使用ODBC和ISE DB（自定義屬性）為大型園區網路簡化訪問策略

目錄

簡介

本文檔介紹大規模園區部署，同時不影響其功能和安全實施。思科的終端安全解決方案，身份服務引擎(ISE)通過與外部身份源整合來滿足此要求。

對於具有50多個地理位置、4000多個不同使用者配置檔案和600,000個或更多個終端的大型網路，需要從不同的角度審視傳統IBN解決方案，而不僅僅是功能，無論其是否隨所有功能進行擴展。在當今傳統大規模網路中，基於意圖的網路(IBN)解決方案需要更多關注可擴充性和易管理性，而不僅僅是功能。

必要條件

需求

思科建議您瞭解以下主題：

- Dot1x/MAB驗證
- 思科身分識別服務引擎(CiscoISE)
- Cisco TrustSec(CTS)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

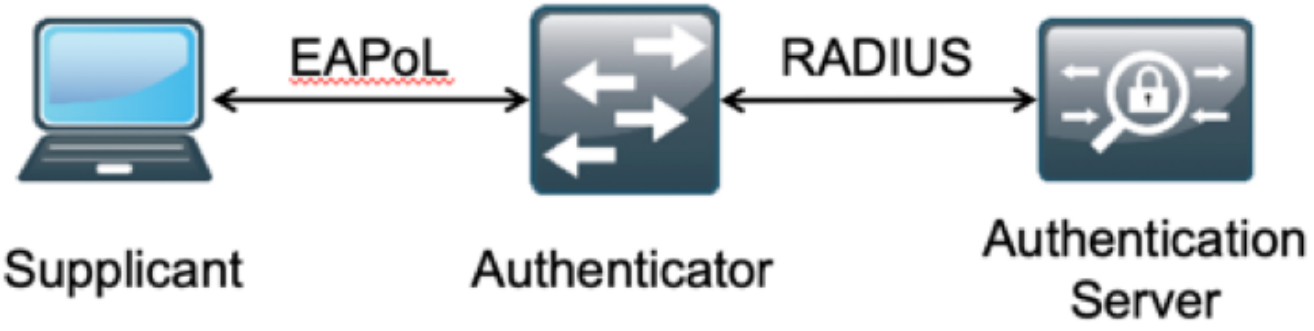
- 思科身分識別服務引擎(ISE)版本2.6補丁2和版本3.0
- Windows Active Directory(AD)Server 2008版本2
- Microsoft SQL Server 2012

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果網路處於活動狀態，請確保瞭解任何配置的潛在影響。

背景資訊

在基於身份的網路(IBN)解決方案中，基本元素是Supplicant、Authenticator和Authentication(AAA)伺服器。請求方是終端上的代理，在請求網路訪問時提供憑證。驗證器或NAS（網路存取伺服器）是存取層，包括網路交換器和WLC，它們會將憑證傳輸到AAA伺服器。身份驗證伺服器根據ID儲存驗證使用者身份驗證請求，並授權訪問接受或訪問拒絕。ID儲存可以位於AAA伺服器內，也可以位於外部專用伺服器上。

此圖顯示了基本IBN元素。



RADIUS是一種以使用者資料包通訊協定(UDP)為基礎的通訊協定，驗證與授權搭配在一起。在思科企業園區的IBN解決方案中，ISE的策略服務節點(PSN)角色充當AAA伺服器，根據企業ID儲存對終端進行身份驗證並根據條件進行授權。

在Cisco ISE中，身份驗證和授權策略配置為滿足這些要求。身份驗證策略包括有線或無線介質型別以及用於使用者驗證的EAP協定。授權策略包括一些條件，這些條件定義了各種終端要匹配的標準和網路訪問結果，可以是VLAN、可下載ACL或安全組標籤(SGT)。 以下是可以配置ISE的策略的最大擴展數。

此表顯示Cisco ISE策略擴展。

屬性	**縮放編號**
身份驗證規則的最大數量	1000（策略設定模式）

最大授權規則數	3,000（策略設定模式） 具有3200 Authz配置檔案

技術趨勢

分段已成為當今企業網路的主要安全要素之一，無需實際邊緣網路。允許端點在內部和外部網路之間漫遊。分段有助於遏制對特定網段的任何安全攻擊，以擴展到整個網路。在思科ISE的TrustSec的幫助下，目前的軟體定義訪問(SDA)解決方案提供了一種根據客戶業務模式進行分段的方法，從而避免對VLAN或IP子網等網路元素的依賴性。

問題

對於具有500多個不同終端配置檔案的大型企業網路的ISE策略配置，授權策略數量可能會增加到一個無法管理的點。即使Cisco ISE支援專用授權條件來滿足如此大量的使用者配置檔案，管理員管理這些數量策略也是一項挑戰。

此外，客戶可能需要通用授權策略而不是專用策略來避免管理開銷，並且還可以根據終端標準為終端提供差異化網路訪問。

例如，考慮以Active Directory(AD)作為真理來**源、端點獨特優勢是AD屬性之一的企業網**絡。在這種情況下，傳統的策略配置方式為每個唯一的終端配置檔案提供了更多的授權策略。

在此方法中，每個終端配置檔案都通過domain.com下的AD屬性進行區分。因此，需要配置專用授權策略。

此表顯示了傳統身份驗證策略。

ABC策略	如果AnyConnect等於User-AND-Machine-Both-Passed 和 如果AD組等於domain.com/groups/ABC 然後 SGT:C2S-ABC和VLAN:1021
DEF策略	如果AnyConnect等於User-AND-Machine-Both-Passed 和 如果AD組等於domain.com/groups/DEF 然後 SGT:C2S-DEF和VLAN:1022
GHI策略	如果AnyConnect等於User-AND-Machine-Both-Passed 和 如果AD組等於domain.com/groups/GHI 然後 SGT:C2S-GHI和VLAN:1023
XYZ策略	如果AnyConnect等於User-AND-Machine-Both-Passed 和 如果AD組等於domain.com/groups/XYZ 然後 SGT:C2S-XYZ和VLAN:1024

建議的解決方案

為了避免違反思科ISE支援的最大可伸縮授權策略數量，建議的解決方案是使用外部資料庫授權每個端點，從其屬性獲取授權結果。例如，如果將AD用作外部資料庫進行授權，則可以引用任何未使用的使用者屬性（如Department或Pin代碼），以提供與SGT或VLAN對映的授權結果。

這是通過思科ISE與外部資料庫或配置自定義屬性的ISE內部資料庫的整合實現的。本節介紹這兩種方案的部署：

> **附註**：在兩個選項中，資料庫都包含**user-id**，但不包含**DOT1X端點的**密碼。DB僅用作**授權**點。在大多數情況下，身份驗證仍可以繼續作為客戶的ID儲存區駐留在Active Directory(AD)伺服器上。

使用外部DB配置

思科ISE與外部DB整合以進行終端憑證驗證：

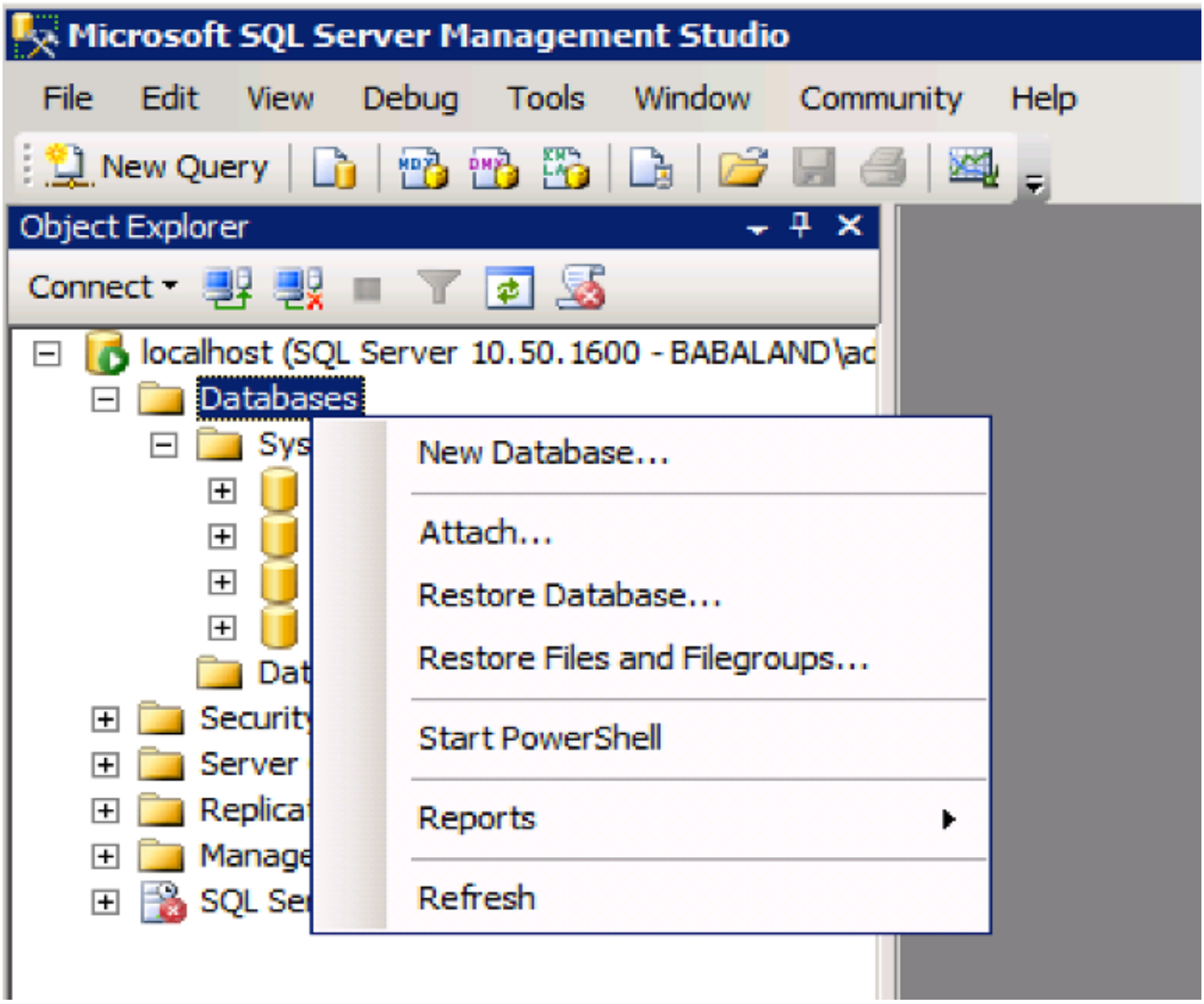
此表顯示了已驗證的外部身份源。

外部身份源	**作業系統/版本**
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伺服器	
SunONE LDAP目錄伺服器	版本5.2
OpenLDAP目錄伺服器	版本2.4.23
任何LDAP v3相容伺服器	—
令牌伺服器	
RSA ACE/伺服器	6.x系列
RSA身份驗證管理器	7.x和8.x系列
任何符合RADIUS RFC 2865的令牌伺服器	—
安全斷言標籤語言(SAML)單一登入(SSO)	
Microsoft Azure	—
Oracle Access Manager(OAM)	版本11.1.2.2.0
Oracle Identity Federation(OIF)	版本11.1.1.2.0
PingFederate伺服器	版本6.10.0.4
PingOne雲端	—
安全身份驗證	8.1.1
任何符合SAMLv2的標識提供程式	—
開放式資料庫連線(ODBC)身份源	
Microsoft SQL Server(MS SQL)	Microsoft SQL Server 2012
Oracle	企業版版本12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
社交登入（用於訪客使用者帳戶）	
臉書	—

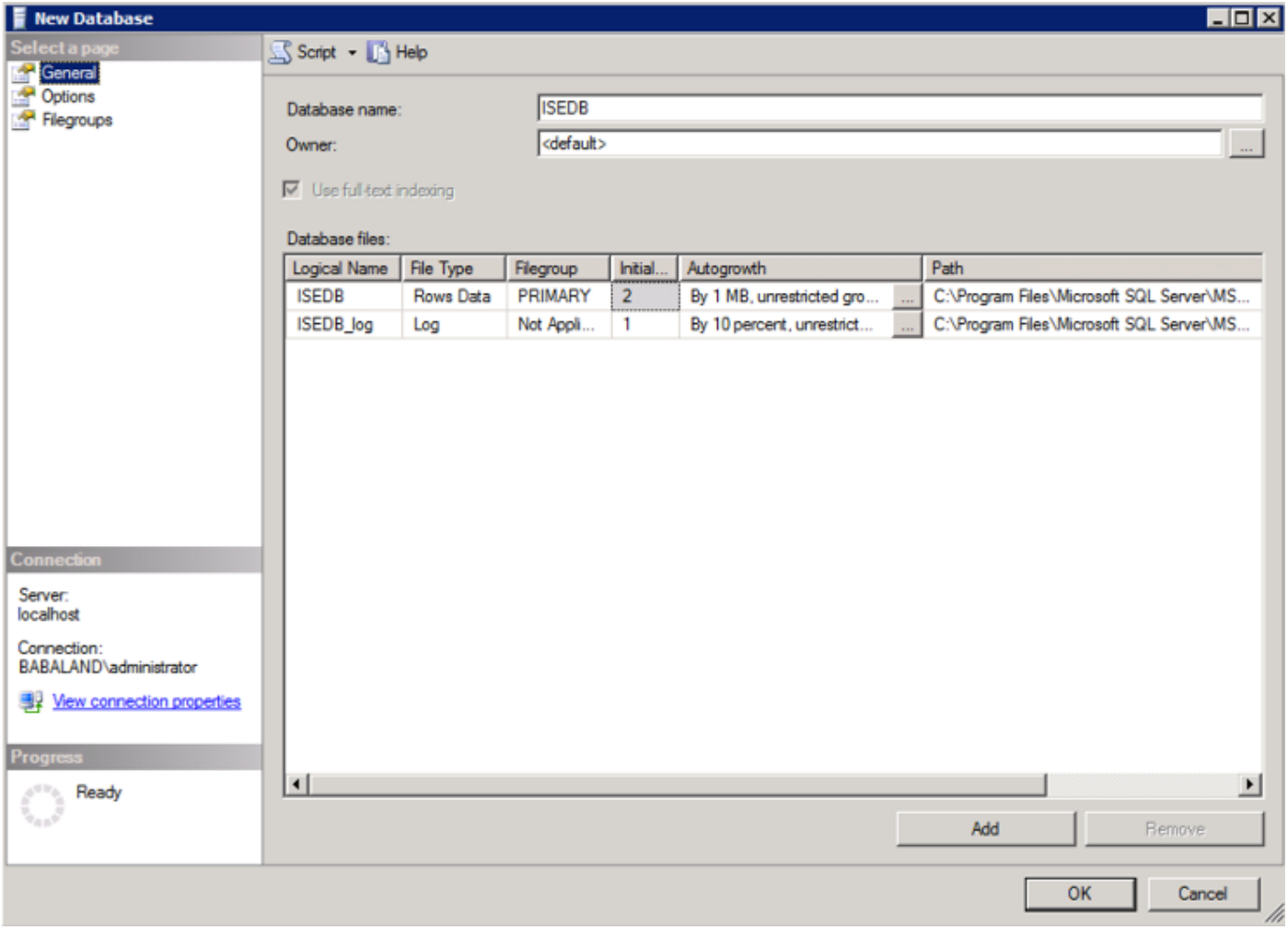
ODBC示例配置

此配置是在Microsoft SQL上完成的，用於構建解決方案：

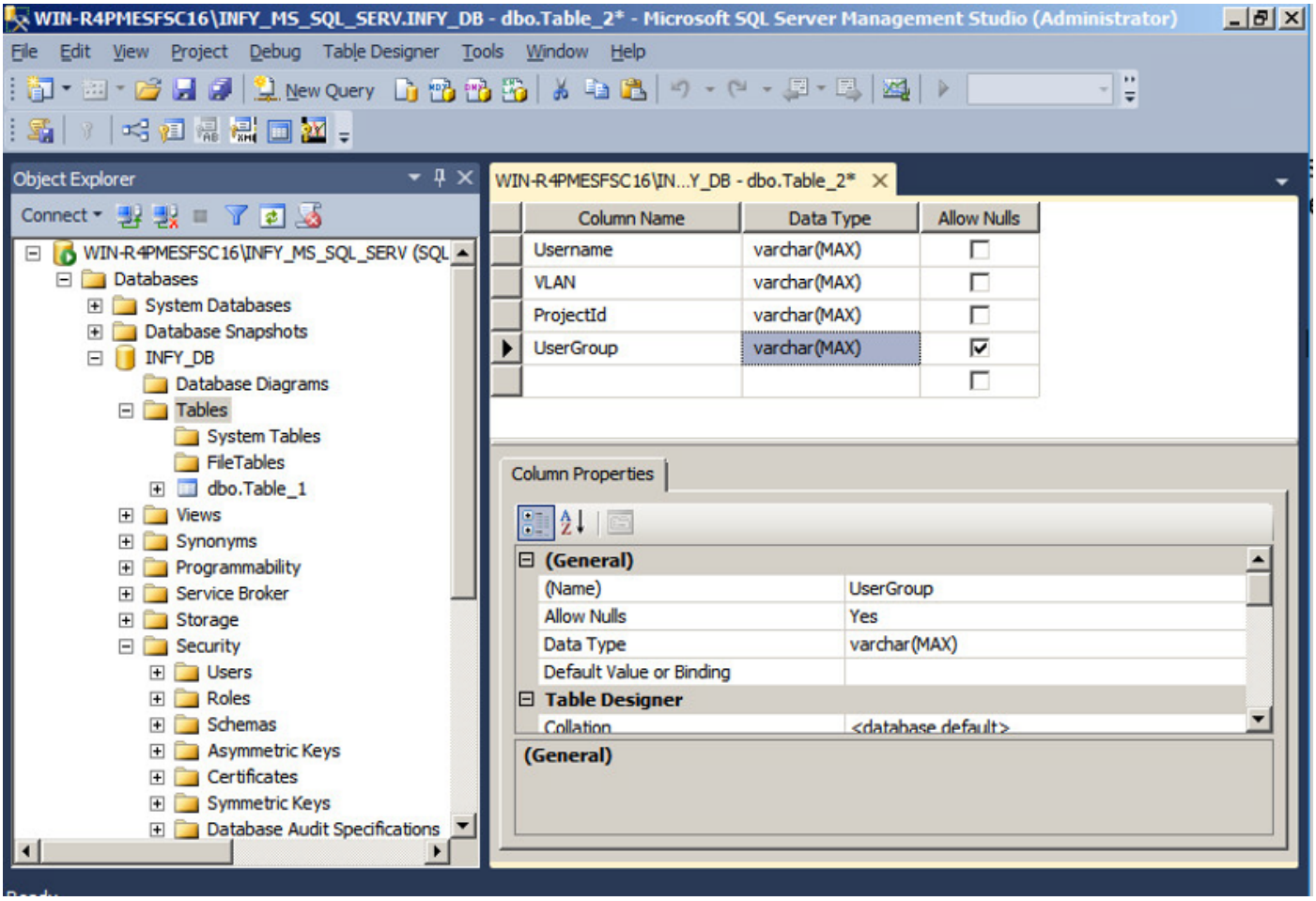
步驟1.開啟SQL Server Management Studio(開始**選單> Microsoft SQL Server)**以建立資料庫：



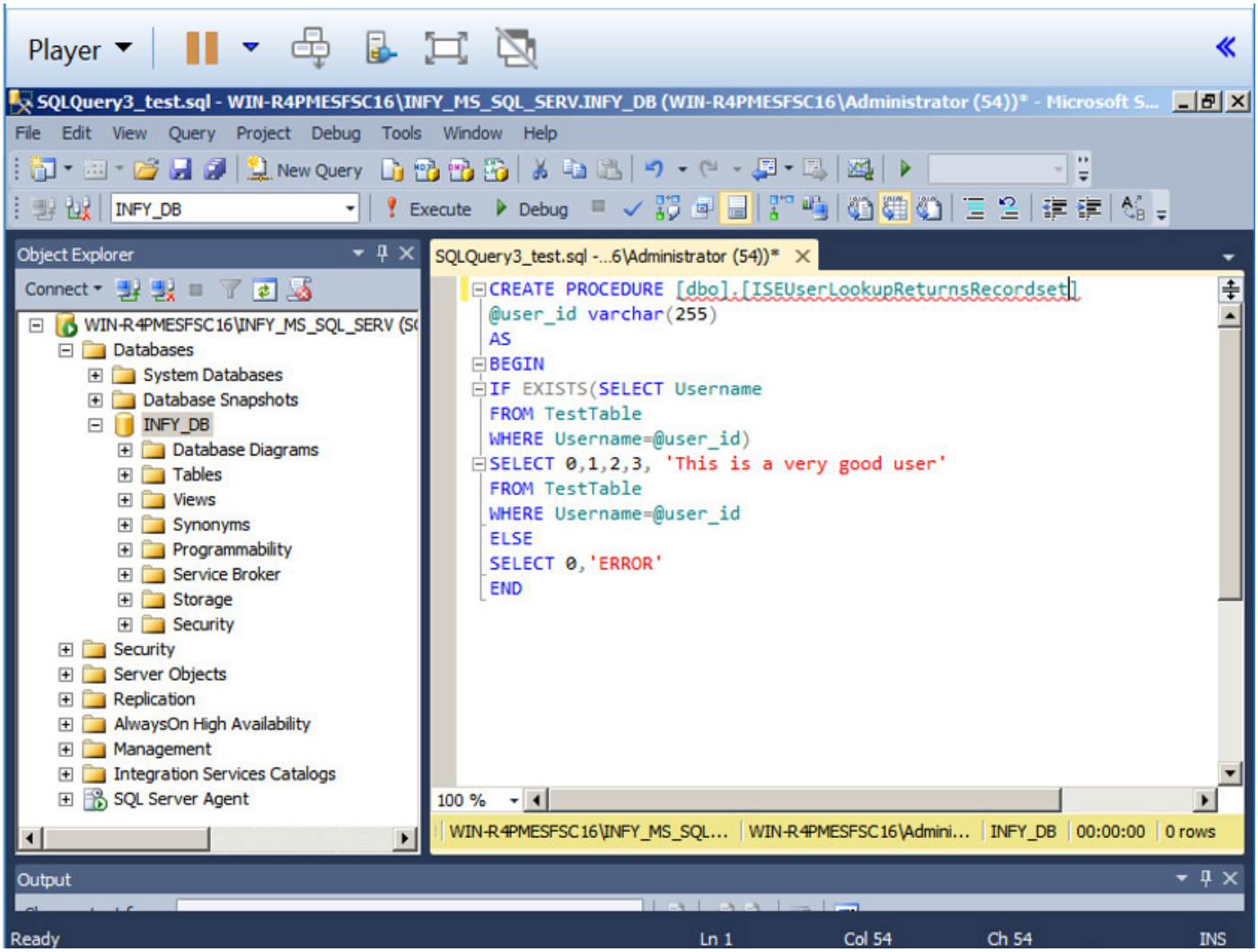
步驟2.提供名稱並建立資料庫。



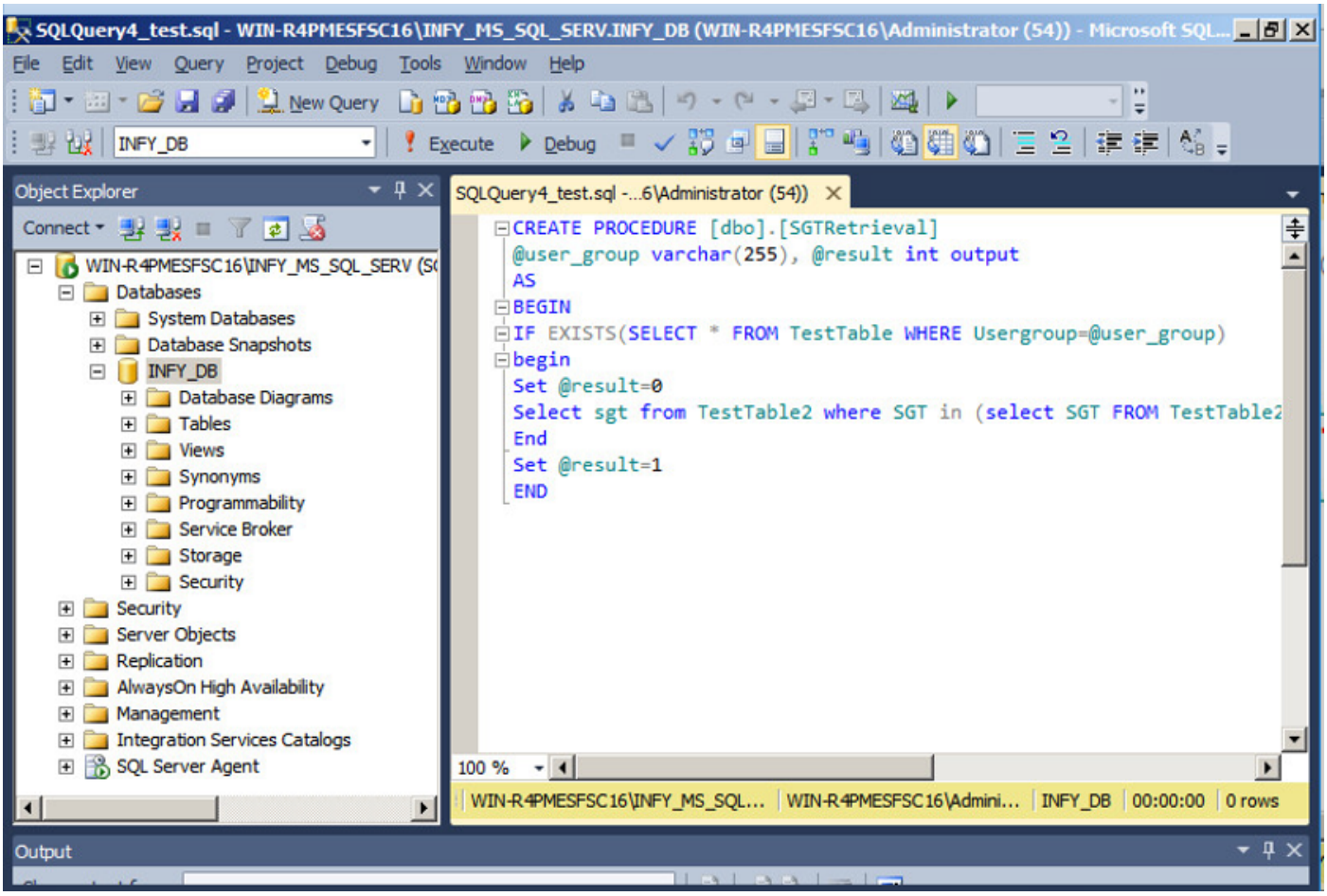
步驟3.建立一個新表，將所需列用作端點獲得授權的引數。



步驟4.建立一個**過程**，檢查使用者名稱是否存在。



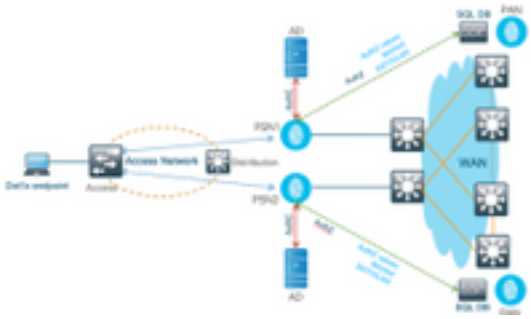
步驟5.建立從表中提取屬性(SGT)的過程。

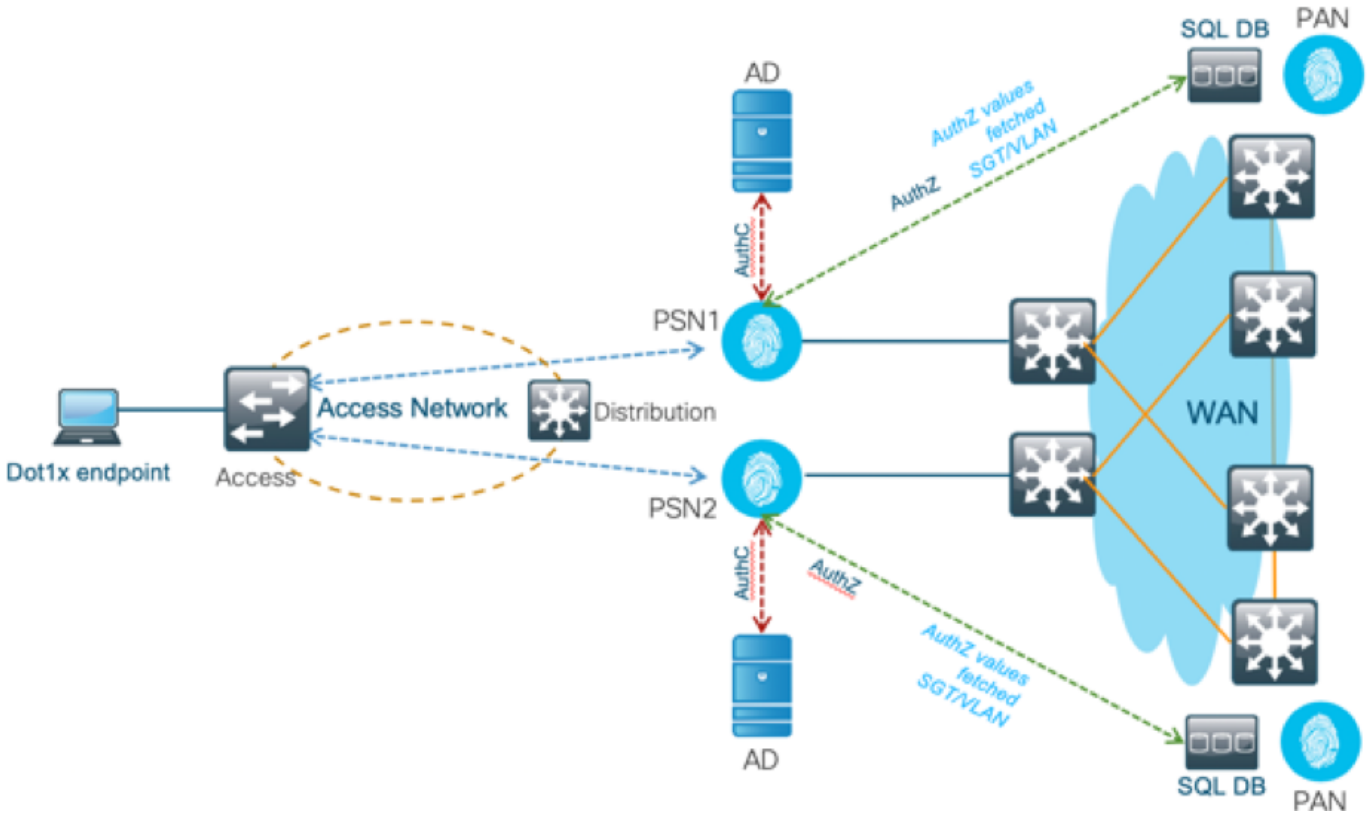


在本文檔中，思科ISE與Microsoft SQL解決方案整合，以滿足大型企業網路的授權規模要求。

解決方案工作流（ISE 2.7及更低版本）

在此解決方案中，思科ISE與Active Directory(AD)和Microsoft SQL整合。AD用作身份驗證ID儲存和MS SQL用於授權。在身份驗證過程中，網路接入裝置(NAD)將使用者憑證轉發到PSN - IBN解決方案中的AAA伺服器。PSN使用Active Directory ID儲存驗證終端憑據並對使用者進行身份驗證。授權策略引用MS SQL資料庫來獲取授權結果，例如**user-id**用作引用的SGT/VLAN。





優勢

此解決方案具有以下優點，使其具有靈活性：

- 思科ISE可以利用外部資料庫提供的所有其他功能。
- 此解決方案不依賴於任何思科ISE規模限制。

缺點

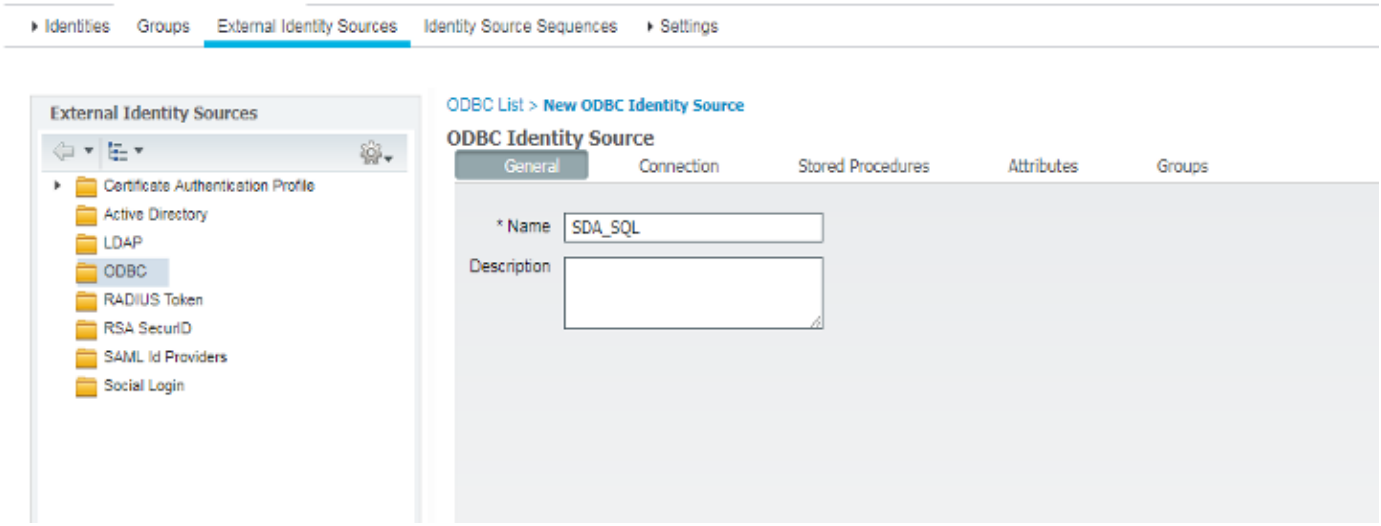
此解決方案具有以下缺點：

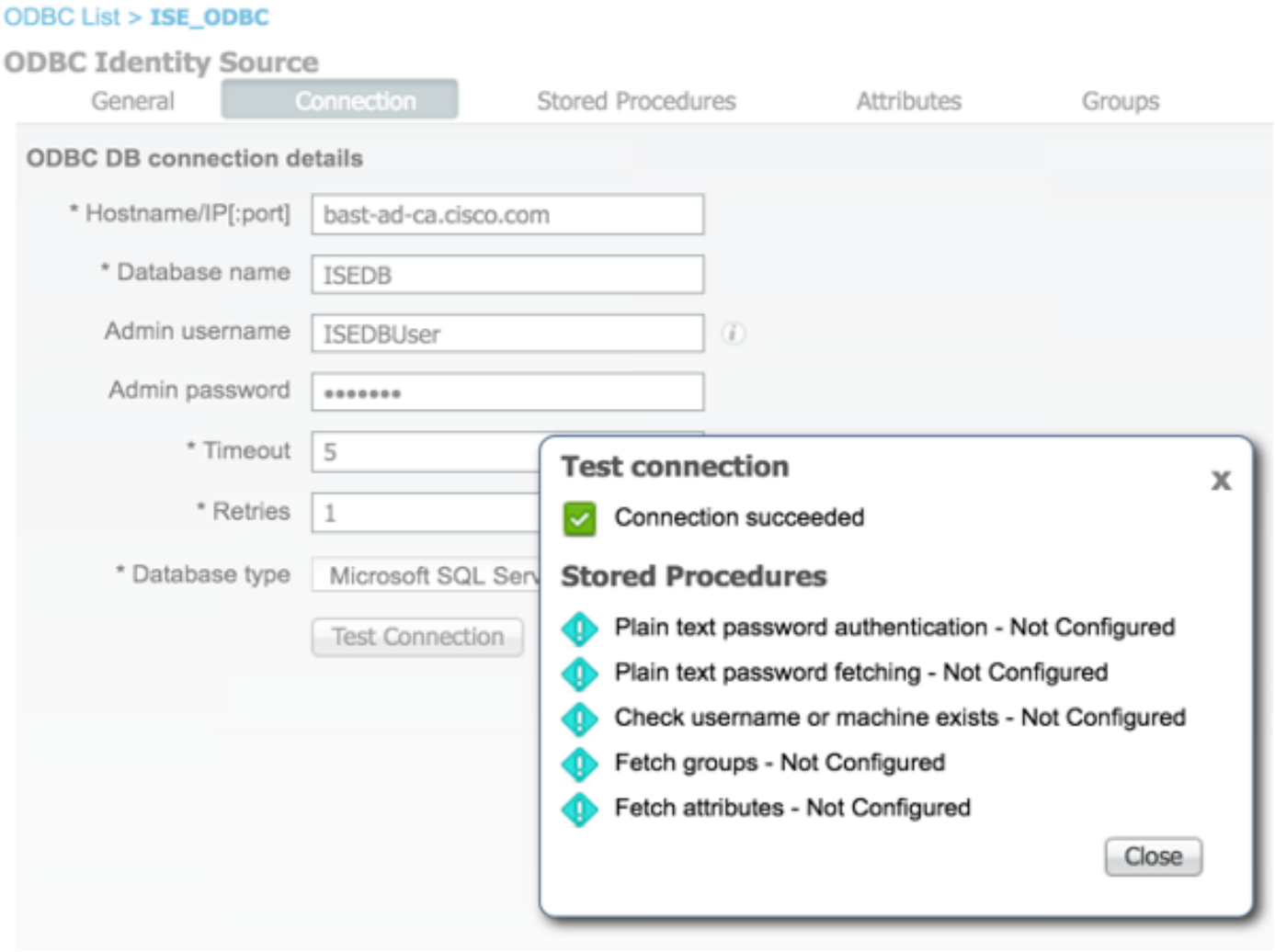
- 需要額外的程式設計以使用終結點憑據填充外部資料庫。
- 如果外部DB不像PSN一樣本地存在，則此解決方案依賴於WAN，而WAN使其成為終端AAA資料流中的第^{3}個故障點。
- 需要更多知識來維護外部資料庫進程和過程。
- 必須考慮將使用者ID手動配置到資料庫導致的錯誤。

外部資料庫示例配置

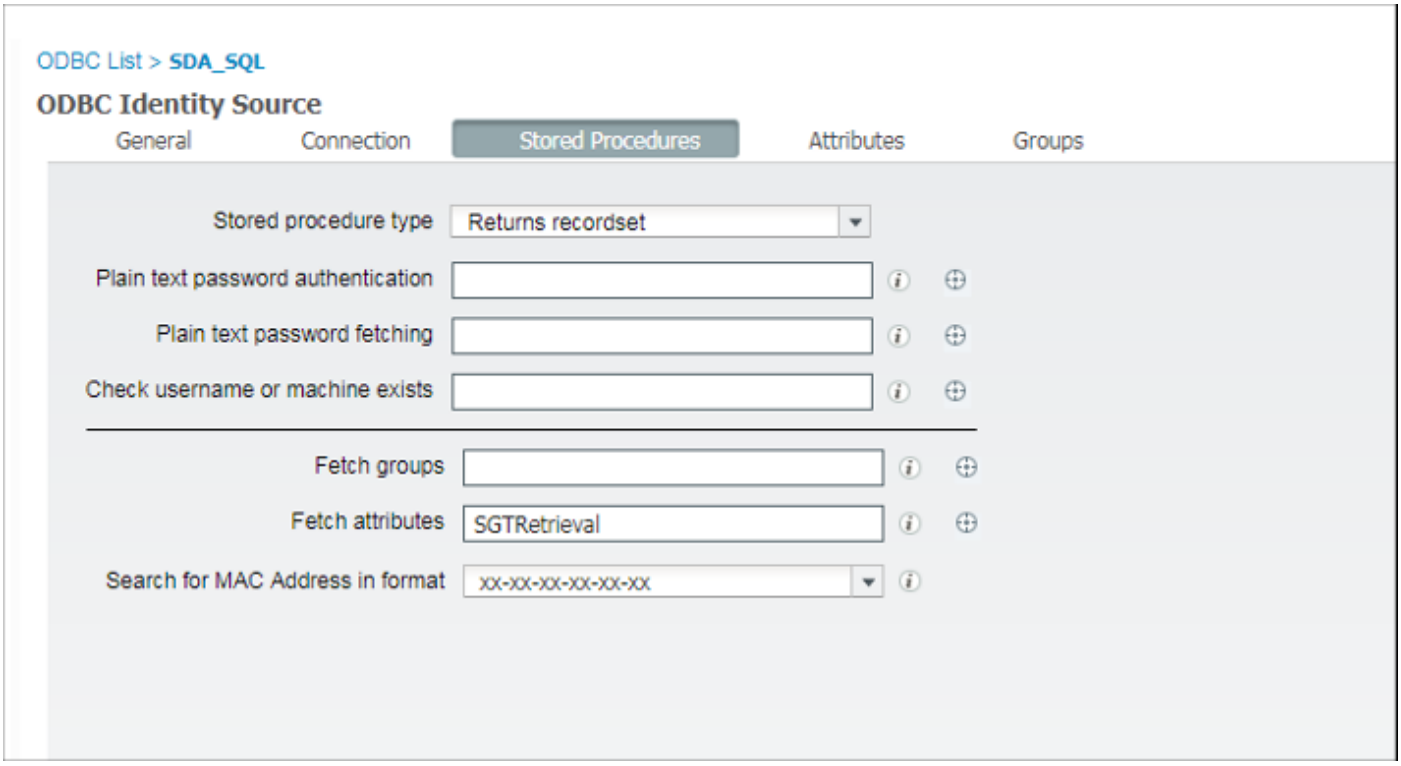
在本文檔中，Microsoft SQL顯示為用作授權點的外部資料庫。

步驟1.從**Administration > External Identity Source > ODBC**選單建立思科ISE中的ODBC身份儲存並測試連線。

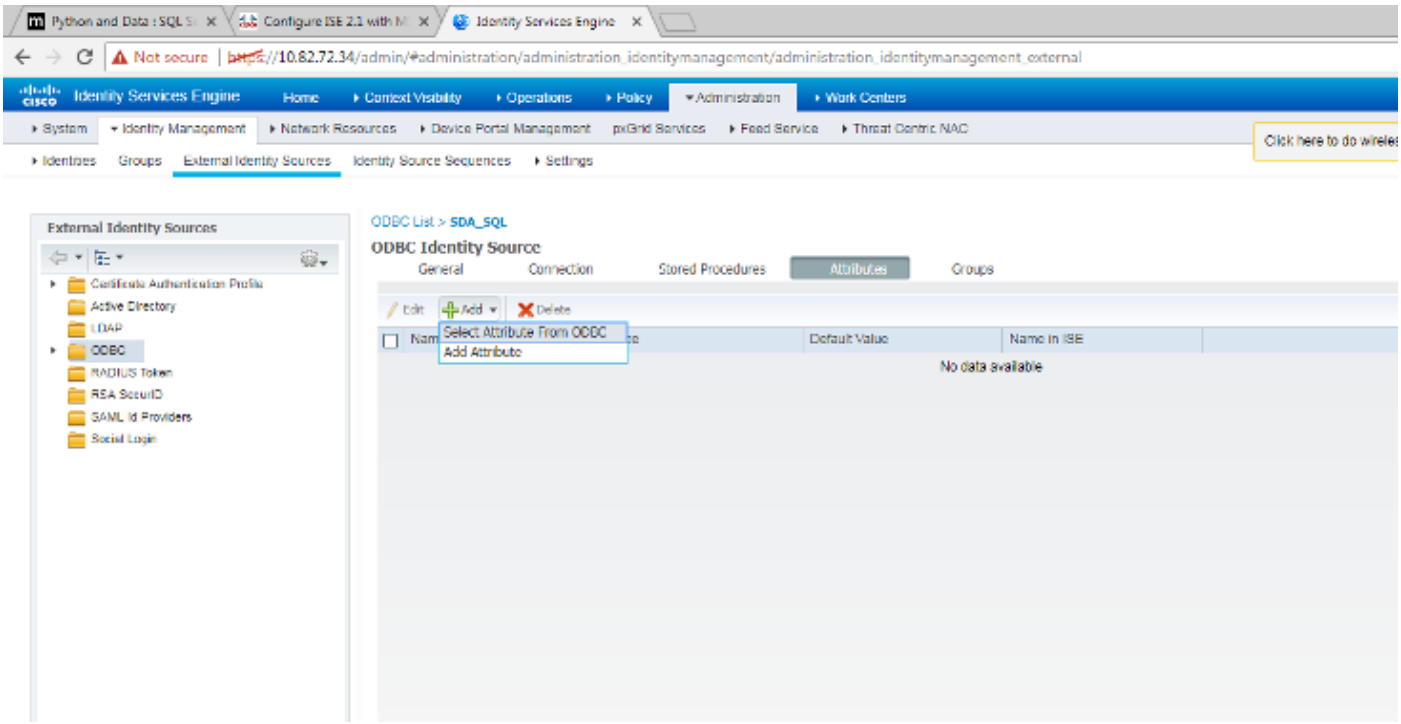


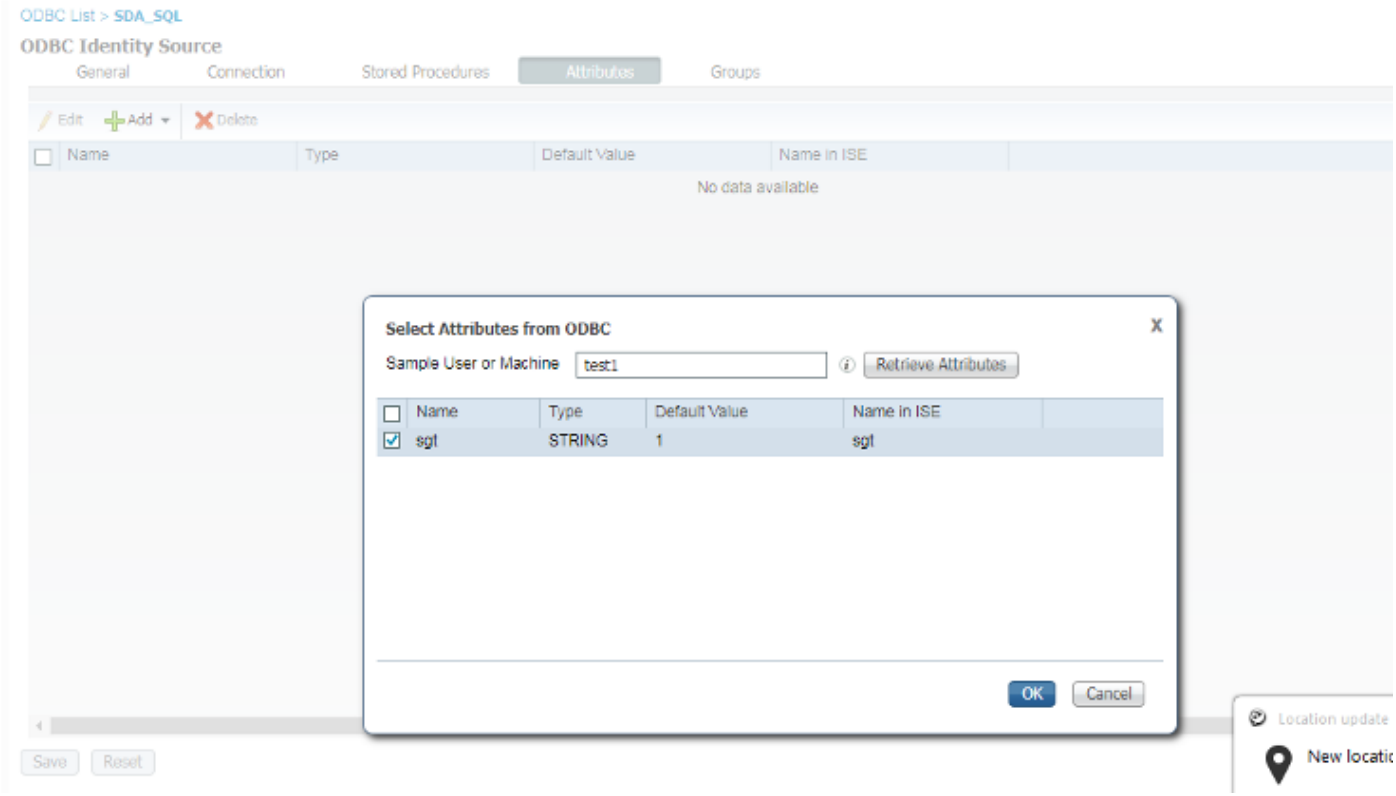


步驟2.導航至ODBC頁面上的[儲存過程]頁籤以配置在Cisco ISE中建立的過程。

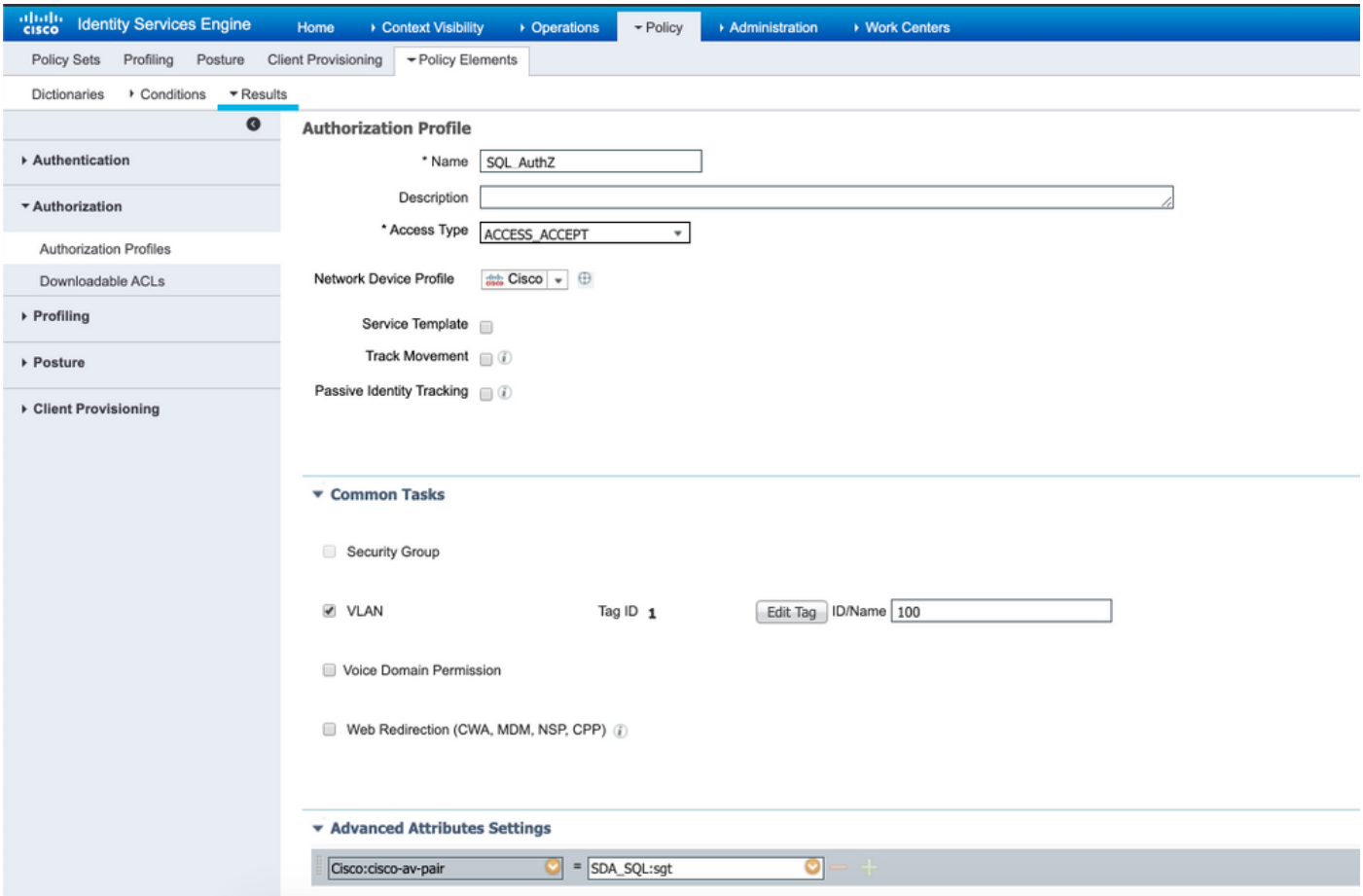


步驟3.從ODBC ID源提取使用者ID的屬性以進行驗證。

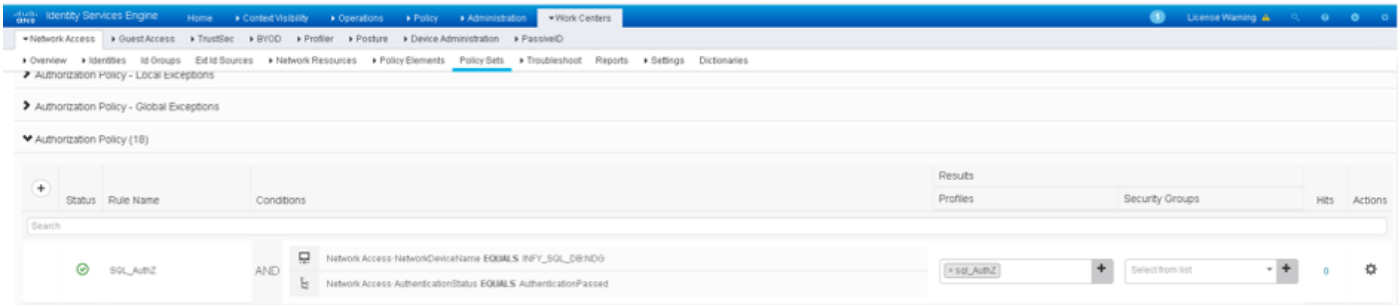




步驟4.建立授權**配置檔案**並進行配置。在Cisco ISE中，轉至**Policy > Results > Authorization profile > Advanced Attributes Settings**，然後將該屬性選擇為**Cisco:cisco-av-pair。**選擇值作為<name of ODBC database>:sgt，然後儲存它。



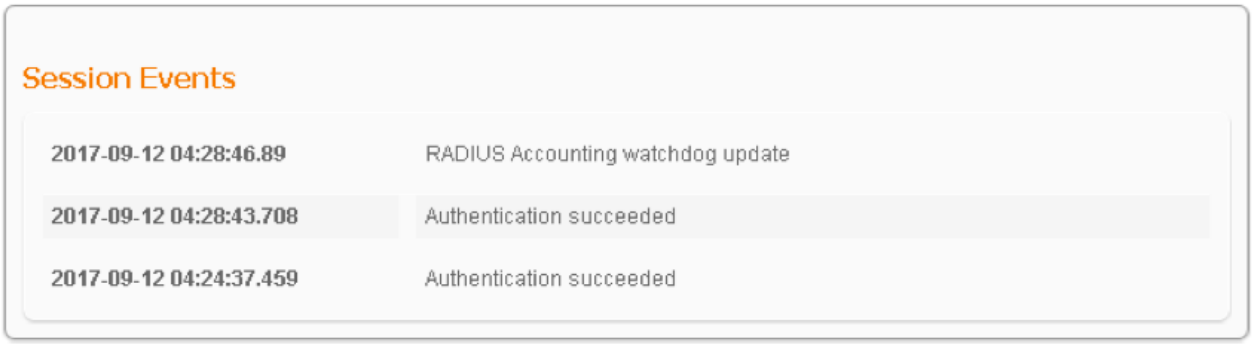
步驟5.建立授**權策略**並進行配置。在Cisco ISE中，導航到**Policy > Policy sets > Authorization Policy > Add**。將條件設定為身份源是SQL Server。選擇結果配置檔案作為先前建立的授權配置檔案。



步驟6.一旦使用者通過驗證和授權，日誌中將包含分配給使用者的sgt以進行驗證。

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



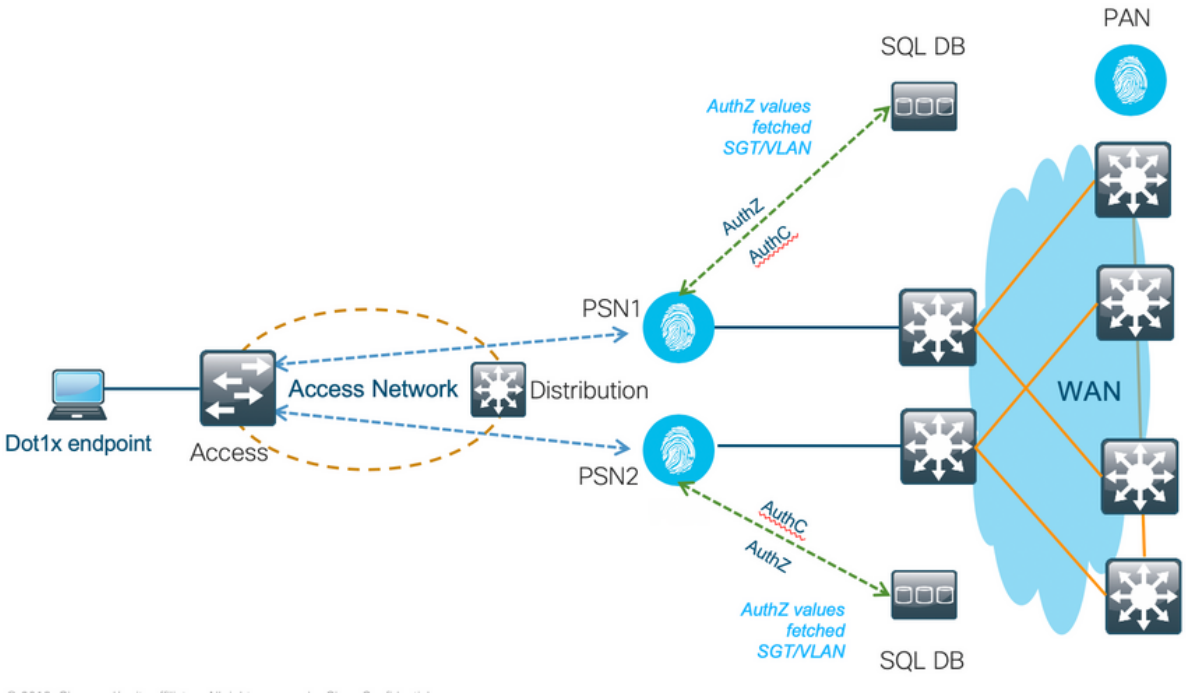
Session Events

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

解決方案工作流（ISE 2.7之後）

在ISE 2.7之後，授權屬性可以從ODBC中獲取，如Vlan、SGT、ACL，這些屬性可以在策略中使用。

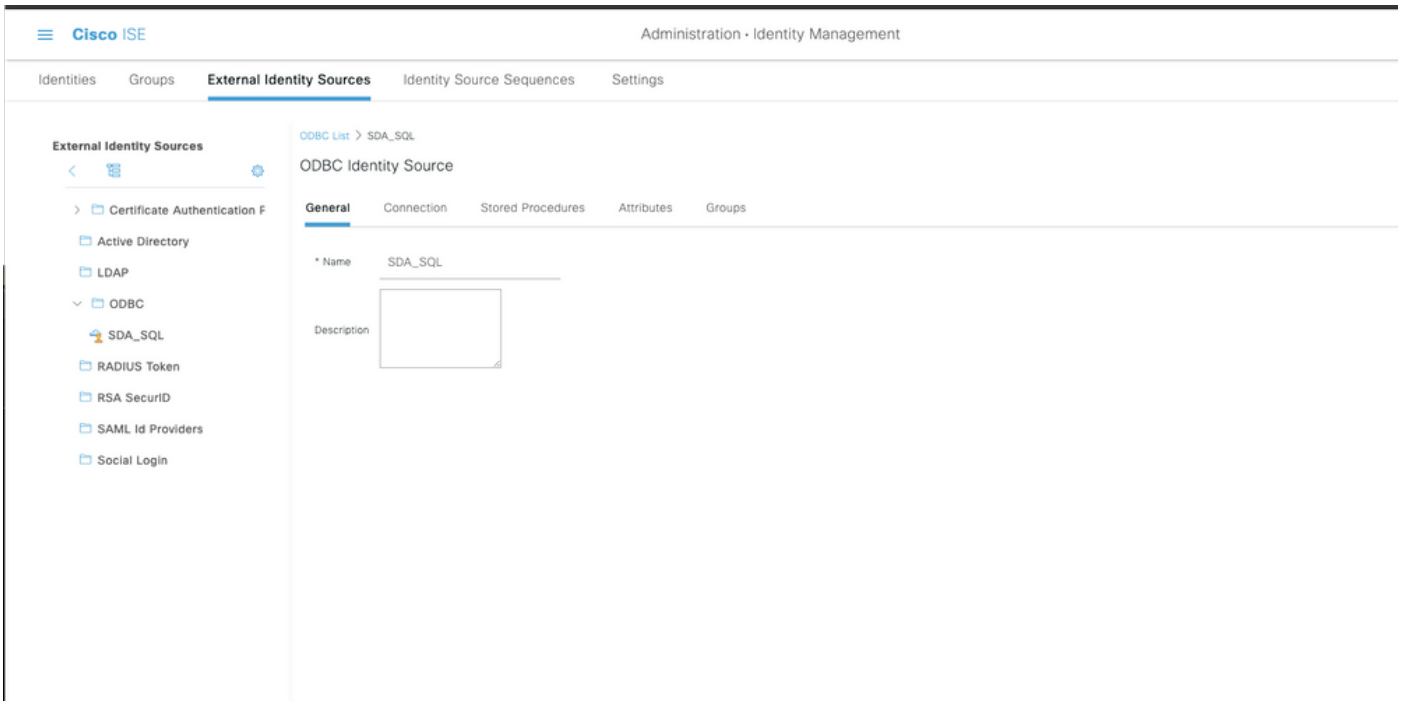
在此解決方案中，思科ISE與Microsoft SQL整合。MS SQL用作身份驗證和授權的ID儲存。當來自端點的憑證被提供給PSN時，它將根據MS SQL資料庫驗證憑證。授權策略引用MS SQL資料庫來獲取授權結果，例如**user-id**用作參考的SGT/VLAN。



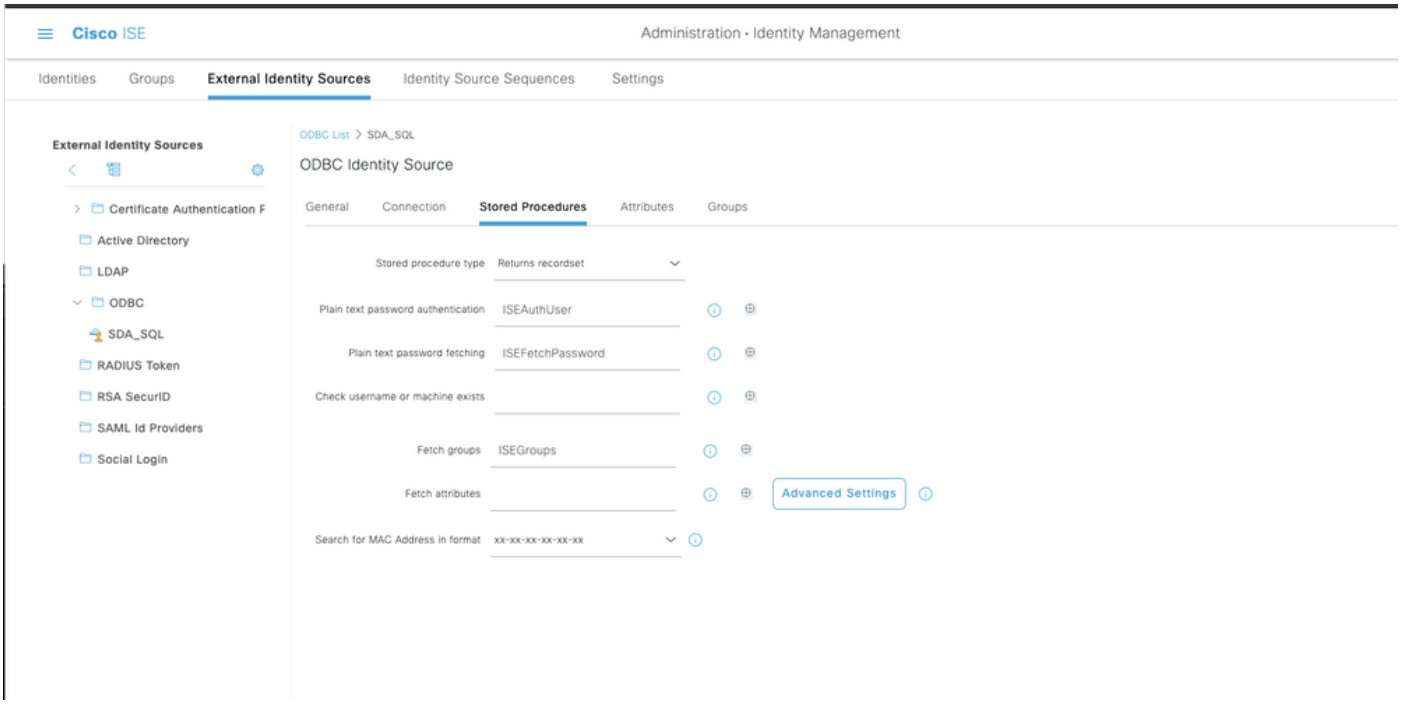
外部資料庫示例配置

按照本文檔前面提供的步驟建立MS SQL資料庫以及使用者名稱、密碼、VLAN ID和SGT。

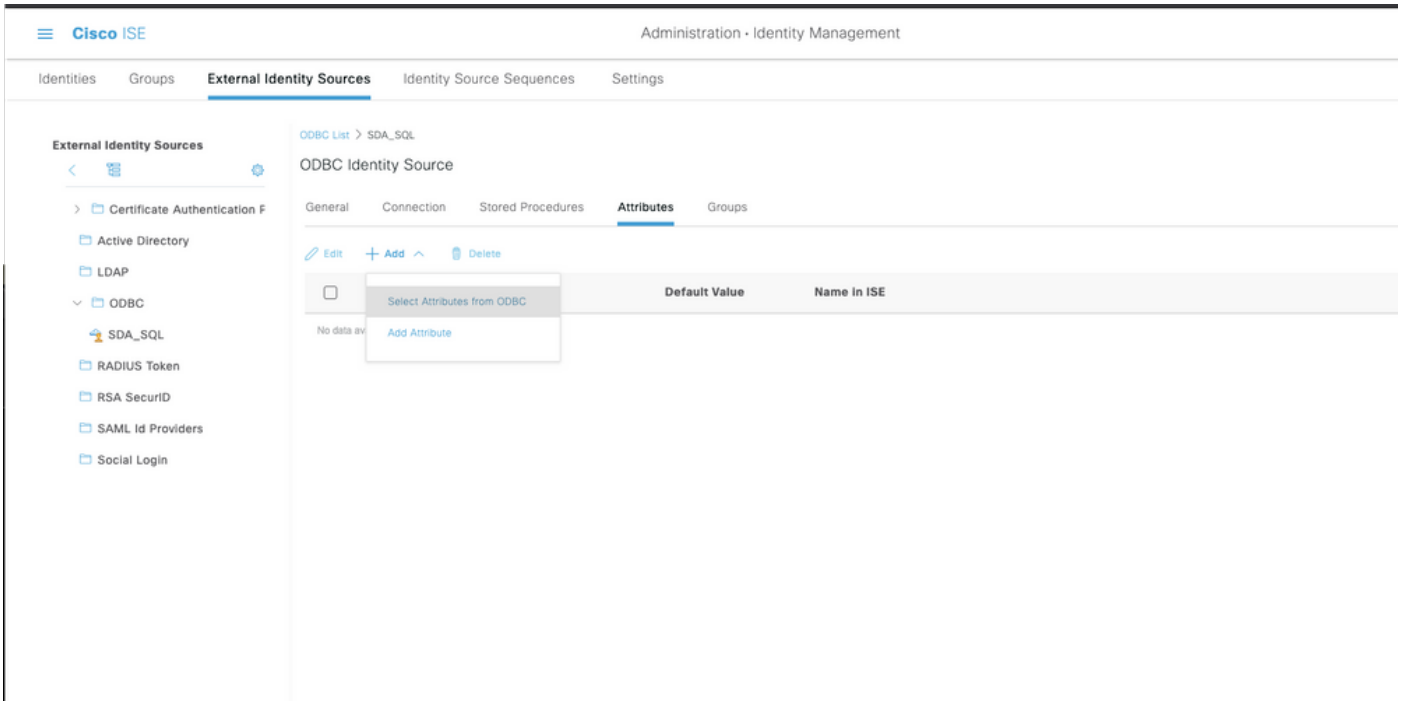
步驟1.從**Administration > External Identity Source > ODBC**選單建立思科ISE中的ODBC身份儲存並測試連線。

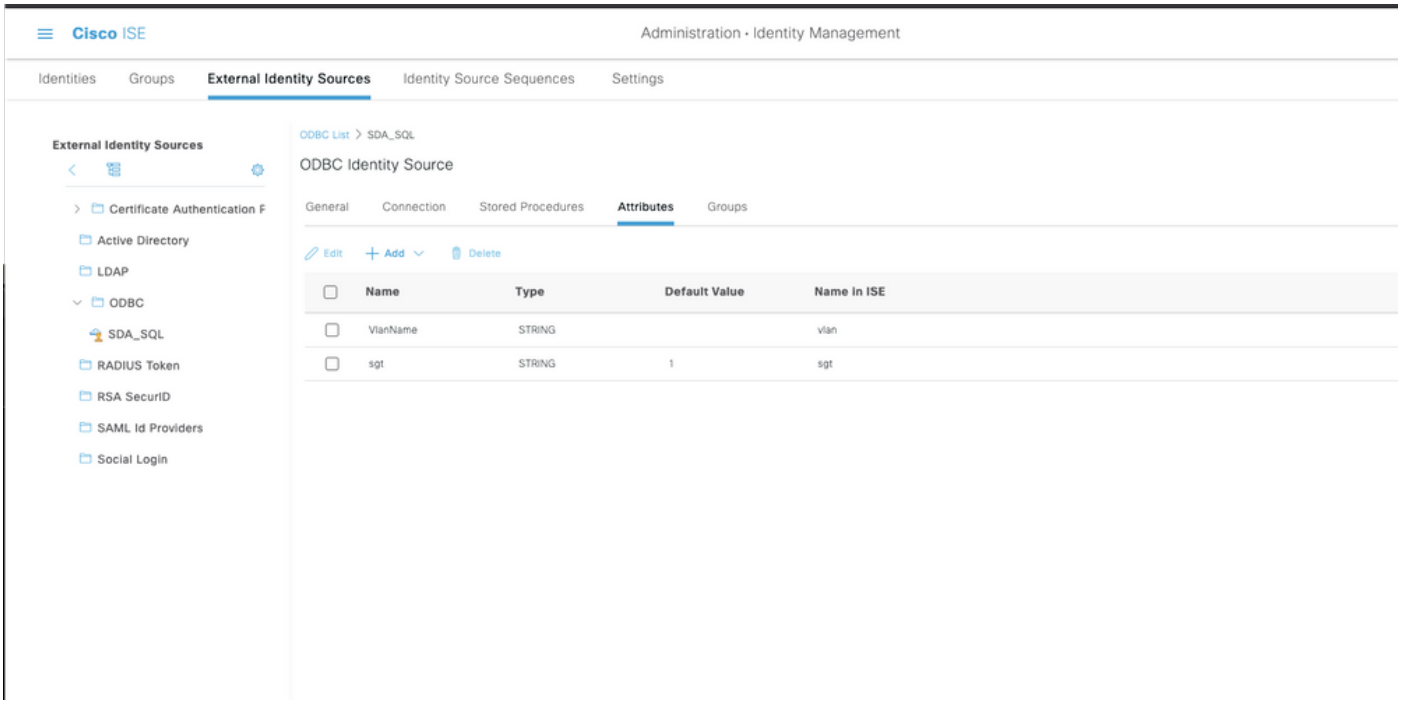


步驟2.導航至ODBC頁面上的[儲存過程]頁籤以配置在Cisco ISE中建立的過程。

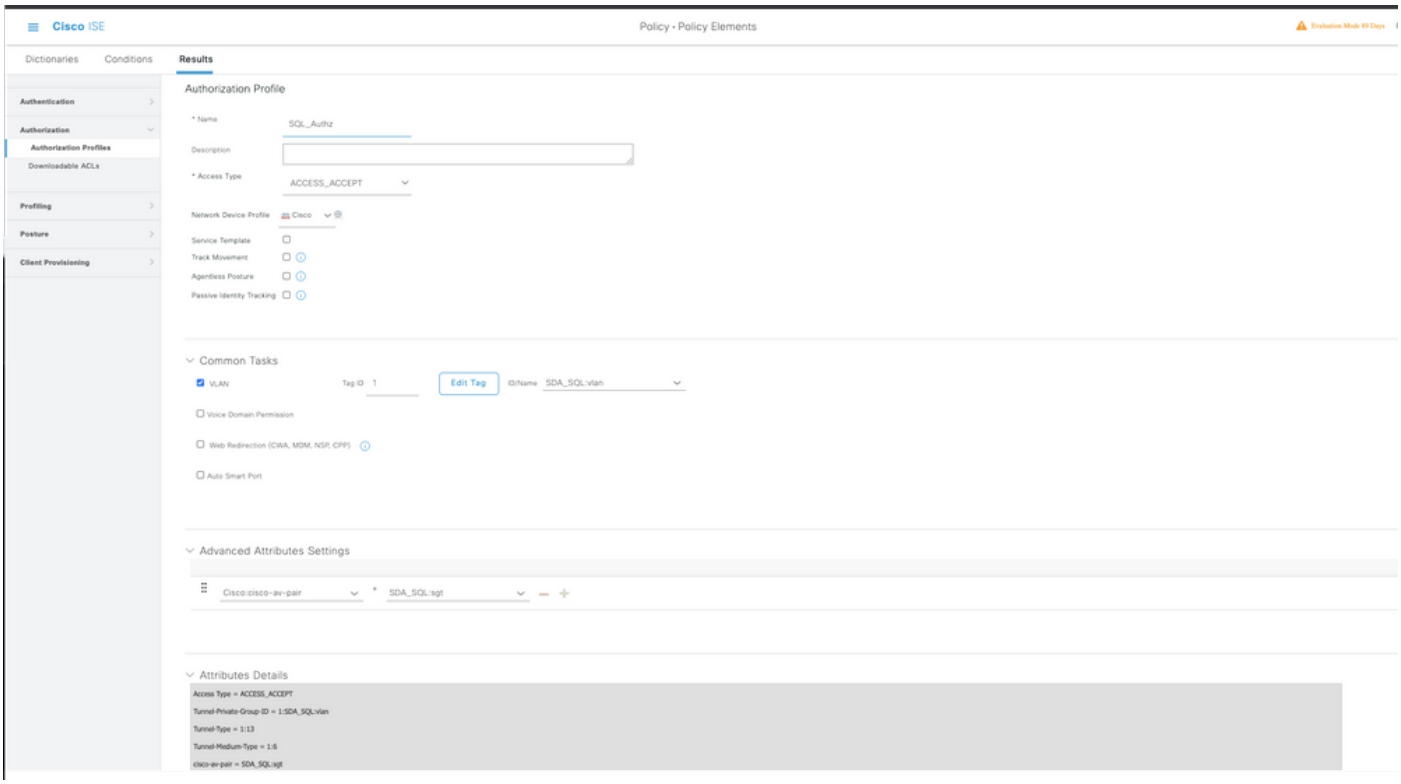


步驟3.從ODBC ID源提取使用者ID的屬性以進行驗證。

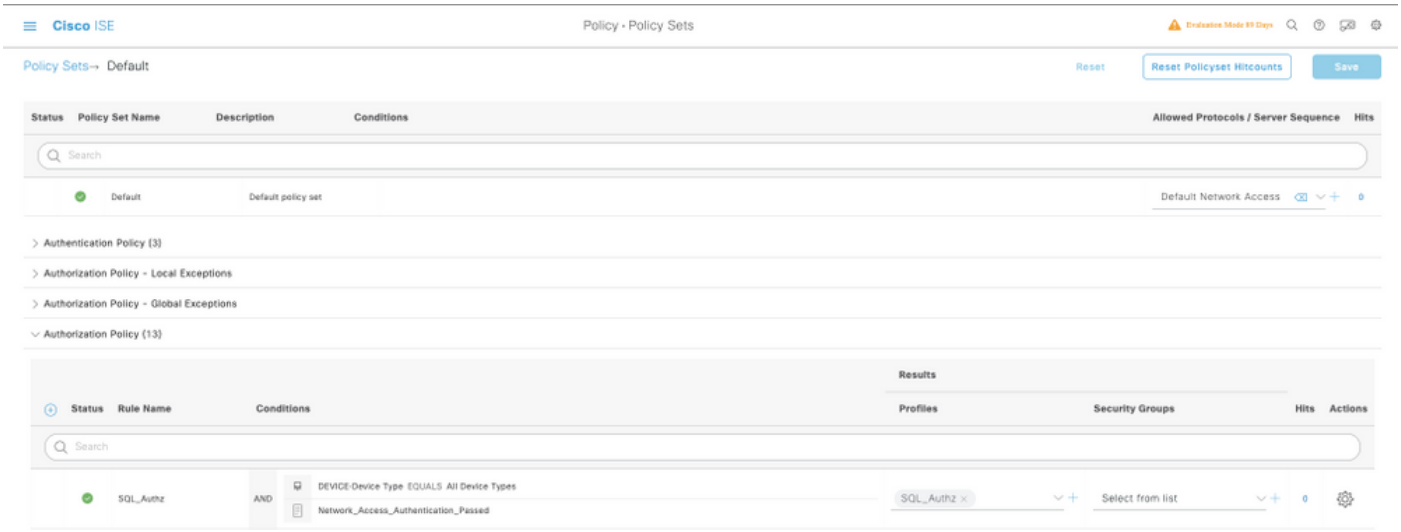




步驟4.建立授權**配置檔案**並進行配置。在Cisco ISE中，轉至**Policy > Results > Authorization profile > Advanced Attributes Settings**，然後將該屬性選擇為**Cisco:cisco-av-pair。** 選擇值為<name of ODBC database>:sgt。在Common Tasks下，選擇**VLAN**，其ID/Name為<name of ODBC database>:vlan，然後將其儲存



步驟5.建立授**權策略**並進行配置。在Cisco ISE中，導航到**Policy > Policy sets > Authorization Policy > Add**。將條件設定為身份源是SQL Server。選擇結果配置檔案作為先前建立的授權配置檔案。

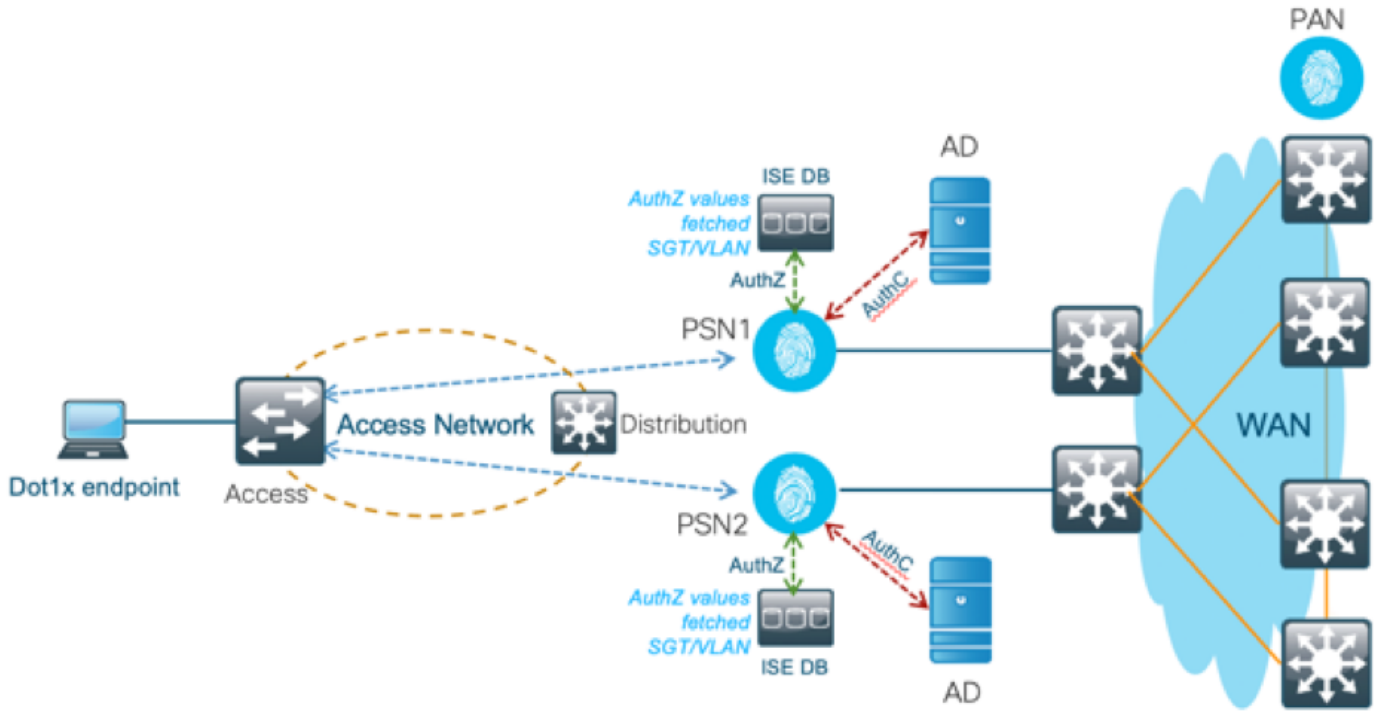


使用內部資料庫

思科ISE本身有一個內建資料庫，可用於擁有使用者ID進行授權。

解決方案工作流

在此解決方案中，思科ISE的內部資料庫用作授權點，而Active Directory(AD)繼續作為身份驗證源。Cisco ISE DB中包含端點的使用者ID以及返回授權結果（如SGT或VLAN）的**自定義**屬性。將來自終端的憑證提供給PSN時，它會使用Active Directory ID儲存檢查終端憑證的有效性，並對終端進行身份驗證。授權策略引用ISE DB獲取授權結果，例如SGT/VLAN，使用者ID用作參考。



優勢

此解決方案具有以下優點，使其成為靈活的解決方案：

- Cisco ISE DB是內建解決方案，因此與外部DB解決方案不同，它沒有第三個故障點。

- 由於Cisco ISE集群確保所有角色之間的即時同步，因此沒有WAN依賴性，因為PSN擁有從PAN即時推送的所有使用者ID和自定義屬性。
- 思科ISE可以利用外部資料庫提供的所有其他功能。
- 此解決方案不依賴於任何思科ISE規模限制。

缺點

此解決方案具有以下缺點：

- Cisco ISE DB可保留的最大使用者ID數為300,000。
- 必須考慮將使用者ID手動配置到資料庫導致的錯誤。

內部資料庫示例配置

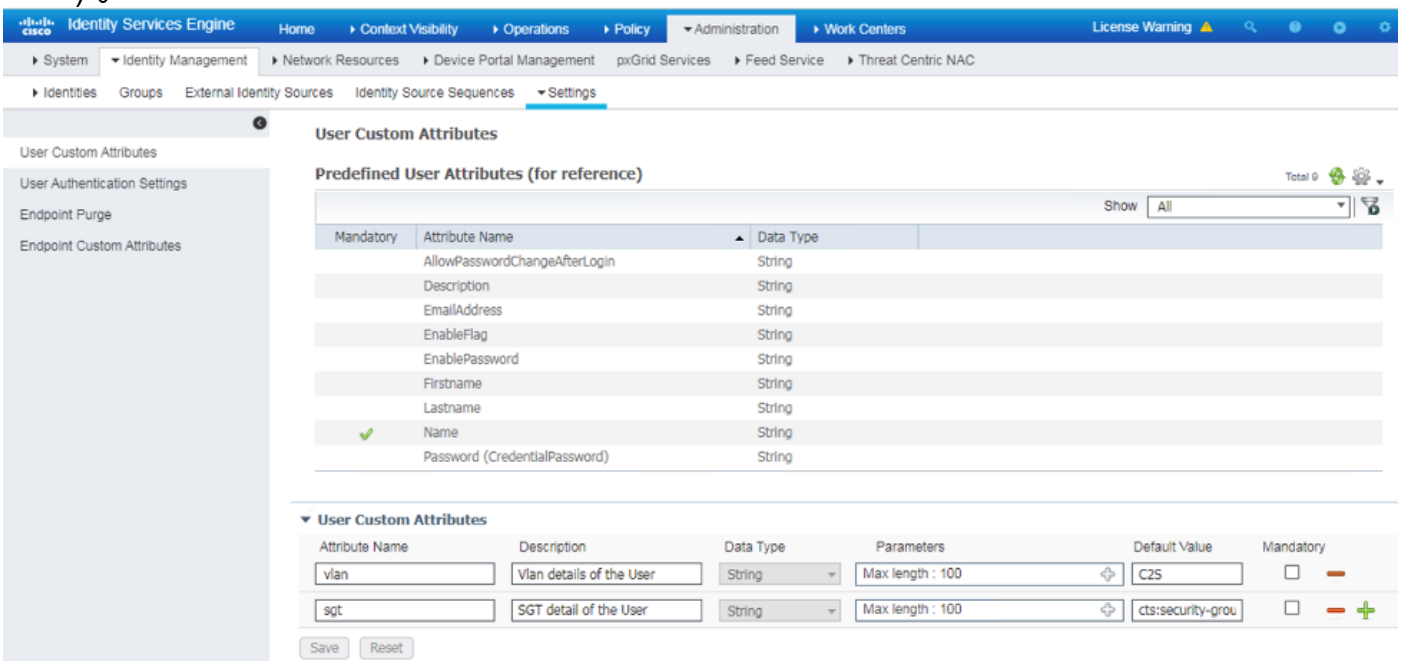
可使用自定義使用者屬性為內部ID儲存中的任何使用者配置每使用者VLAN和SGT。

步驟1.建立新使用者自定義屬性，以表示各自使用者的VLAN和SGT值。導航到**管理>身份管理>設定>使用者自定義屬性。建立新使用者自定義屬性，如下表所示。**

此處顯示ISE資料庫表以及自定義屬性。

屬性名稱	**資料型別**	**引數（長度）**	**預設值**
VLAN	字串	100	C2S（預設Vlan名稱）
sgt	字串	100	cts:security-group-tag=0003-0（預設SGT值）

- 在此案例中，VLAN值代表vlan name & sgt value代表SGT的cisco-av-pair屬性（十六進位制）。

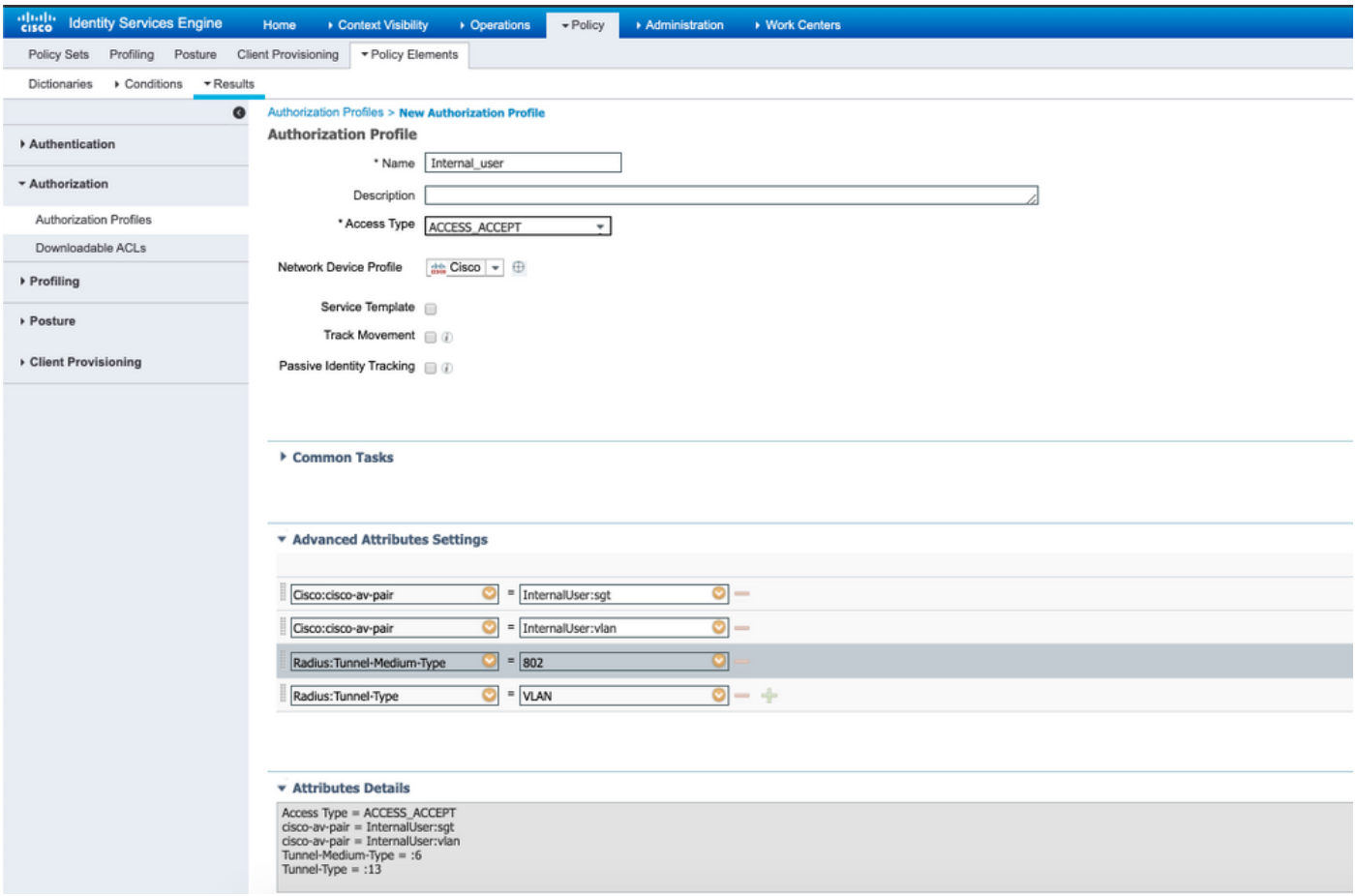


步驟2.使用使用者自定義屬性建立授權配置檔案，以表示各自使用者的vlan和sgt值。導航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add。**在Advanced Attributes Settings下新增下列屬性。

此表顯示了內部使用者的身份驗證配置檔案。

屬性	價值
Cisco:cisco-av-pair	內部使用者：sgt
Radius:Tunnel-Private-Group-ID	內部使用者：vlan
Radius:Tunnel-Medium-Type	802
Radius:Tunnel-Type	VLAN

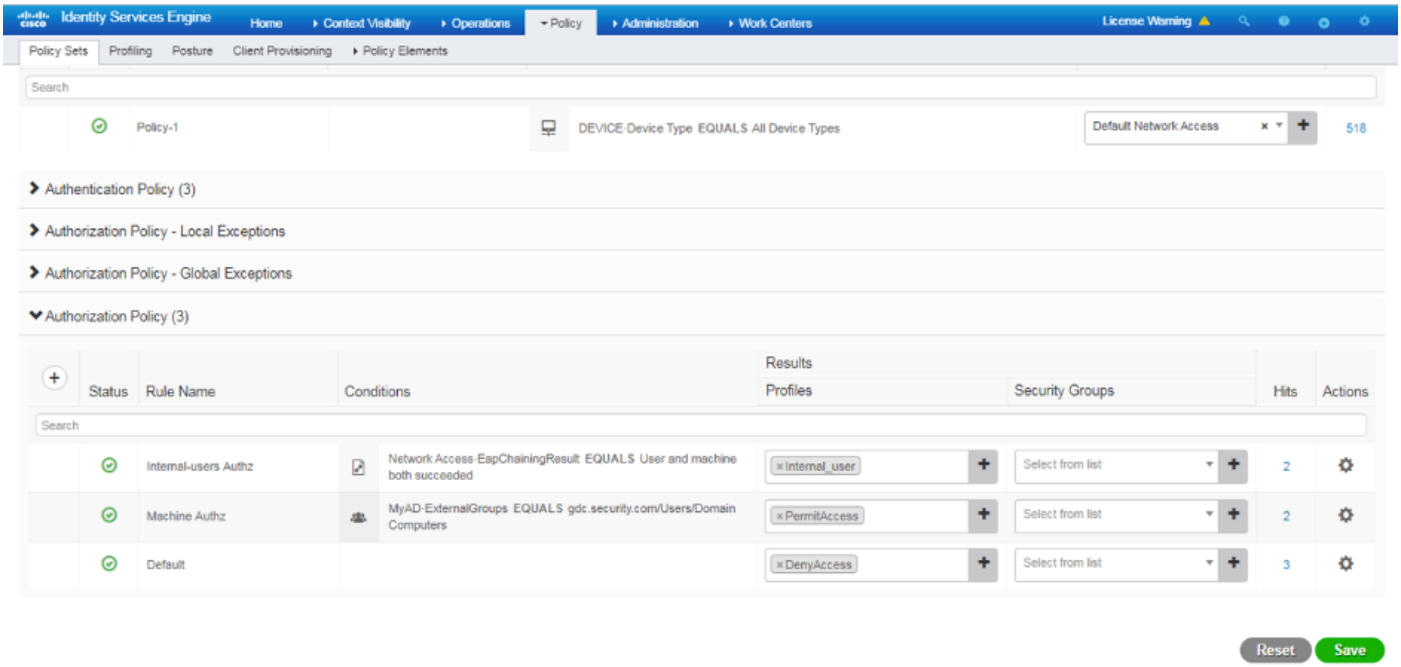
如圖所示，對於內部使用者，配置檔案**Internal_user**已分別配置為**InternalUser:sgt** & **InternalUser:vlan**的SGT和Vlan。



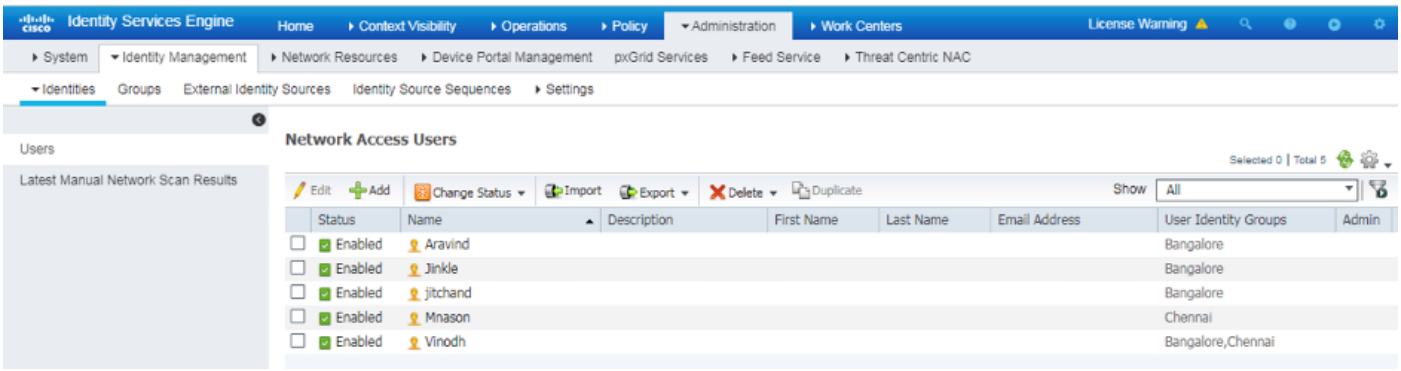
步驟3.建立授權策略，導航到**Policy > Policy Sets > Policy-1 > Authorization。使用下列條件建立授權策略並將其對映到各自的授權配置文**件。

此表顯示了內部使用者的身份驗證策略。

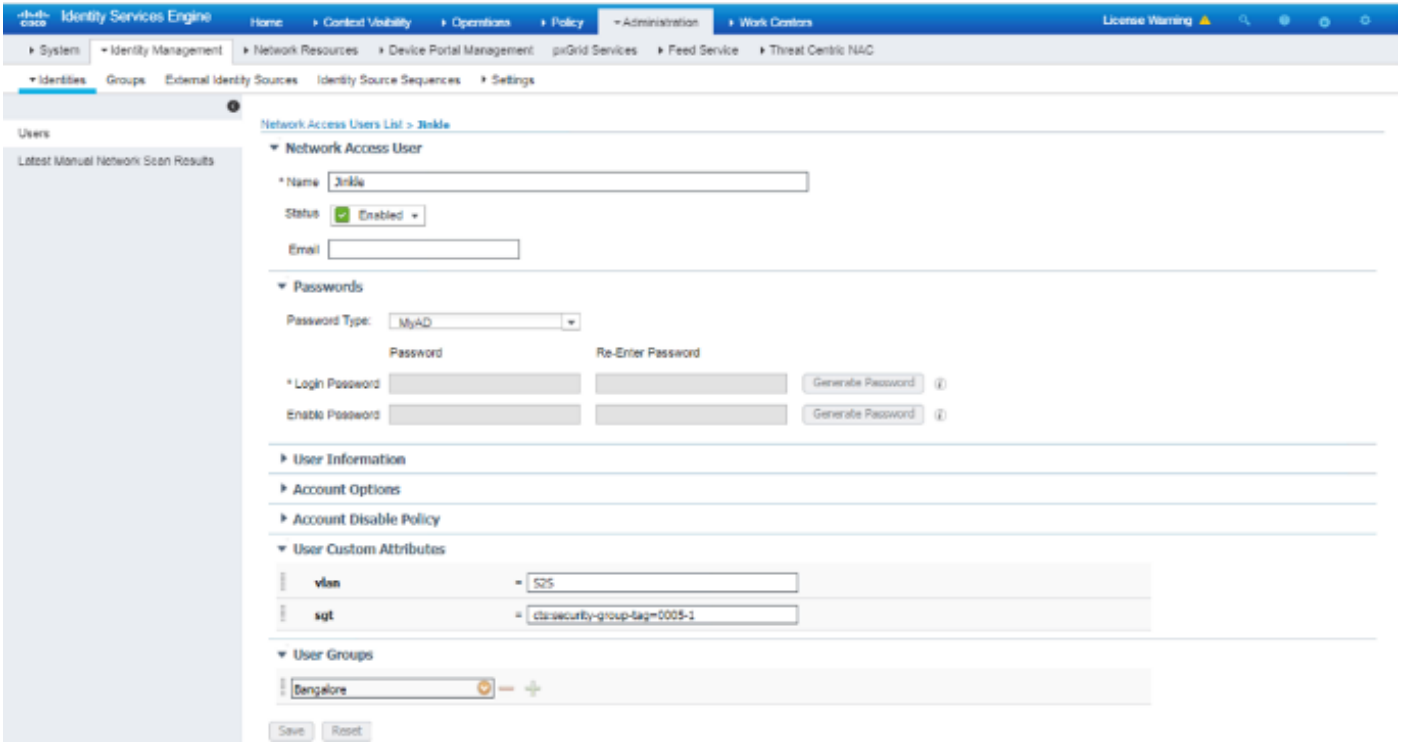
規則名稱	條件	結果授權配置檔案
Internal_User_Authz	如果網路訪問.EapChainingResults EQUALS使用者和電腦都成功	Internal_user
Machine_Only_Authz	如果MyAD.ExternalGroups等於 gdc.security.com/Users/Domain電腦	PermitAccess



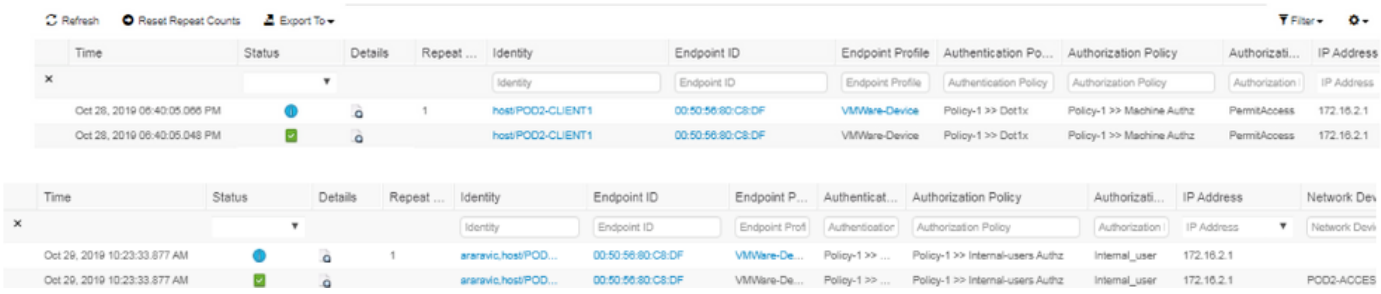
步驟4.在csv模板中使用自定義屬性及其各自的自定義屬性建立批次使用者身份。 通過導航到**管理>身份管理>身份>使用者>匯入>選擇檔案>匯入來匯入csv。**



此圖片顯示了具有自定義屬性詳細資訊的示例使用者。選擇使用者並按一下編輯以檢視對映到相應使用者的自定義屬性詳細資訊。



第5步：驗證即時日誌：



檢查**Result**部分以驗證**Vlan & SGT**屬性是否作為Access-Accept的一部分被傳送。

結論

此解決方案允許一些大型企業客戶擴展以滿足其需求。新增/刪除使用者id時需要小心。如果觸發錯誤，可能會導致正版使用者未經授權的訪問，反之亦然。

相關資訊

通過ODBC使用MS SQL配置Cisco ISE:

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

IPS簽名提示

AAA	驗證授權記帳
AD	Active Directory
AuthC	驗證
AuthZ	Authorization
資料庫	資料庫
DOT1X	802.1X
IBN	基於身份的網路
ID	身份資料庫
ISE	身分識別服務引擎
MnT	監控和故障排除
MsSQL	Microsoft SQL
ODBC	開放式資料庫連線

PAN	策略管理節點
PSN	策略服務節點
SGT	安全組標籤
SQL	結構化查詢語言
VLAN	虛擬LAN
WAN	廣域網

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。