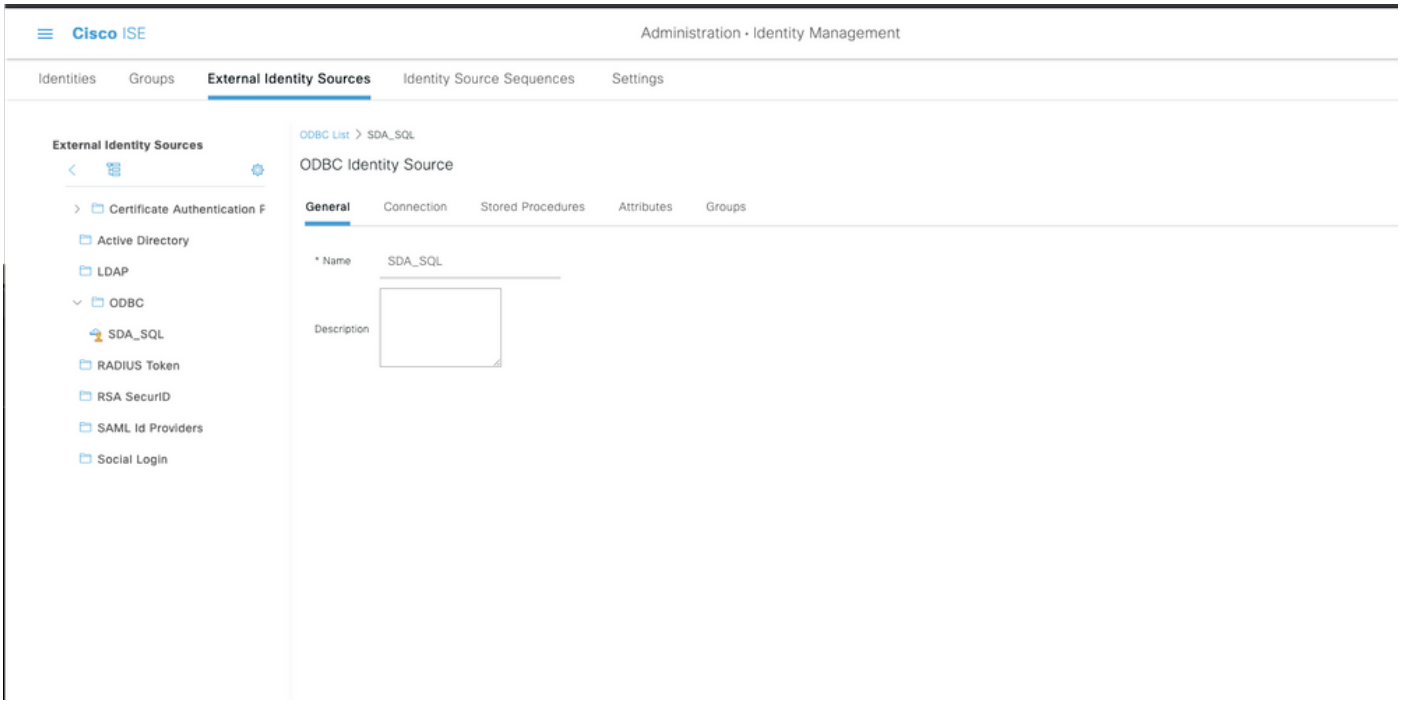
Dans cette solution, Cisco ISE est intégré à Microsoft SQL. MS SQL est utilisé comme magasin d'ID pour l'authentification ainsi que pour l'autorisation. Lorsque les informations d'identification des points d'extrémité sont fournies à PSN, elles sont validées par rapport à la base de données MS SQL. La stratégie d'autorisation fait référence à la base de données MS SQL pour récupérer les résultats autorisés tels que SGT / VLAN pour lequel **user-id** est utilisé comme référence.



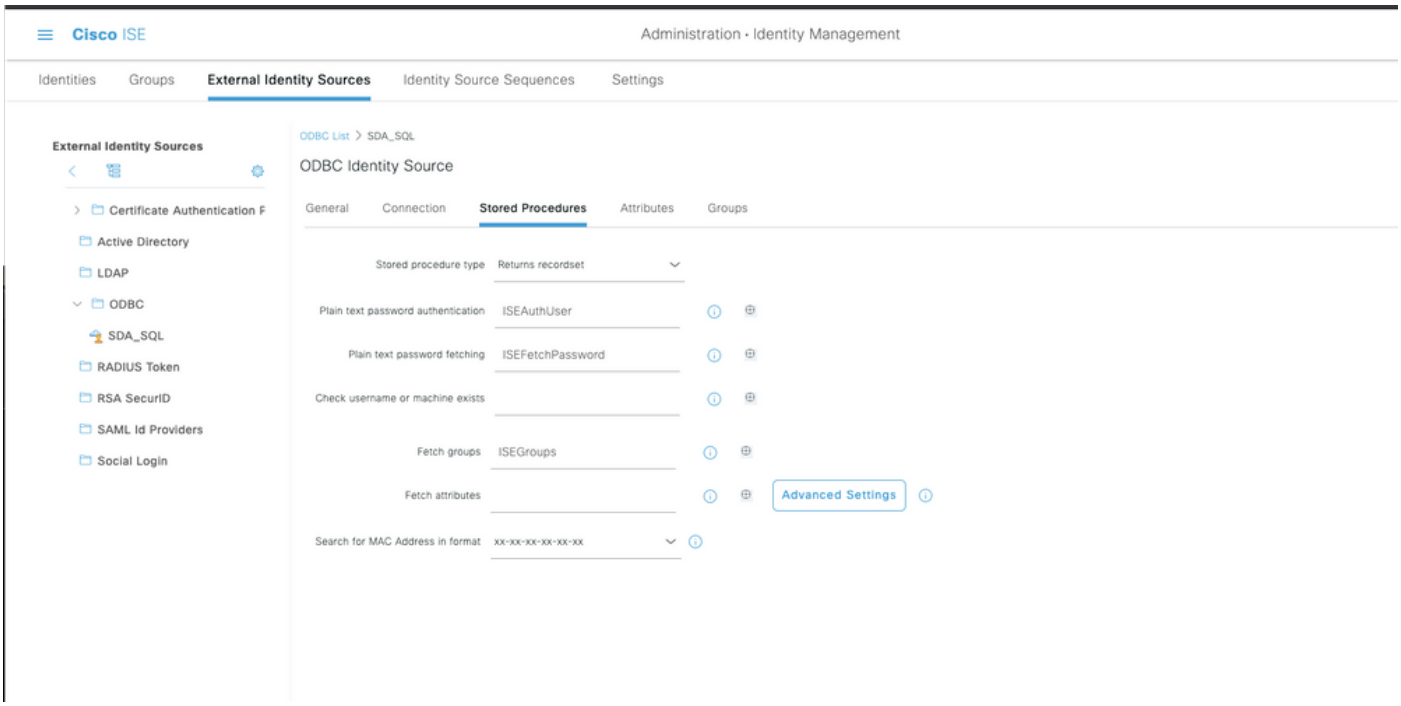
Exemples de configurations de base de données externe

Suivez la procédure fournie précédemment dans ce document pour créer MS SQL DB avec Username, Password, VLAN id et SGT.

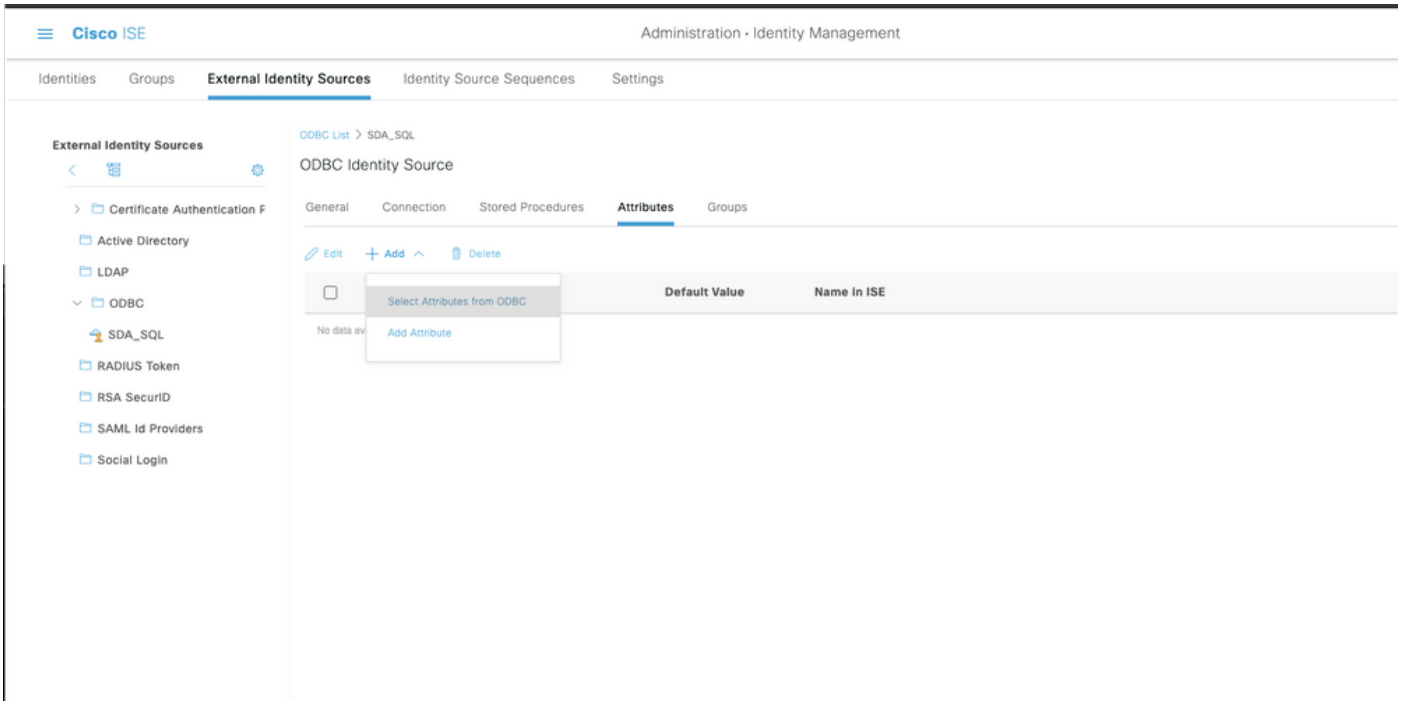
Étape 1. Créez un magasin d'identités ODBC dans Cisco ISE à partir du menu **Administration > External Identity Source > ODBC** et testez les connexions.

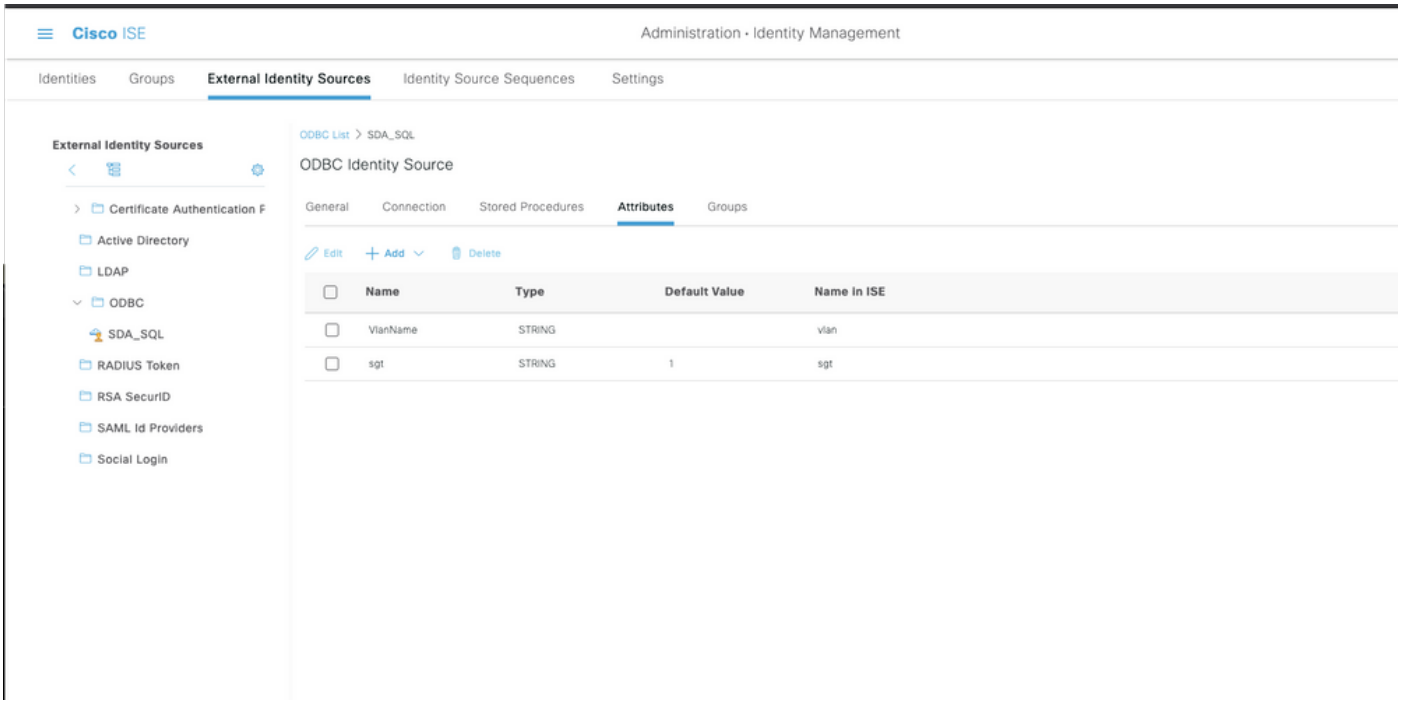


Étape 2. Accédez à l'onglet Procédures stockées de la page ODBC pour configurer les procédures créées dans Cisco ISE.

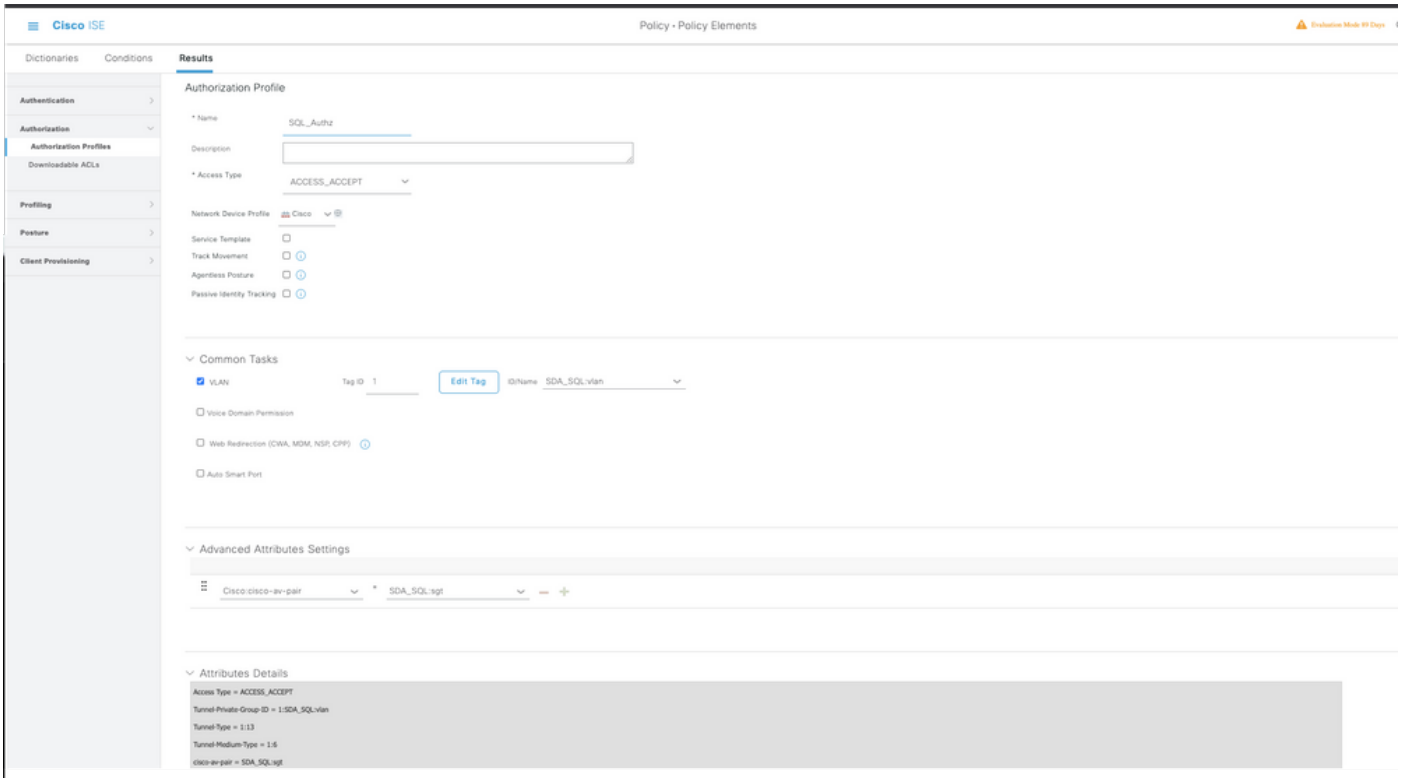


Étape 3. Récupérez les attributs de l'ID utilisateur à partir de la source d'ID ODBC pour vérification.

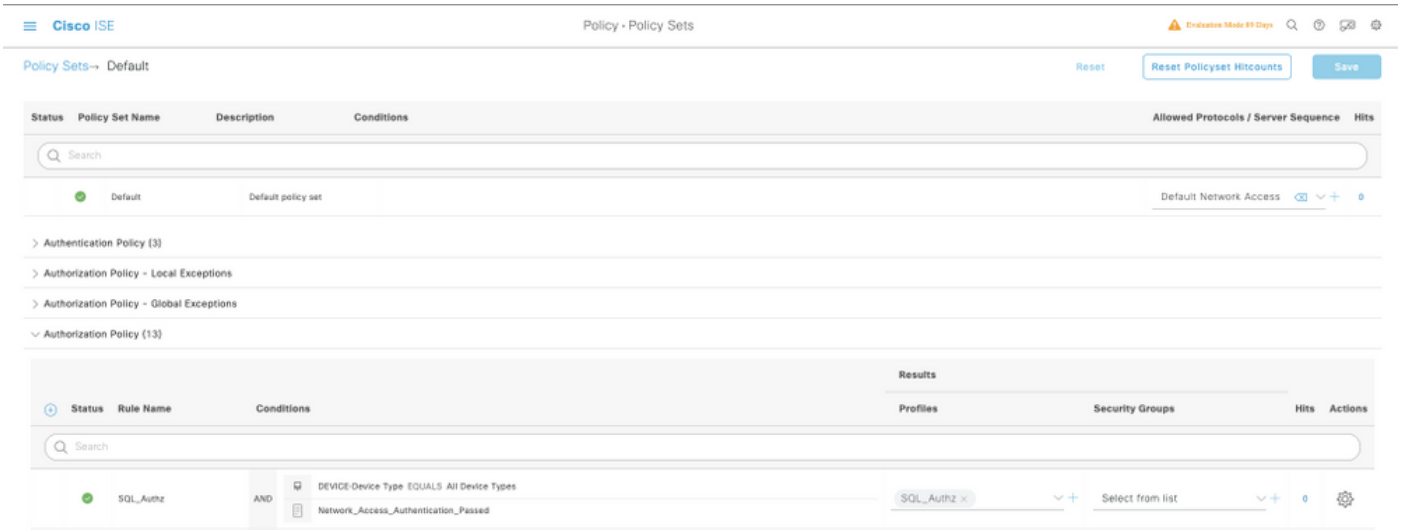




Étape 4 : création d'un **profil d'autorisation** et configuration Dans Cisco ISE, accédez à **Policy > Results > Authorization profile > Advance Attributes Settings** et sélectionnez l'attribut **Cisco : cisco-av-pair.** Sélectionnez les valeurs comme <nom de la base de données ODBC>:sgt. Sous Common Tasks, sélectionnez **VLAN** with ID/Name as <nom de la base de données ODBC>:vlan et enregistrez-le



Étape 5 : création d'une **stratégie d'autorisation** et configuration de celle-ci Dans Cisco ISE, accédez à **Policy > Policy sets > Authorization Policy > Add.** Placez la condition comme Identity Source est le serveur SQL. Sélectionnez le profil Résultat comme profil d'autorisation créé précédemment.

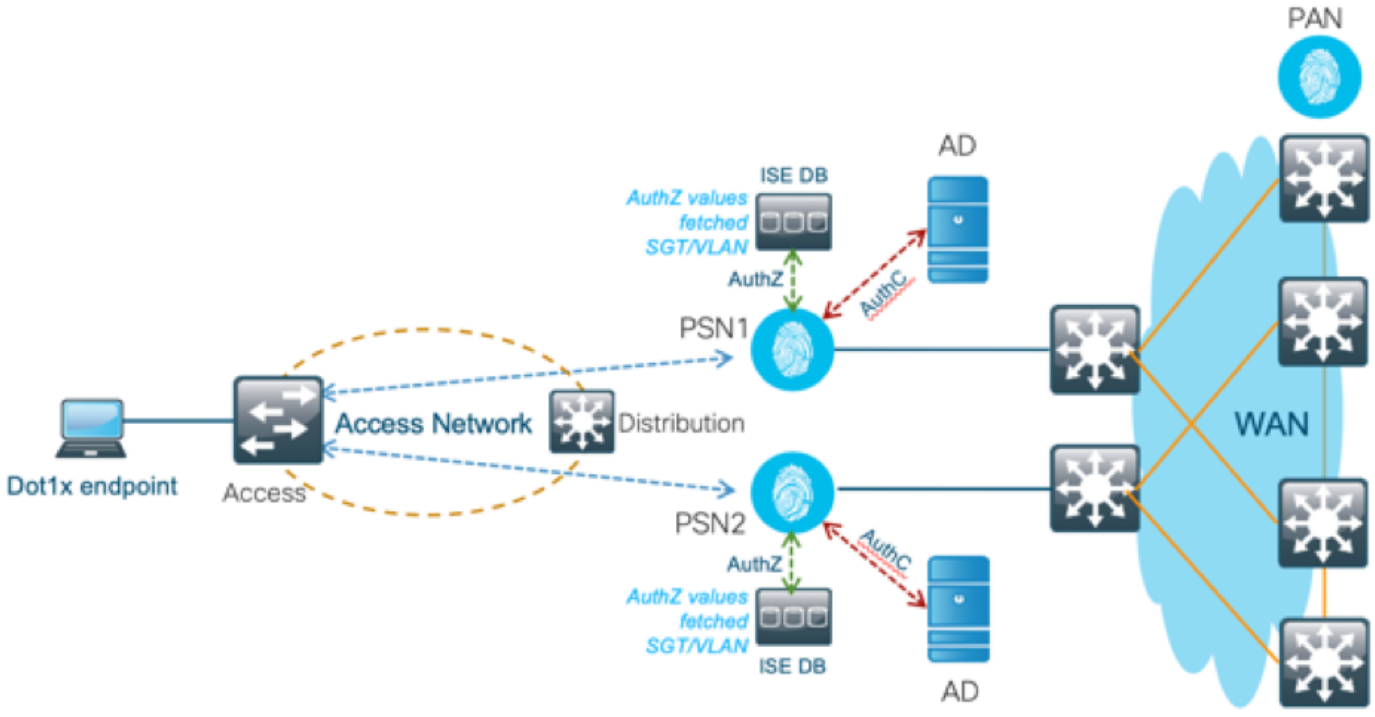


Utiliser la base de données interne

Cisco ISE possède lui-même une base de données intégrée qui peut être utilisée pour avoir des ID utilisateur pour l'autorisation.

Workflow de solution

Dans cette solution, la base de données interne de Cisco ISE est utilisée comme point d'autorisation tandis qu'Active Directory (AD) continue d'être la source d'authentification. L'ID utilisateur des terminaux est inclus dans la base de données Cisco ISE avec des **attributs personnalisés** qui renvoient les résultats autorisés tels que SGT ou VLAN. Lorsque les informations d'identification des terminaux sont fournies à PSN, il vérifie la validité des informations d'identification des terminaux avec le magasin d'ID Active Directory et authentifie le terminal. La stratégie d'autorisation fait référence à la base de données ISE pour extraire les résultats autorisés tels que SGT / VLAN pour lesquels l'ID d'utilisateur est utilisé comme référence.



Avantages

Cette solution présente les avantages suivants, ce qui en fait une solution flexible :

- La base de données Cisco ISE est une solution intégrée et n'a donc pas de 3e point de défaillance, contrairement à la solution de base de données externe.
- Comme le cluster Cisco ISE assure la synchronisation en temps réel entre toutes les personnes, il n'y a pas de dépendance WAN, car le PSN dispose de tous les ID utilisateur et attributs personnalisés transmis par le PAN en temps réel.
- Cisco ISE peut tirer parti de toutes les fonctionnalités supplémentaires que la base de données externe peut offrir.
- Cette solution ne dépend d'aucune limite d'évolutivité Cisco ISE.

Inconvénients

Cette solution présente les inconvénients suivants :

- Le nombre maximal d'ID utilisateur que Cisco ISE DB peut refuser est de 300 000.
- Les erreurs provoquées par la configuration manuelle de l'ID d'utilisateur dans la base de données doivent être prises en compte.

Exemples de configurations de base de données interne

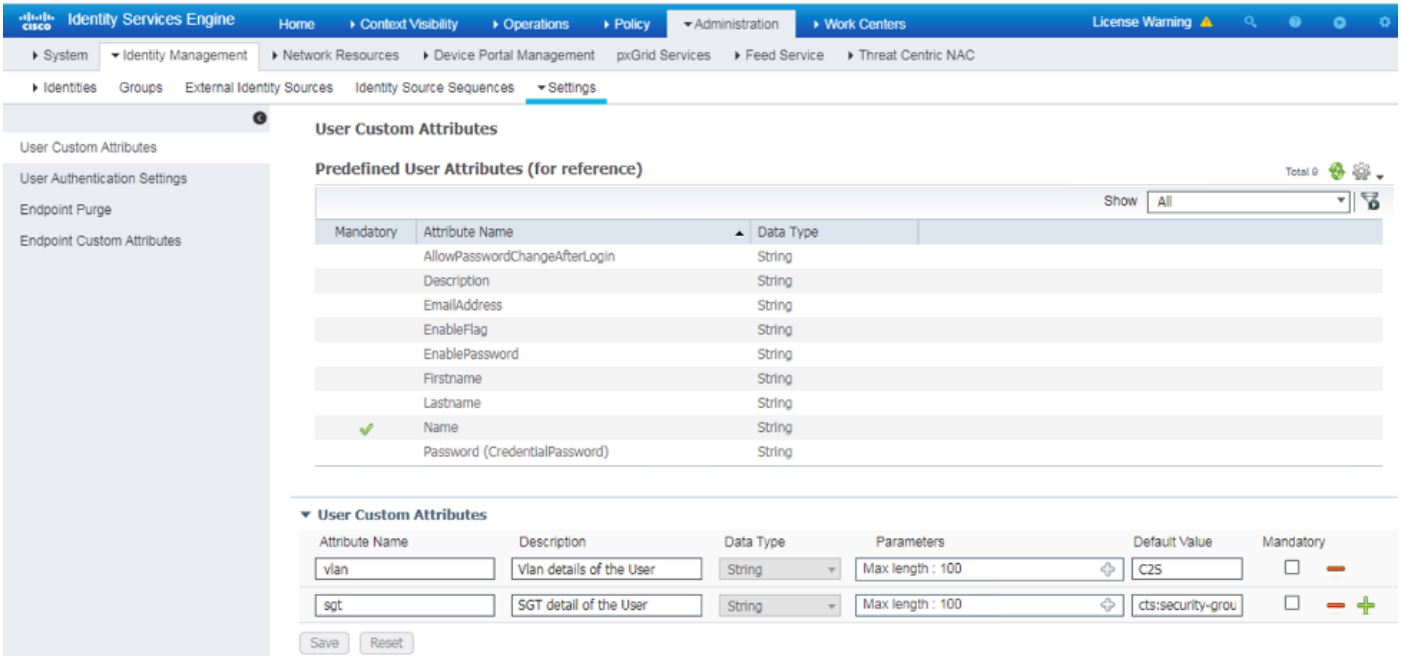
Les VLAN et SGT par utilisateur peuvent être configurés pour n'importe quel utilisateur dans le magasin d'ID interne avec un attribut utilisateur personnalisé.

Étape 1. Créez de nouveaux attributs personnalisés utilisateur pour représenter la valeur VLAN et SGT des utilisateurs respectifs. Accédez à **Administration > Identity Management > Settings > User Custom Attributes.** Créez de nouveaux attributs personnalisés utilisateur comme indiqué dans ce tableau.

Ici, la table de base de données ISE est affichée avec des attributs personnalisés.

Nom d'attribut	Type de données	Paramètres (longueur)	Valeur par défaut
vlan	Chaîne (string)	100	C2S (Nom De Vlan Par Défaut)
sgt	Chaîne (string)	100	cts : security-group-tag=0003-0 (valeur SGT par défaut)

- Dans ce scénario, la valeur VLAN représente le nom du VLAN et la valeur sgt représente l'attribut cisco-av-pair de SGT au format hexadécimal.

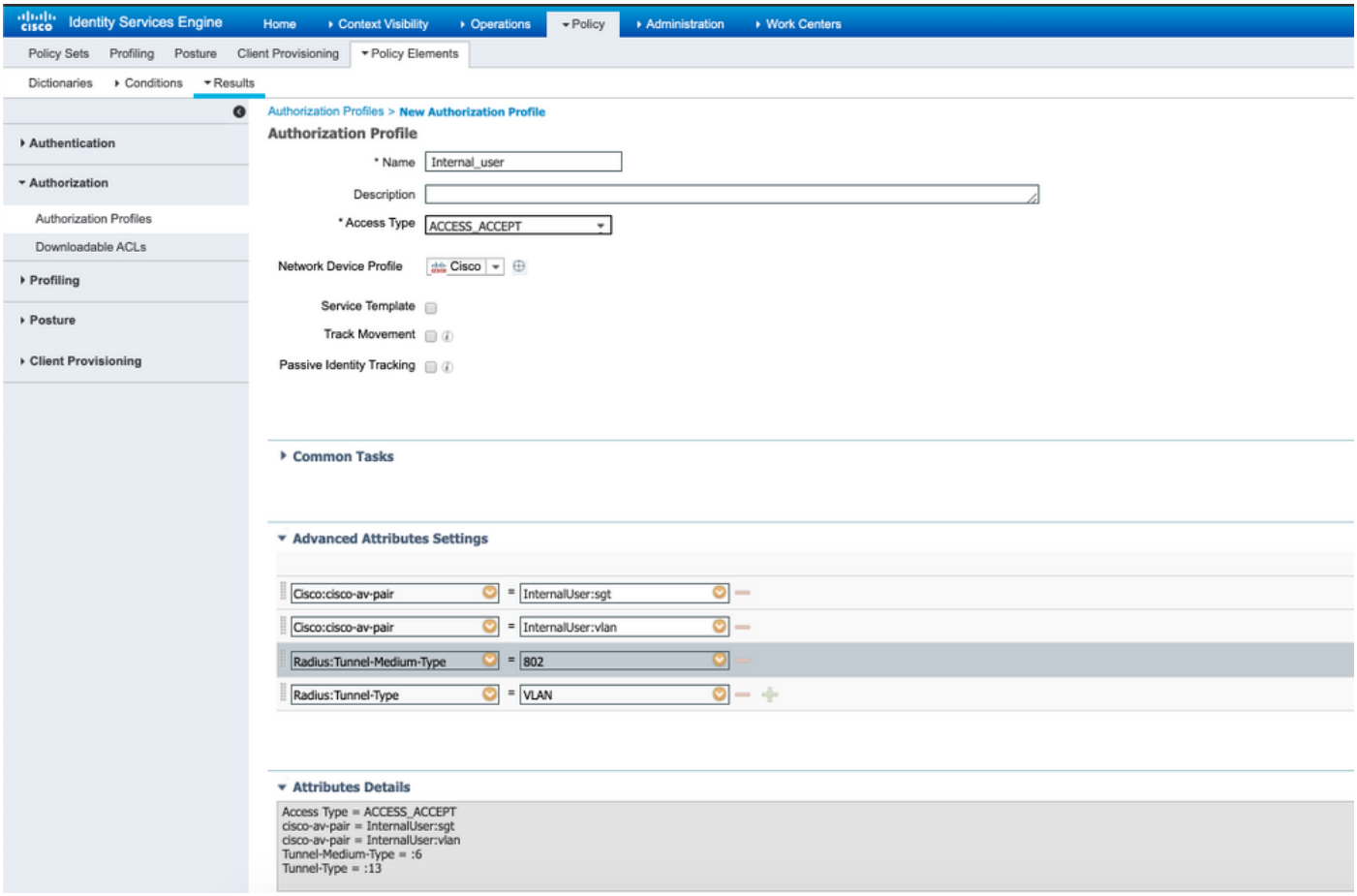


Étape 2 : création d'un profil d'autorisation avec des attributs utilisateur personnalisés pour impliquer les valeurs vlan et sgt des utilisateurs respectifs. Accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation > Ajouter.** Ajoutez les attributs mentionnés ci-dessous sous Paramètres d'attributs avancés.

Ce tableau présente le profil AuthZ pour l'utilisateur interne.

Attribut	Valeur
Cisco:paire-av-cisco	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	InternalUser:vlan
Rayon:Tunnel-Medium-Type	802
Rayon:Type De Tunnel	VLAN

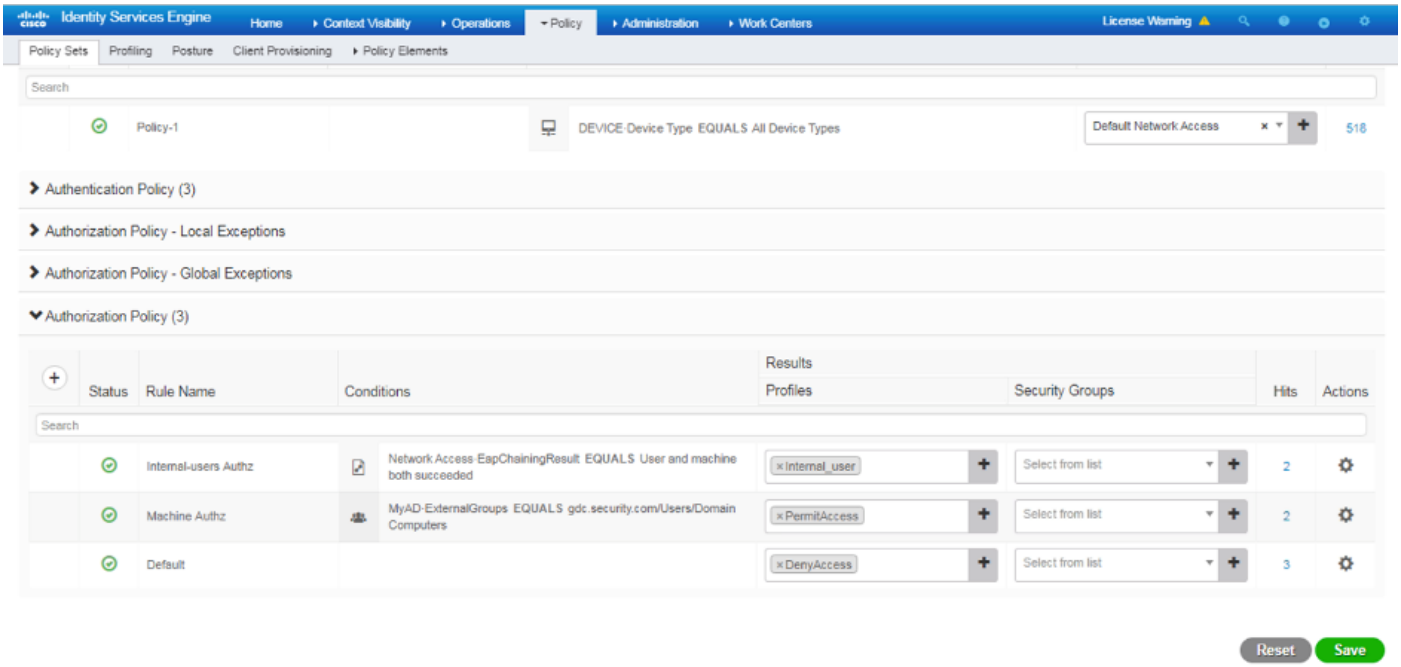
Comme l'illustre l'image, pour les utilisateurs internes, le profil **Internal_user** est configuré avec le SGT et le Vlan configurés en tant que **InternalUser:sgt** et **InternalUser:vlan** respectivement.



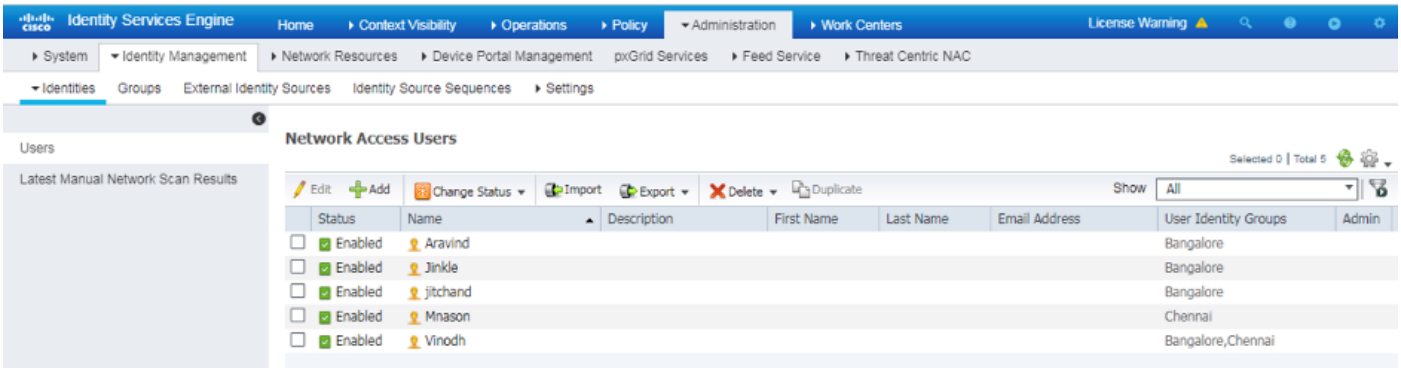
Étape 3. Créez une stratégie d'autorisation, accédez à **Stratégie > Jeux de stratégies > Stratégie-1 > Autorisation.** Créez des stratégies d'autorisation avec les conditions mentionnées ci-dessous et mappez-les aux profils d'autorisation respectifs.

Ce tableau présente la stratégie AuthZ pour l'utilisateur interne.

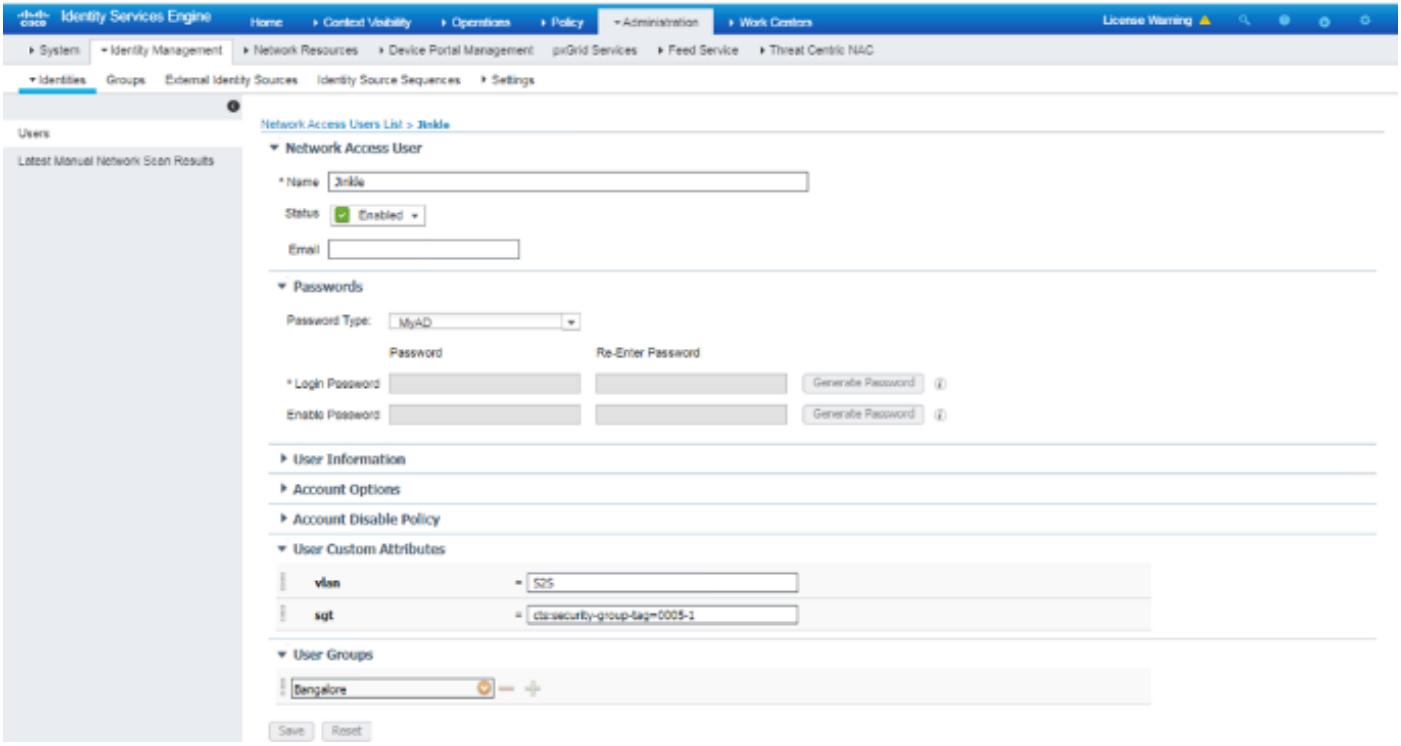
Nom de règle	Condition	Résultat Authz Profile
Authentification_Utilisateur_Interne	Si Network Access.EapChainingResults EST ÉGAL à Utilisateur et machine ont réussi	Utilisateur_interne
Machine_Only_Authz	Si MyAD.ExternalGroups EST ÉGAL À gdc.security.com/Users/Domain Ordinateurs	AutoriserAccès



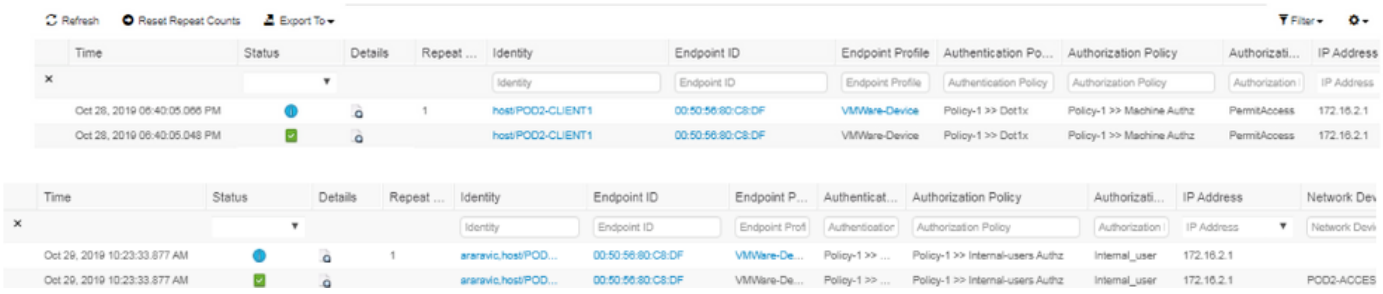
Étape 4. Créez des identités d'utilisateur en masse avec des attributs personnalisés avec les détails de l'utilisateur et leurs attributs personnalisés respectifs dans le modèle CSV. Importez le fichier CSV en accédant à **Administration > Identity Management > Identities > Users > Import > Choisissez le fichier > Import.**



Cette image présente un exemple d'utilisateur avec des détails d'attribut personnalisés. Sélectionnez l'utilisateur et cliquez sur Modifier pour afficher les détails d'attribut personnalisés mappés à l'utilisateur respectif.



Étape 5 : Vérifiez les journaux actifs :



Consultez la section **Result** pour vérifier si l'attribut **Vlan** & **SGT** est envoyé en tant que partie de Access-Accept.

Conclusion

Cette solution permet à certains des clients des grandes entreprises de s'adapter à leurs besoins. L'ajout/la suppression d'ID utilisateur doit être effectué avec prudence. Les erreurs, si elles sont déclenchées, peuvent entraîner un accès non autorisé pour les utilisateurs authentiques ou vice versa.

Informations connexes

Configuration de Cisco ISE avec MS SQL via ODBC :

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

Glossaire

AAA	Authentication Authorization Accounting
PUBLICITÉ	Active Directory
AuthC	Authentification
AuthZ	Autorisation
DB	Base de données
DOT1X	802.1X
IBN	Réseau basé sur l'identité
ID	Base De Données D'Identité
ISE	Plateforme de services d’identité

MnT	Surveillance et dépannage
MsSQL	Microsoft SQL
ODBC	Connectivité Open DataBase
POÊLE	Noeud Administration de stratégie
PSN	Noeud Services de stratégie
SGT	Balise Groupe sécurisé
SQL	langage d'interrogation structuré
VLAN	Réseau local virtuel
Réseau WAN	réseau étendu

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.