使用ODBC和ISE DB（自定义属性）为大型园区网络简化访问策略

目录

简介

本文档介绍大规模园区部署，且不会影响其功能和安全实施。思科的终端安全解决方案 — 身份服务引擎(ISE)通过集成外部身份源满足此要求。

对于具有50多个地理位置、4000多个不同用户配置文件和600,000个或更多个终端的大型网络，传统IBN解决方案需要从不同的角度进行审视 — 不仅仅是功能，无论其是否随所有功能进行扩展。在当今传统的大型网络中，基于意图的网络(IBN)解决方案需要更多地关注可扩展性和易管理性，而不仅仅是功能。

先决条件

要求

Cisco 建议您了解以下主题：

- Dot1x/MAB身份验证
- 思科身份服务引擎(CiscoISE)
- 思科TrustSec(CTS)

使用的组件

本文档中的信息基于以下软件和硬件版本：

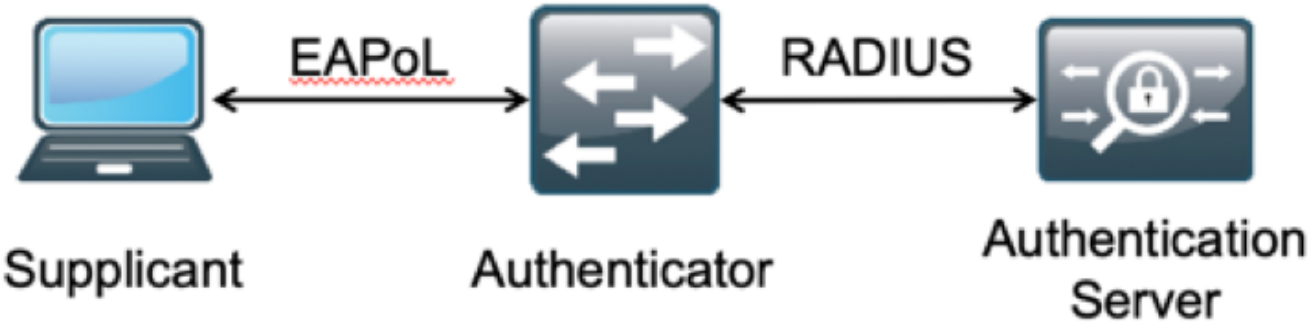
- 思科身份服务引擎(ISE)版本2.6补丁2和版本3.0
- Windows Active Directory(AD)Server 2008版本2
- Microsoft SQL Server 2012

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果网络处于活动状态，请确保了解任何配置的潜在影响。

背景信息

在基于身份的网络(IBN)解决方案中，基本元素是Supplicant客户端、身份验证器和身份验证(AAA)服务器。请求方是终端上的代理，在请求网络访问时提供凭证。身份验证器或NAS（网络接入服务器）是接入层，包括网络交换机和WLC，它们将凭证传输到AAA服务器。身份验证服务器根据ID存储验证用户身份验证请求，并使用访问接受或访问拒绝进行授权。ID存储可以位于AAA服务器或外部专用服务器上。

此图显示了基本IBN元素。



RADIUS是基于用户数据报协议(UDP)的协议，身份验证和授权结合到一起。在思科的企业园区IBN解决方案中，ISE的策略服务节点(PSN)角色充当AAA服务器，根据企业ID存储对终端进行身份验证并根据条件进行授权。

在Cisco ISE中，身份验证和授权策略配置为满足这些要求。身份验证策略包括有线或无线介质类型以及用于用户验证的EAP协议。授权策略包括定义各种终端匹配条件的条件以及网络访问结果，可以是VLAN、可下载ACL或安全组标记(SGT)。 这些是ISE可配置的最大策略规模数。

此表显示思科ISE策略扩展。

属性	**缩放编号**
身份验证规则的最大数量	1000（策略集模式）
授权规则的最大数量	3,000（策略集模式）

技术趋势

分段已成为当今企业网络的主要安全要素之一，无需实际部署边缘网络。允许终端在内部和外部网络之间漫游。分段有助于遏制特定网段上要扩展至整个网络的任何安全攻击。当今的软件定义访问(SDA)解决方案在Cisco ISE的TrustSec的帮助下提供了一种根据客户业务模式进行分段的方法，从而避免对VLAN或IP子网等网络元素的依赖。

问题

对于具有500多个不同终端配置文件的大型企业网络的ISE策略配置，授权策略的数量可能会增加到一个无法管理的点。即使Cisco ISE支持专用授权条件来满足如此大量的用户配置文件，管理员管理这些数量的策略也会面临挑战。

此外，客户可能需要通用授权策略而不是专用策略，以避免管理开销，并且还能根据终端标准为终端提供差异化的网络访问。

例如，假设企业网络以Active Directory(AD)作为真理来源，而端点的独特优势是AD中的属性之一。在这种情况下，传统的策略配置方式为每个唯一的终端配置文件提供更多授权策略。

在此方法中，每个终端配置文件通过domain.com下的AD属性进行区分。因此，需要配置专用授权策略。

此表显示了传统授权策略。

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

建议方案

为了避免违反思科ISE支持的最大可扩展数量授权策略，推荐的解决方案是使用外部数据库授权每

个终端从其属性获取的授权结果。例如，如果将AD用作外部数据库进行授权，则可以引用任何未使用的用户属性（如Department或Pin代码），以提供与SGT或VLAN映射的授权结果。

这是通过思科ISE与外部数据库集成或在配置了自定义属性的ISE内部数据库内实现的。本节介绍以下两种方案的部署：

> **注意：**在两个选项中，数据库包含**user-id**，但不包含**DOT1X端点的密码。**DB仅用作**授权**点。身份验证仍可以继续作为客户的ID存储，在大多数情况下，它驻留在Active Directory(AD)服务器上。

使用外部数据库配置

Cisco ISE与外部数据库集成，用于终端凭证验证：

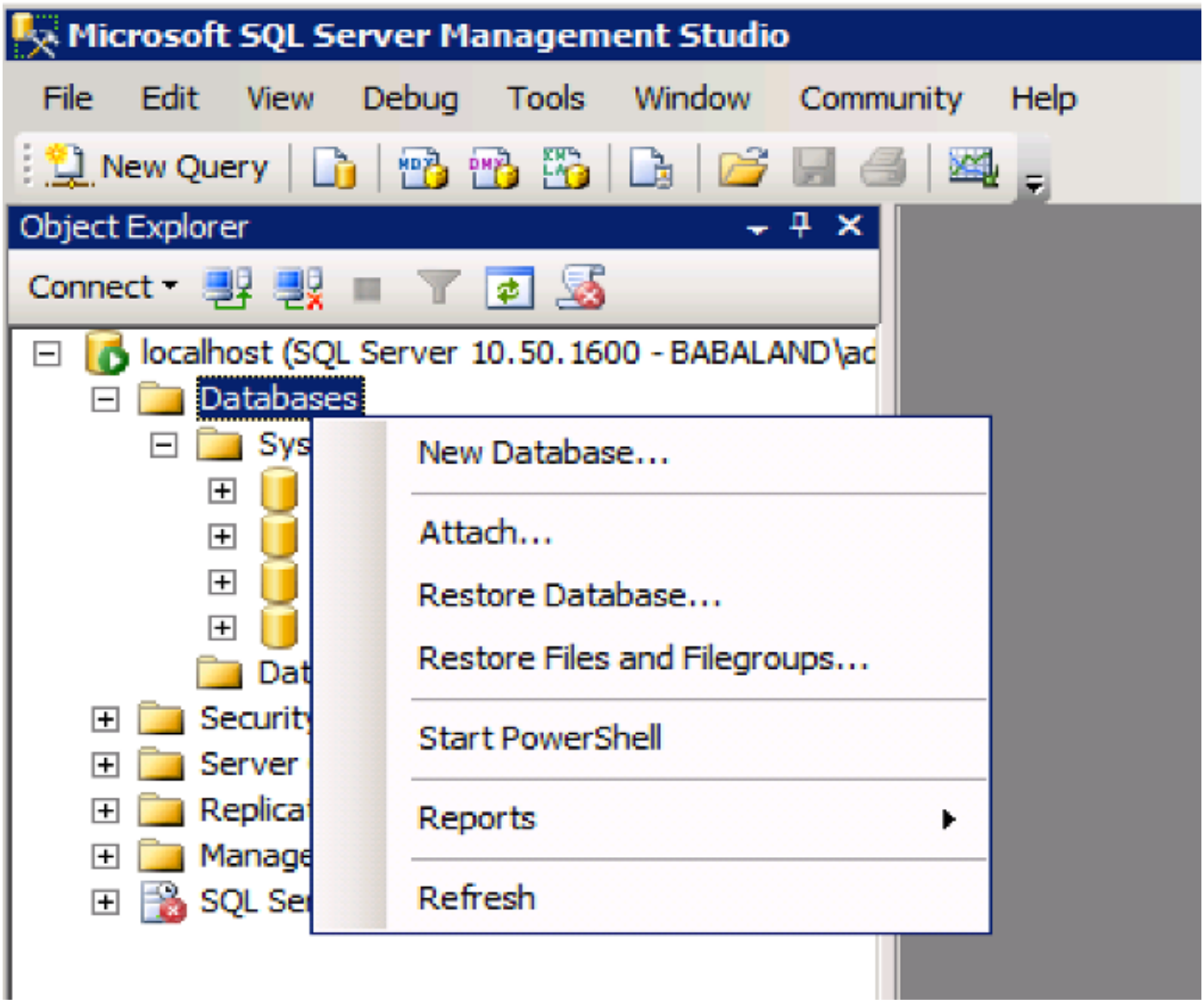
此表显示已验证的外部身份源。

外部身份源	**操作系统/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服务器	
SunONE LDAP目录服务器	V 5.2
OpenLDAP目录服务器	2.4.23 版
任何LDAP v3兼容服务器	—
令牌服务器	
RSA ACE/服务器	6.x系列
RSA身份验证管理器	7.x和8.x系列
任何符合RADIUS RFC 2865的令牌服务器	—
安全断言标记语言(SAML)单点登录(SSO)	
Microsoft Azure	—
Oracle Access Manager(OAM)	11.1.2.2.0 版
Oracle Identity Federation(OIF)	11.1.1.2.0 版
PingFederate服务器	6.10.0.4 版
PingOne云	—
安全身份验证	8.1.1
任何符合SAMLv2的身份提供程序	—
开放式数据库连接(ODBC)身份源	
Microsoft SQL Server(MS SQL)	Microsoft SQL Server 2012
甲骨文	企业版版本12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
社交登录（用于访客用户帐户）	
脸书	—

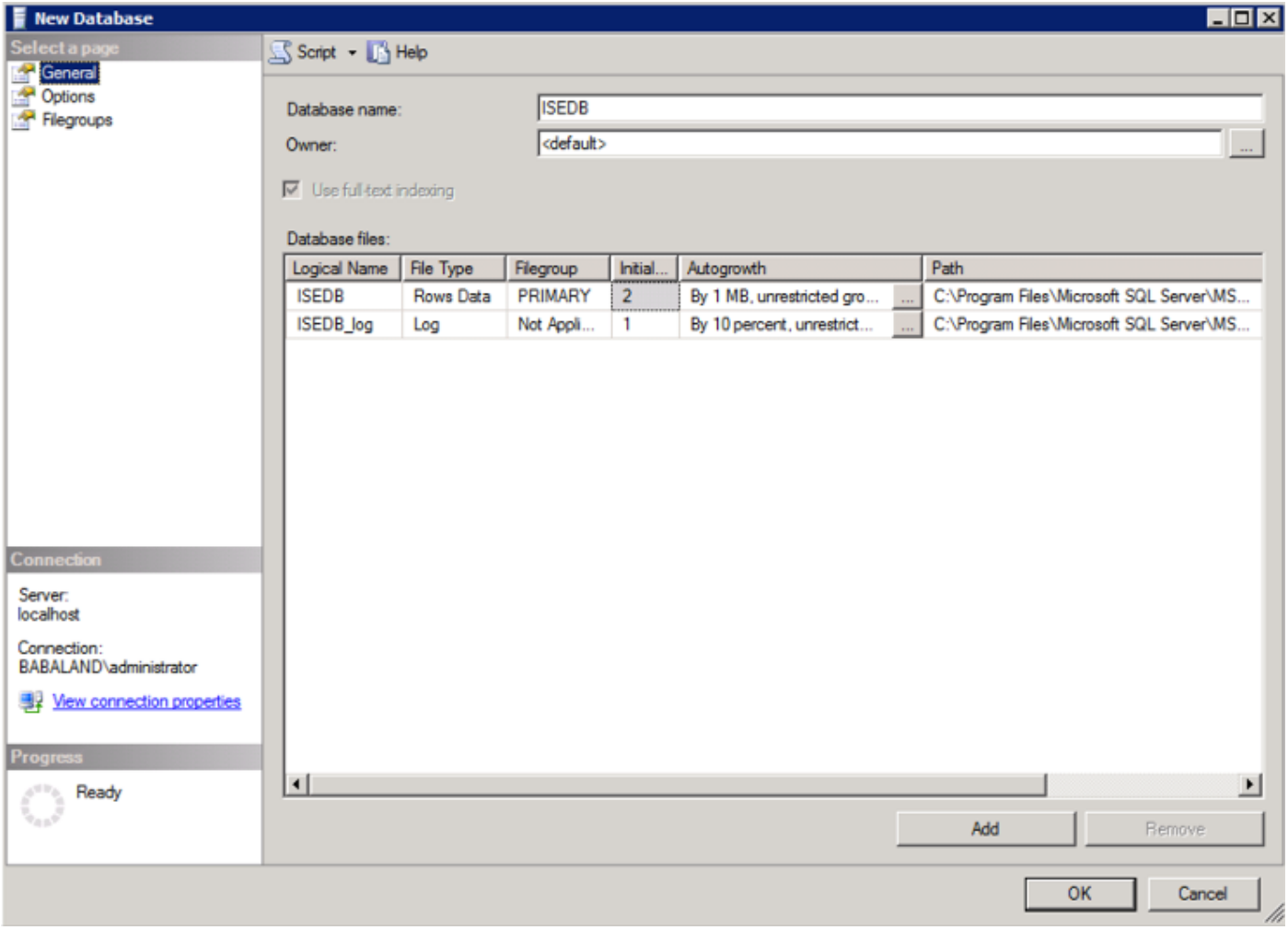
ODBC示例配置

此配置在Microsoft SQL上完成，用于构建解决方案：

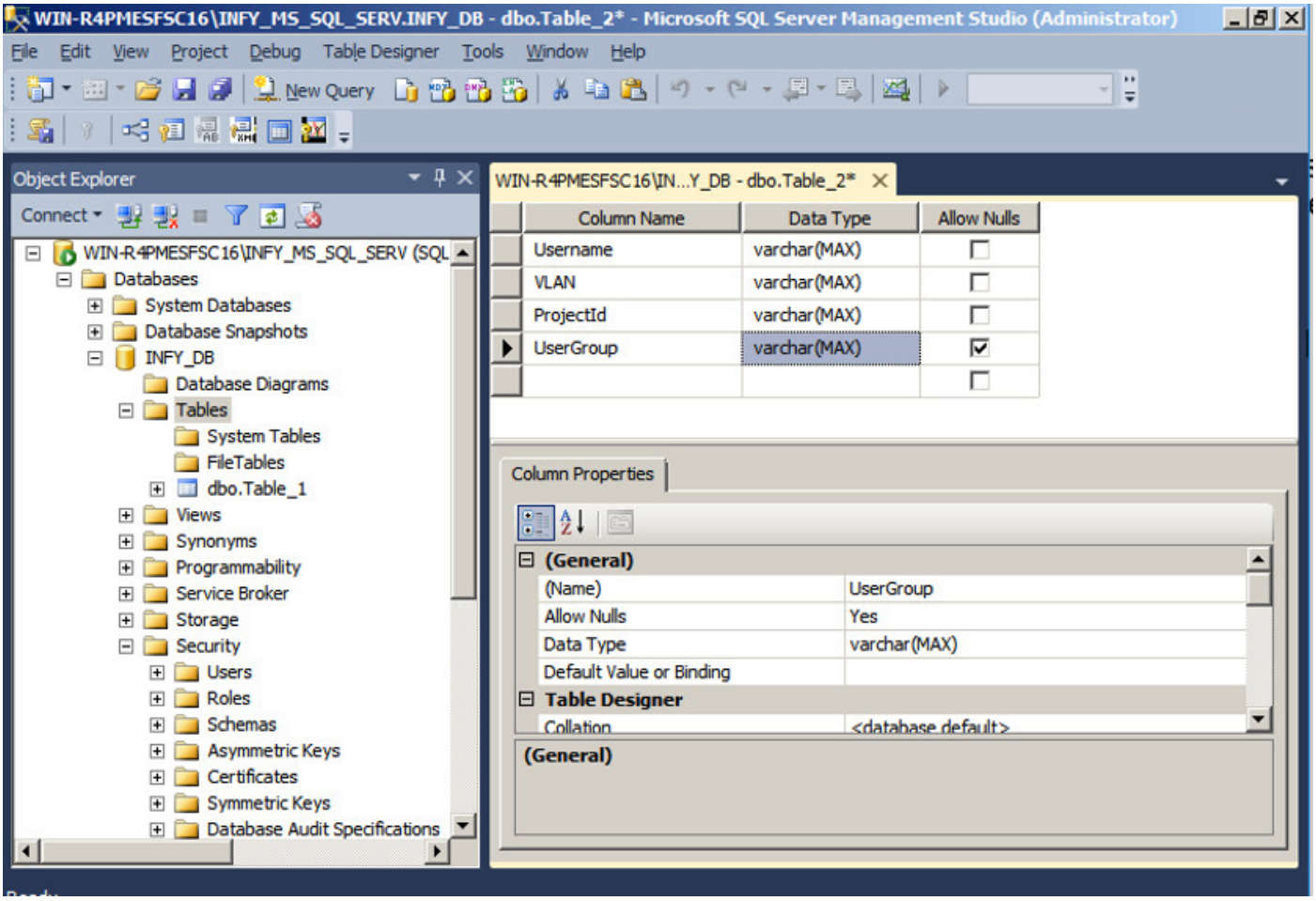
步骤1.打开SQL Server Management Studio(开始**菜单> Microsoft SQL Server**)以创建数据库：



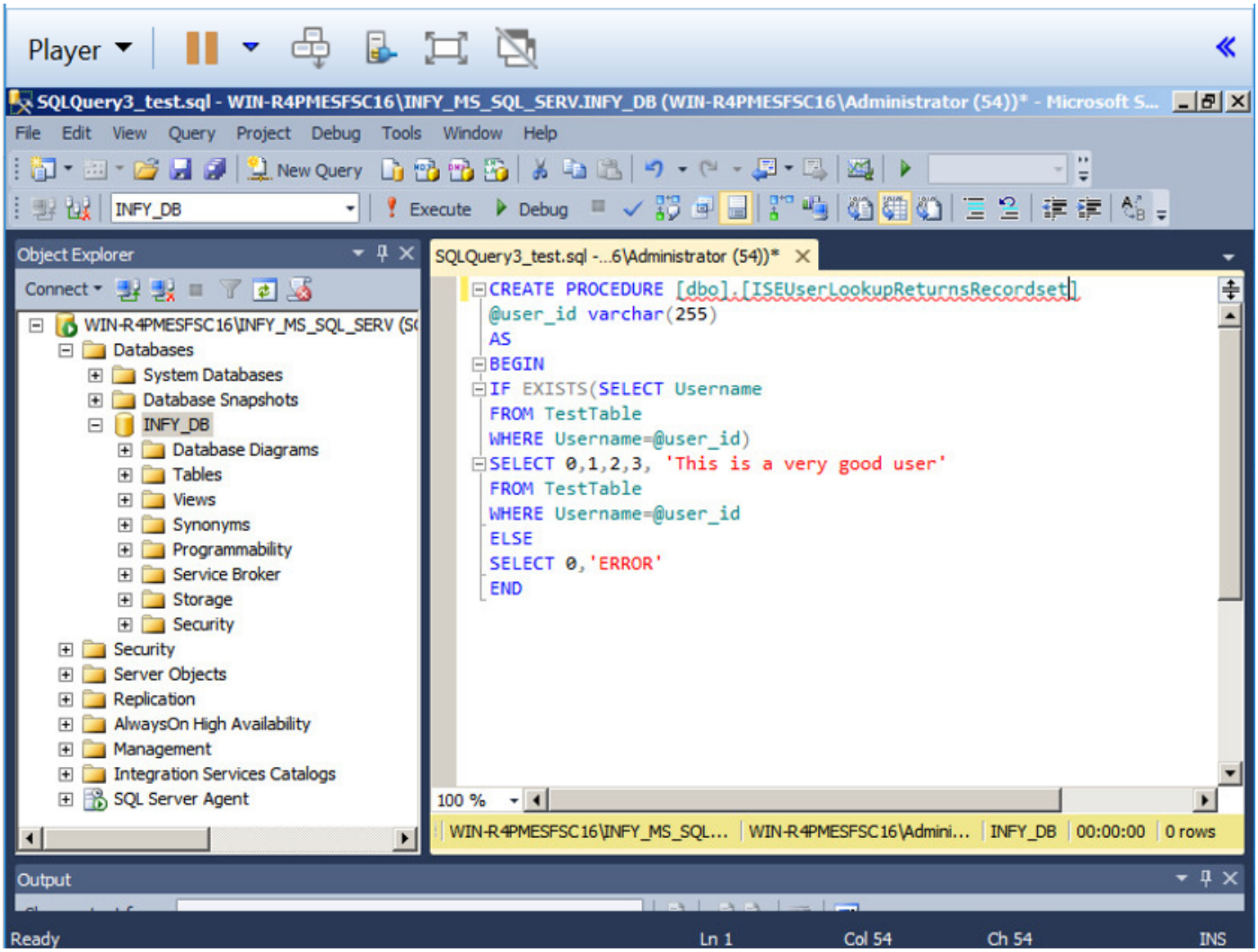
步骤2.提供名称并创建数据库。



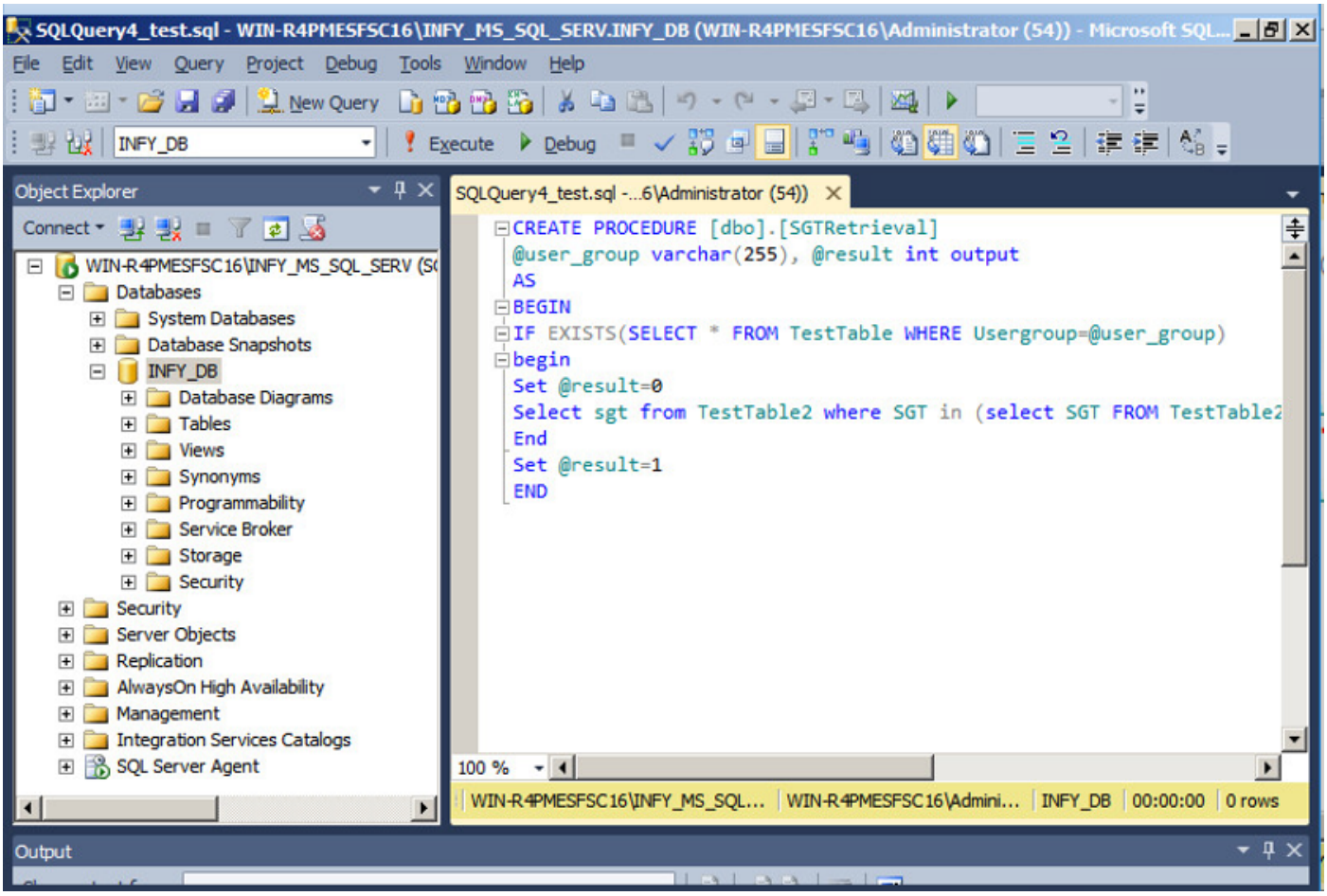
步骤3.创建一个新表，将所需列用作终端获得授权的参数。



步骤4.创建**过程**检查用户名是否存在。



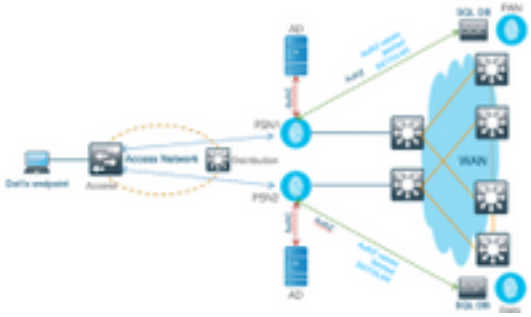
步骤5.创建从表中获取属性(SGT)的过程。

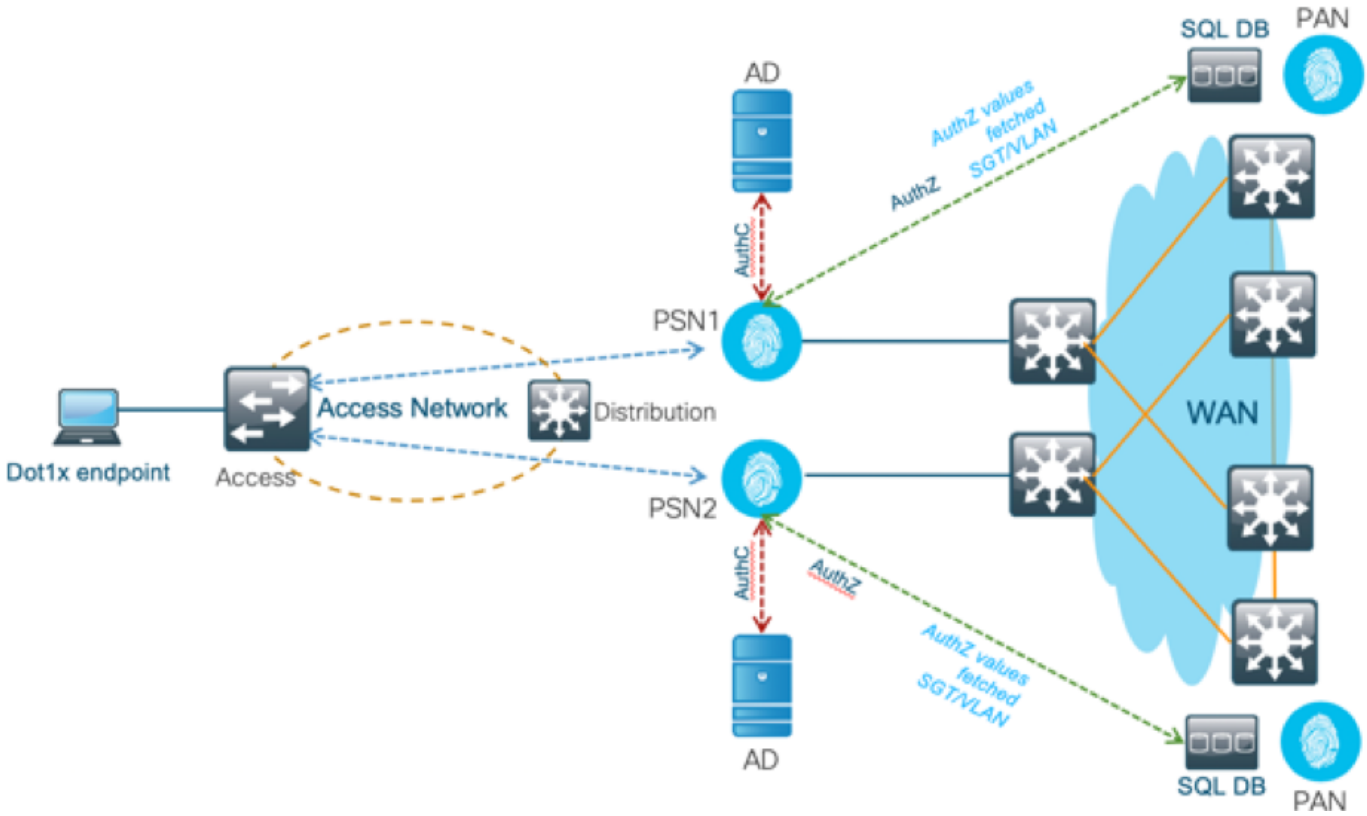


在本文档中，思科ISE与Microsoft SQL解决方案集成，以满足大型企业网络的授权规模要求。

解决方案工作流程（ISE 2.7及更低版本）

在此解决方案中，思科ISE与Active Directory(AD)和Microsoft SQL集成。AD用作身份验证ID存储和MS SQL进行授权。在身份验证过程中，网络接入设备(NAD)将用户凭证转发到PSN - IBN解决方案中的AAA服务器。PSN使用Active Directory ID存储验证终端凭证并对用户进行身份验证。授权策略引用MS SQL数据库以获取授权结果，例如**user-id**用作参考的SGT/VLAN。





优势

此解决方案具有以下优势，使其具有灵活性：

- Cisco ISE可以利用外部数据库提供的所有其他功能。
- 此解决方案不依赖于任何思科ISE扩展限制。

缺点

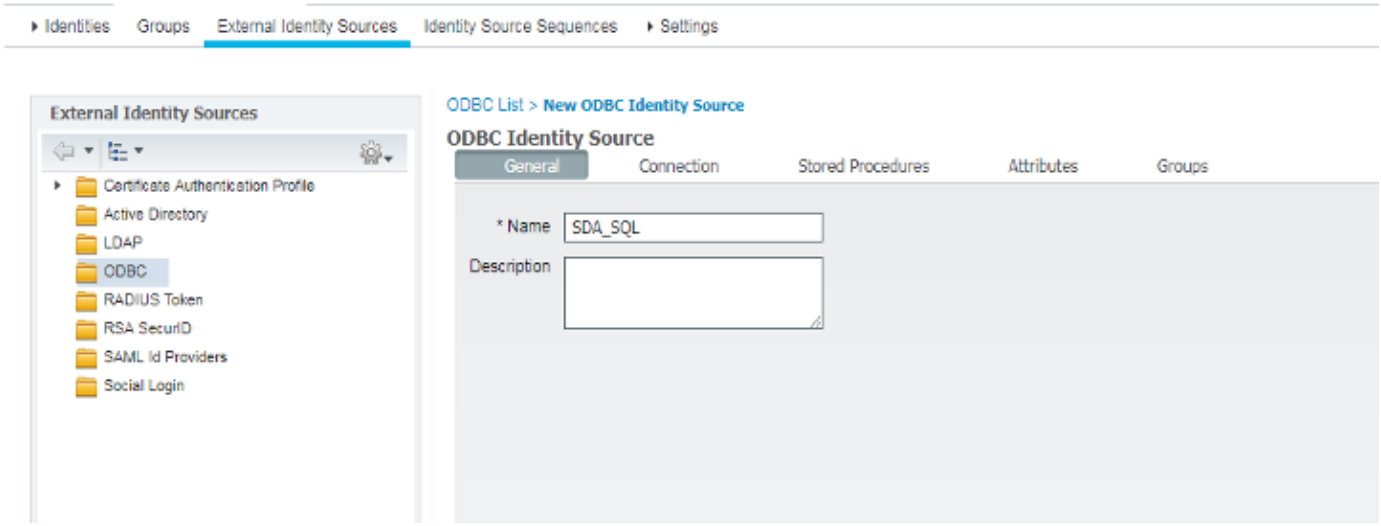
此解决方案有以下缺点：

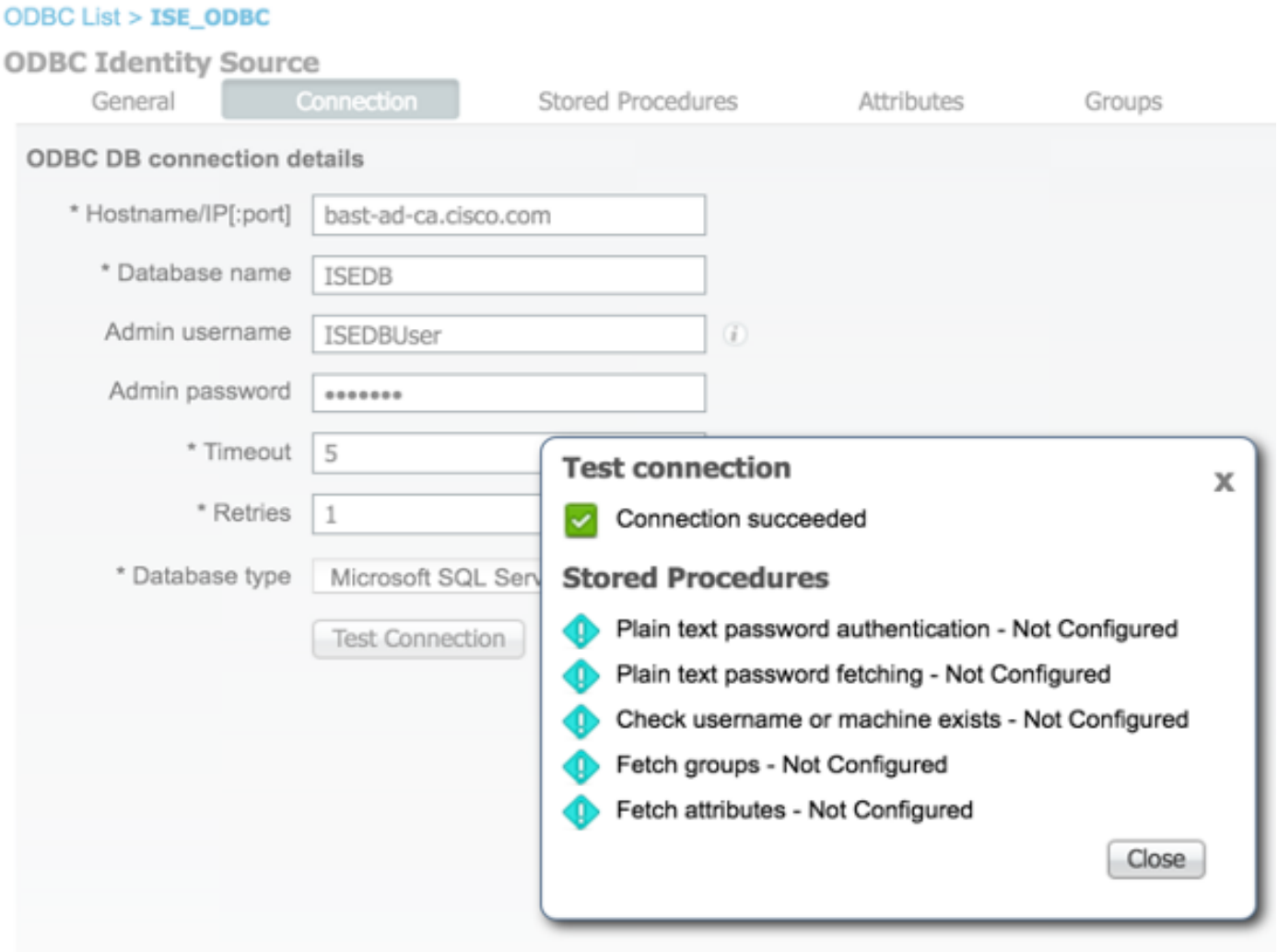
- 需要其他编程以使用终端凭证填充外部数据库。
- 如果外部数据库不像PSN一样存在于本地，则此解决方案取决于WAN，WAN使其成为终端AAA数据流中的第3个故障点。
- 需要更多知识来维护外部数据库进程和过程。
- 必须考虑手动将用户ID配置到数据库引起的错误。

外部数据库示例配置

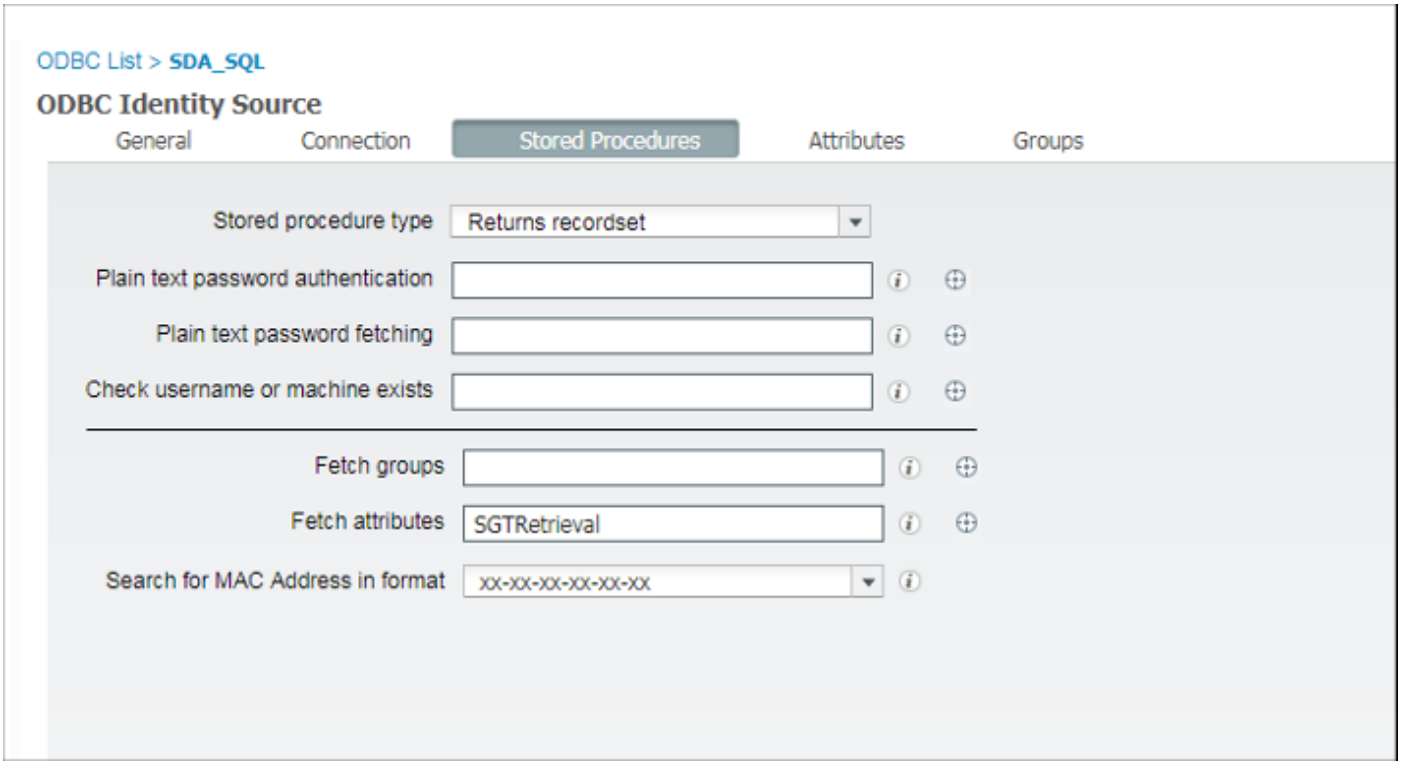
在本文档中，Microsoft SQL显示为用作授权点的外部数据库。

步骤1.在Cisco ISE中创建ODBC身份库从菜单**Administration > External Identity Source > ODBC**并测试连接。

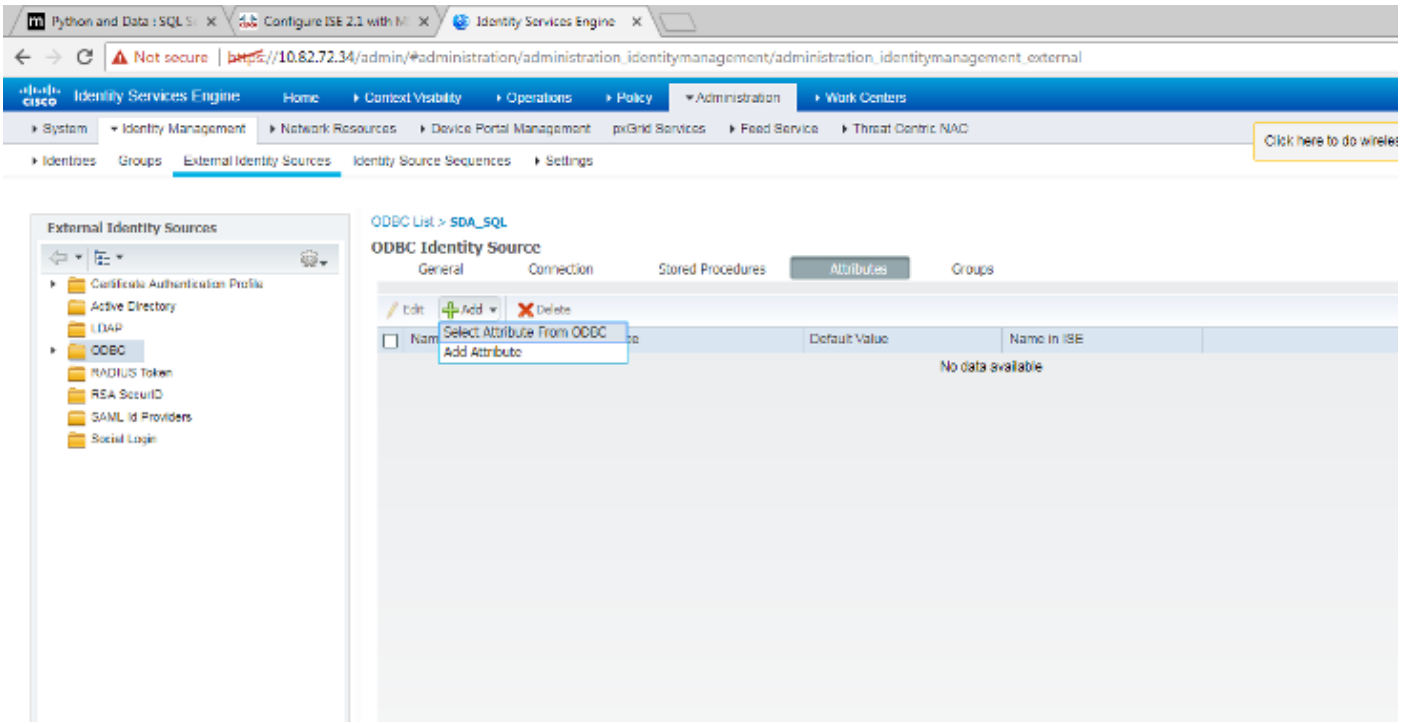


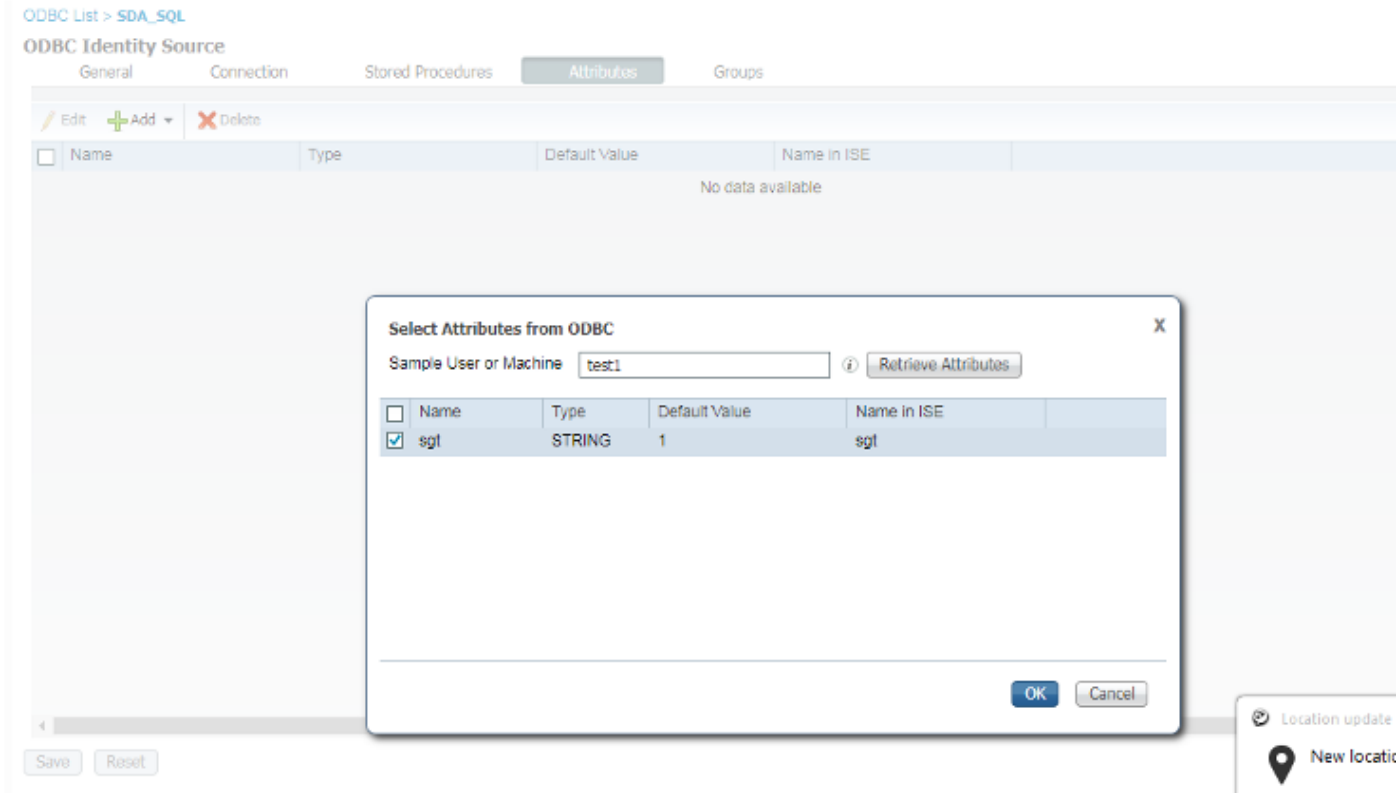


步骤2.导航到ODBC页面上的Stored Procedures选项卡，以在Cisco ISE中配置创建的过程。

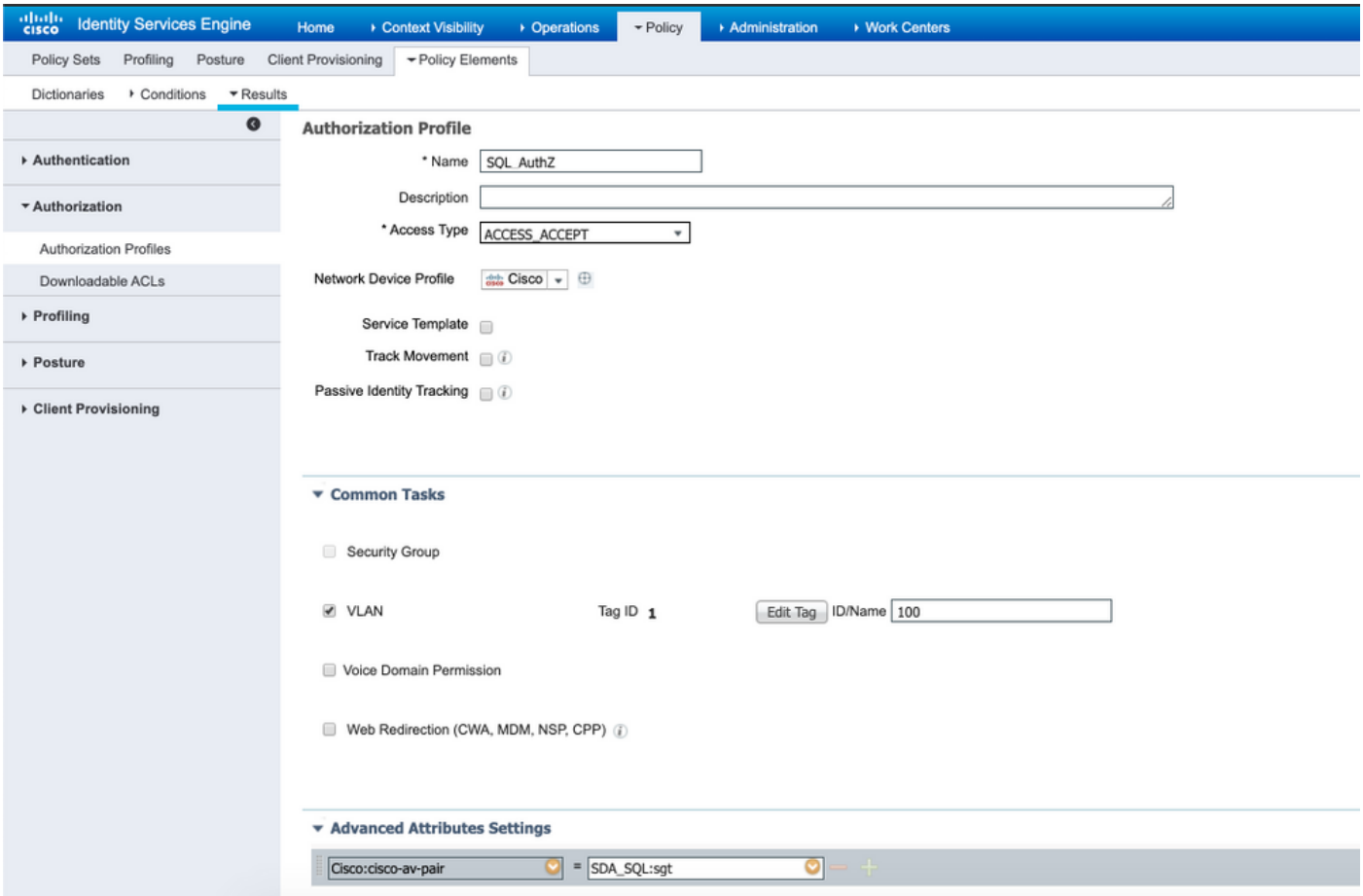


步骤3.从ODBC ID源获取用户ID的属性以进行验证。

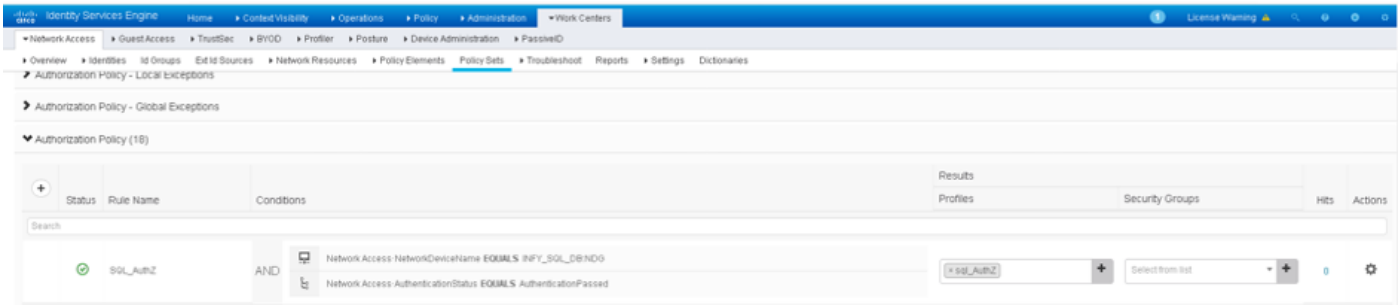




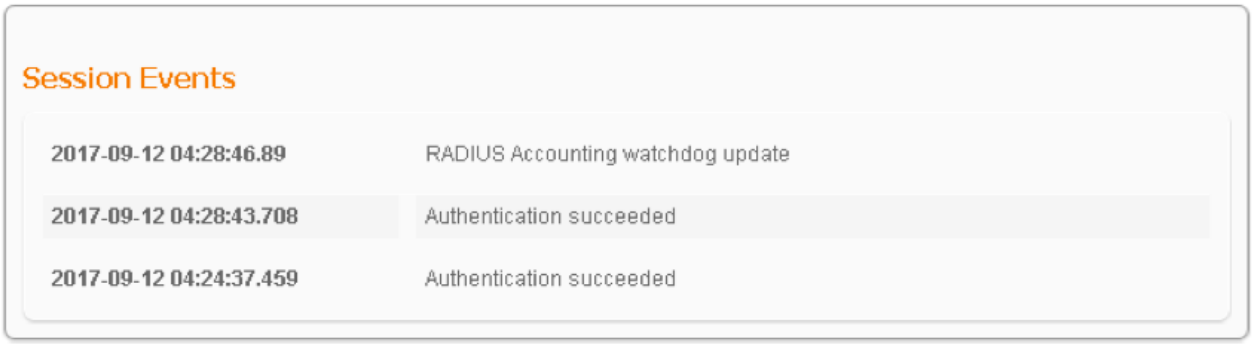
步骤4.创建授权配**置文件**并进行配置。在Cisco ISE中，转至**Policy > Results > Authorization profile > Advance Attributes Settings**，然后选择属性为**Cisco:cisco-av-pair**。选择值作为<name of ODBC database>:sgt，然后将其保存。



步骤5.创建授**权策略**并进行配置。在Cisco ISE中，导航到**Policy > Policy sets > Authorization Policy > Add**。Put the condition as Identity Source is the SQL server。选择结果配置文件作为之前创建的授权配置文件。



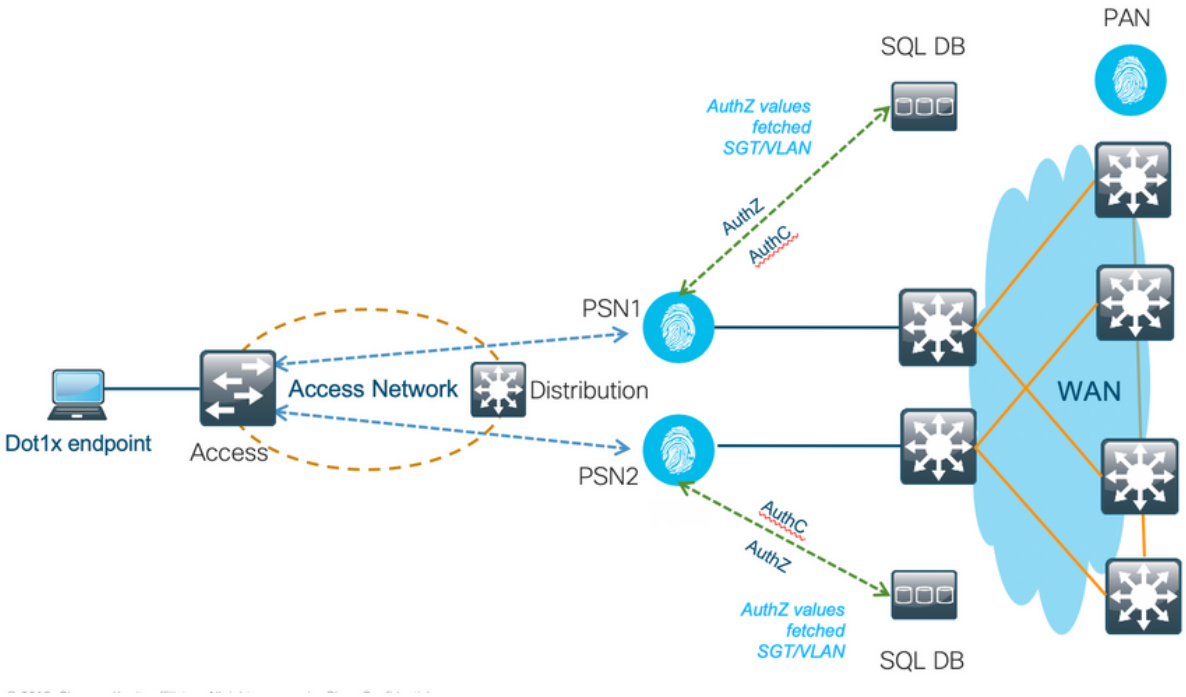
步骤6.用户通过身份验证和授权后，日志应包含分配给用户的sgt以进行验证。



解决方案工作流程（ISE 2.7之后）

在ISE 2.7之后，授权属性可以从ODBC获取，例如Vlan、SGT、ACL，这些属性可以在策略中使用。

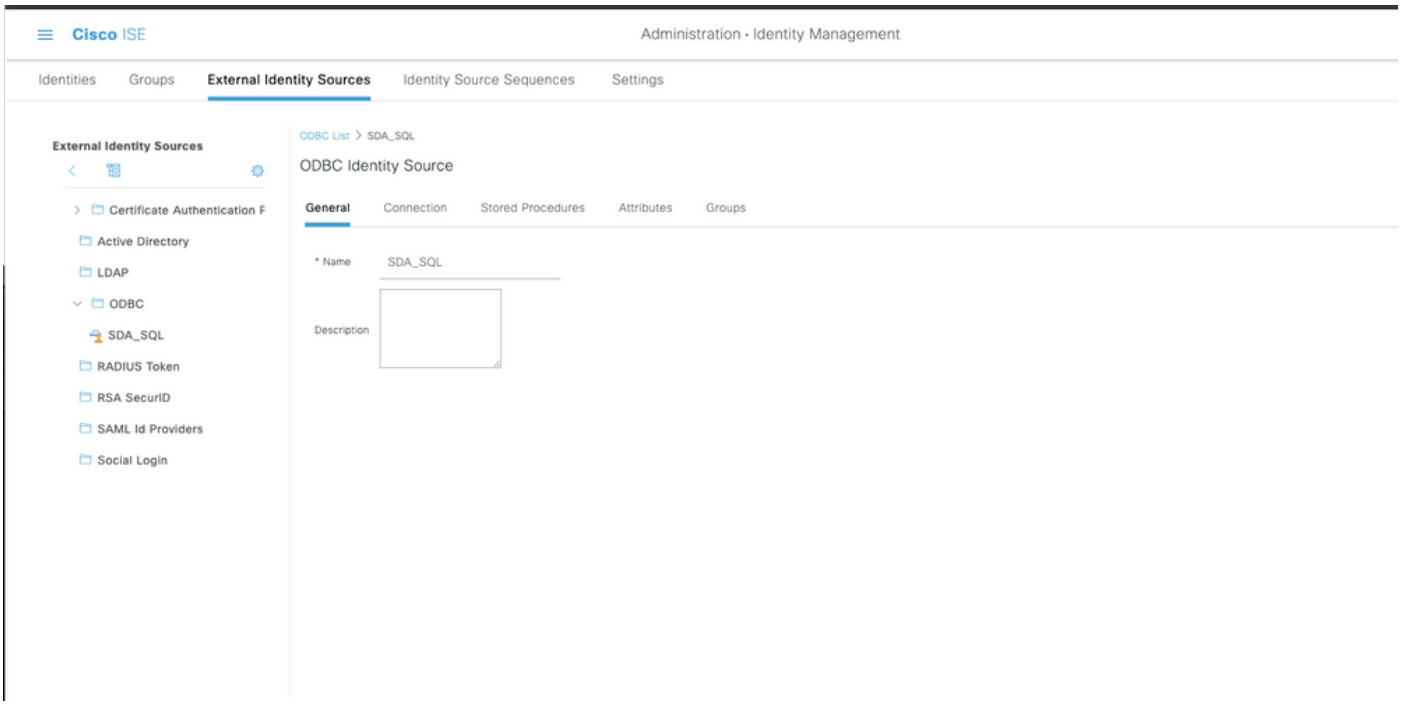
在此解决方案中，Cisco ISE与Microsoft SQL集成。MS SQL用作身份验证和授权的ID存储。当来自终端的凭证提供给PSN时，它会根据MS SQL数据库验证凭证。授权策略引用MS SQL数据库以获取授权结果，例如**user-id**用作参考的SGT/VLAN。



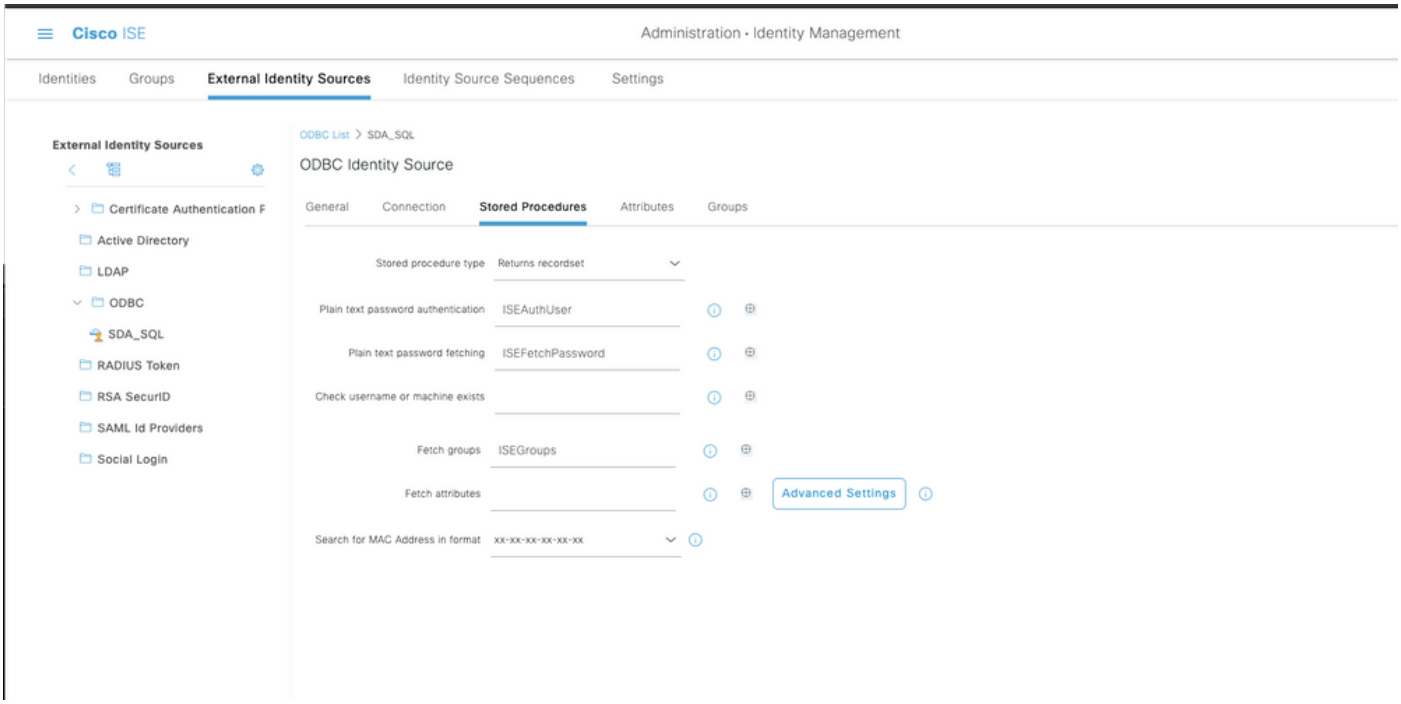
外部数据库示例配置

按照本文档前面介绍的过程创建MS SQL数据库以及用户名、密码、VLAN ID和SGT。

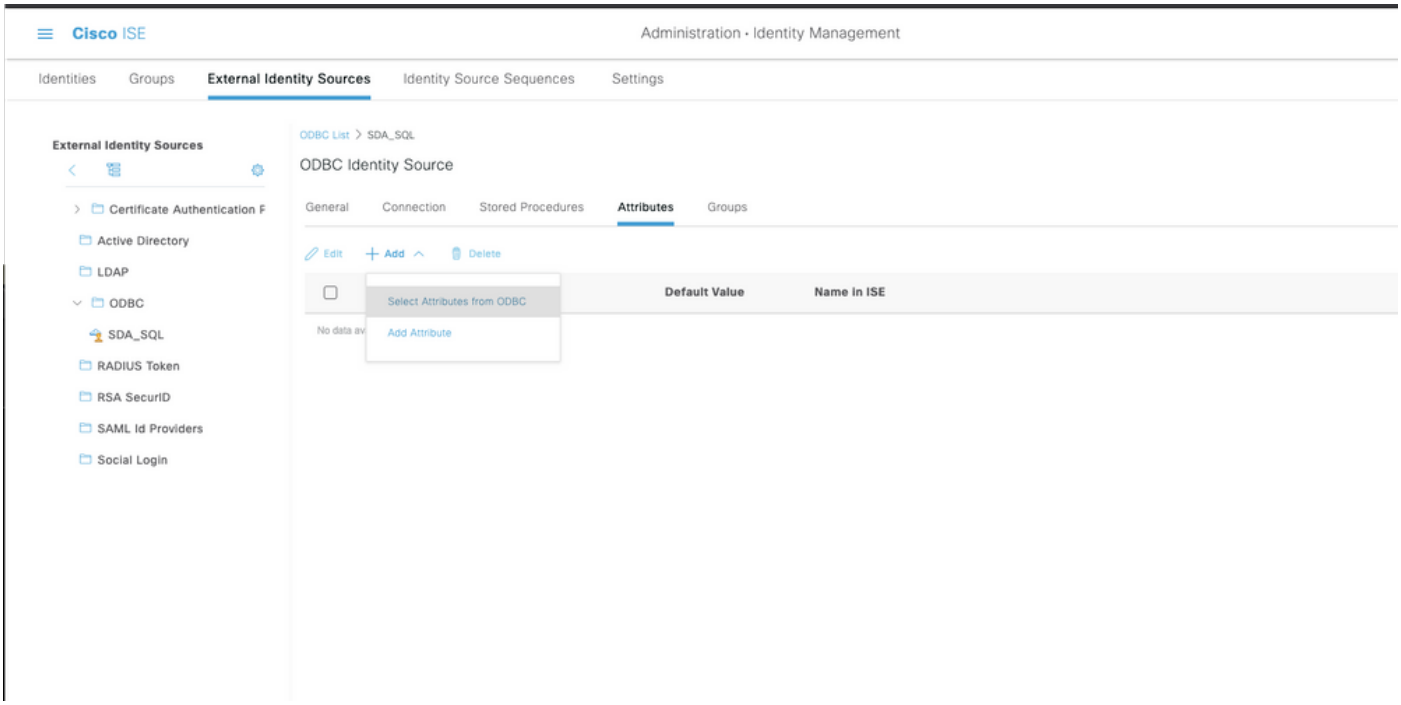
步骤1.在Cisco ISE中从**Administration > External Identity Source > ODBC**菜单创建ODBC身份库并测试连接。

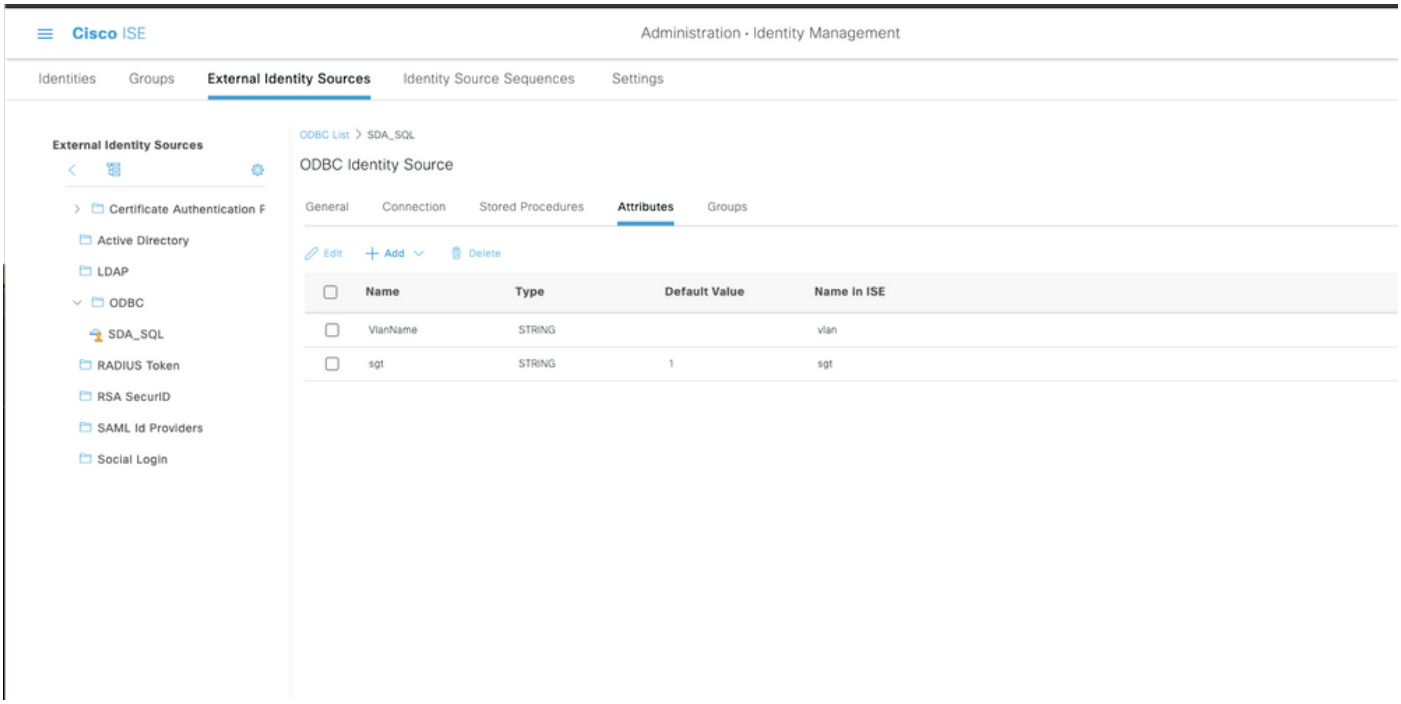


步骤2.导航到ODBC页面上的Stored Procedures选项卡，以在Cisco ISE中配置创建的过程。

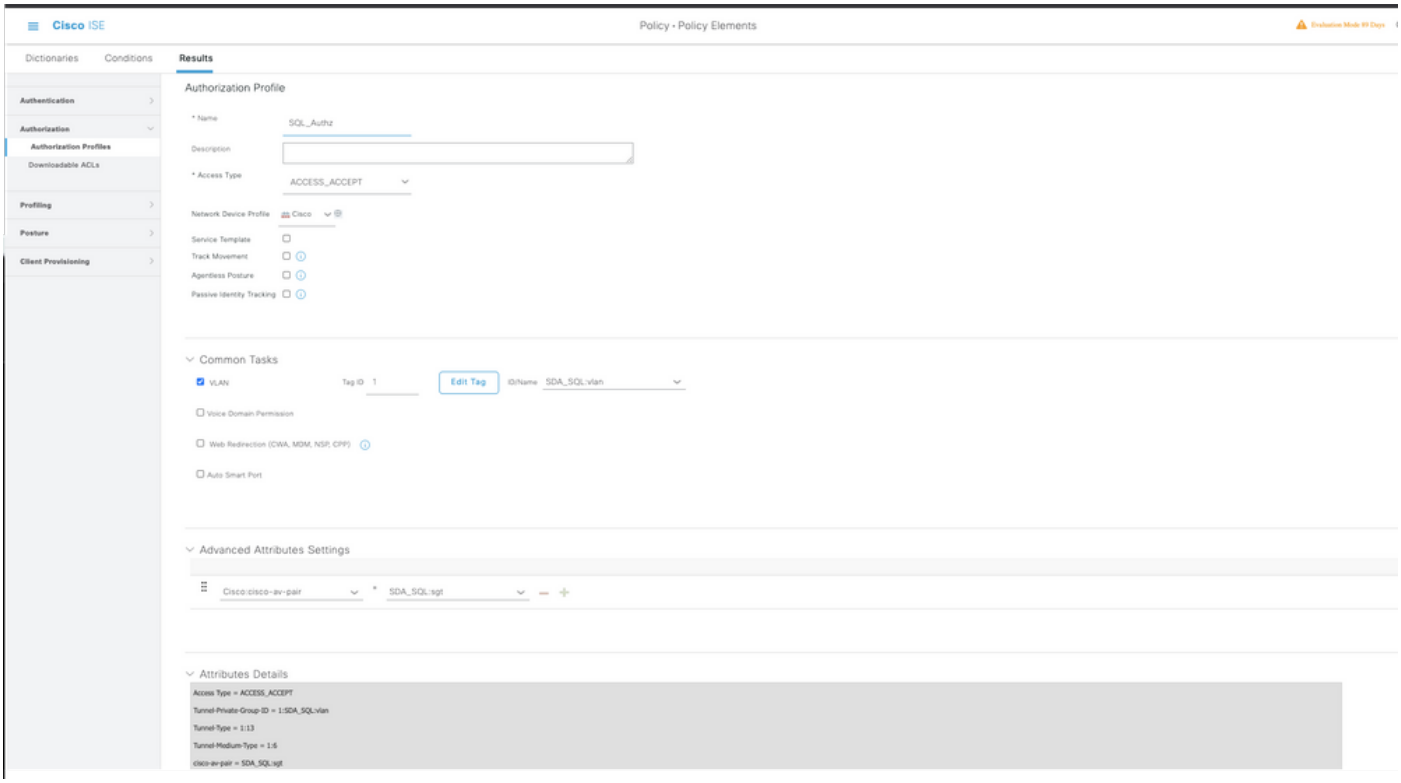


步骤3.从ODBC ID源获取用户ID的属性以进行验证。

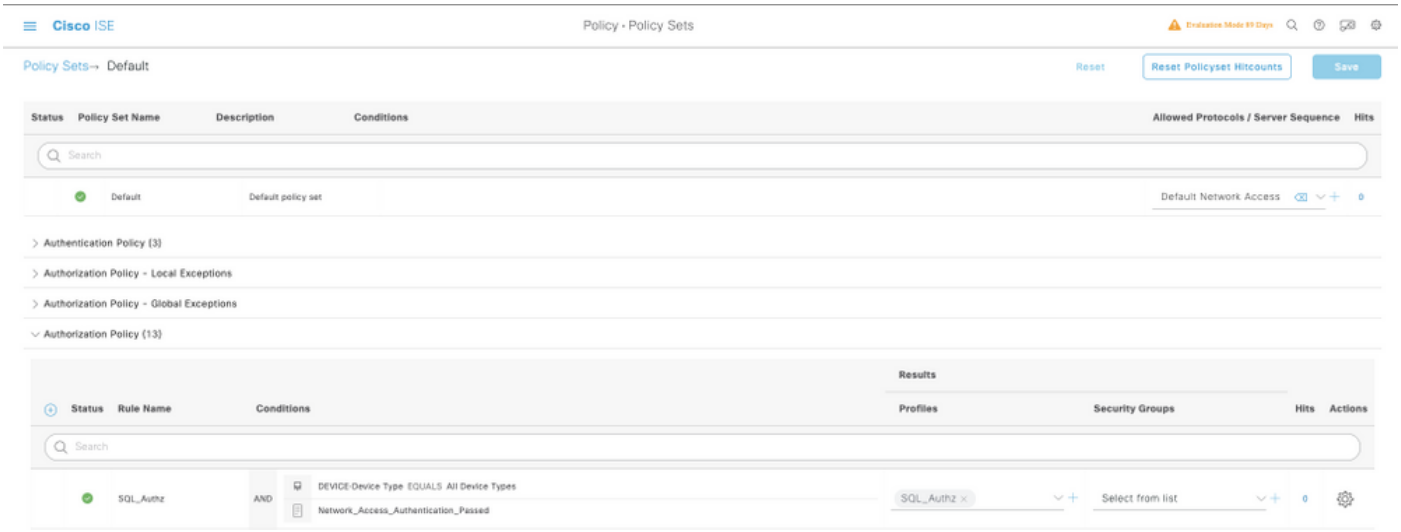




步骤4.创建授权配**置文件**并进行配置。在Cisco ISE中，转至**Policy > Results > Authorization profile > Advance Attributes Settings**，选择属性为**Cisco:cisco-av-pair**。选择值为<name of ODBC database>:sgt。在Common Tasks下，选择**VLAN**,ID/Name为<name of ODBC database>:vlan并保存



步骤5.创建授**权策略**并进行配置。在Cisco ISE中，导航到**Policy > Policy sets > Authorization Policy > Add**。Put the condition as Identity Source is the SQL server。选择结果配置文件作为之前创建的授权配置文件。

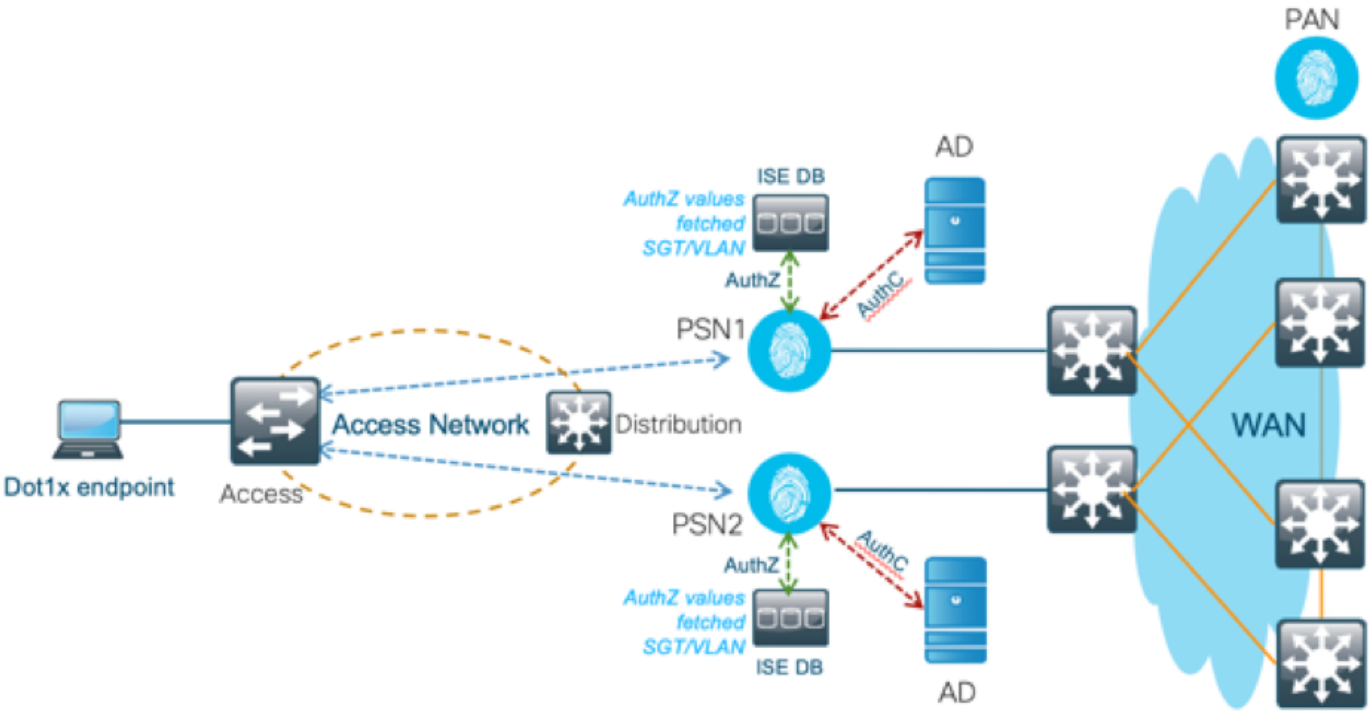


使用内部数据库

思科ISE本身有一个内置数据库，可用于拥有用户ID进行授权。

解决方案工作流程

在此解决方案中，思科ISE的内部数据库用作授权点，而Active Directory(AD)继续作为身份验证源。Cisco ISE DB中包含终端用户ID以及返回授权结果（如SGT或VLAN）的**自定义属性**。将来自终端的凭证提供给PSN时，它会使用Active Directory ID存储检查终端凭证的有效性，并对终端进行身份验证。授权策略引用ISE DB获取授权结果，例如SGT/VLAN，用户ID用作参考。



优势

此解决方案具有以下优势，使其成为灵活的解决方案：

- Cisco ISE DB是内置解决方案，因此与外部DB解决[方案]不同，它没有第三个故障点。

- 由于思科ISE集群确保所有角色之间的实时同步，因此没有WAN依赖性，因为PSN拥有从PAN实时推送的所有用户ID和自定义属性。
- Cisco ISE可以利用外部数据库提供的所有其他功能。
- 此解决方案不依赖于任何思科ISE扩展限制。

缺点

此解决方案有以下缺点：

- 思科ISE数据库可以保留的最大用户ID数为300,000。
- 必须考虑手动将用户ID配置到数据库引起的错误。

内部数据库示例配置

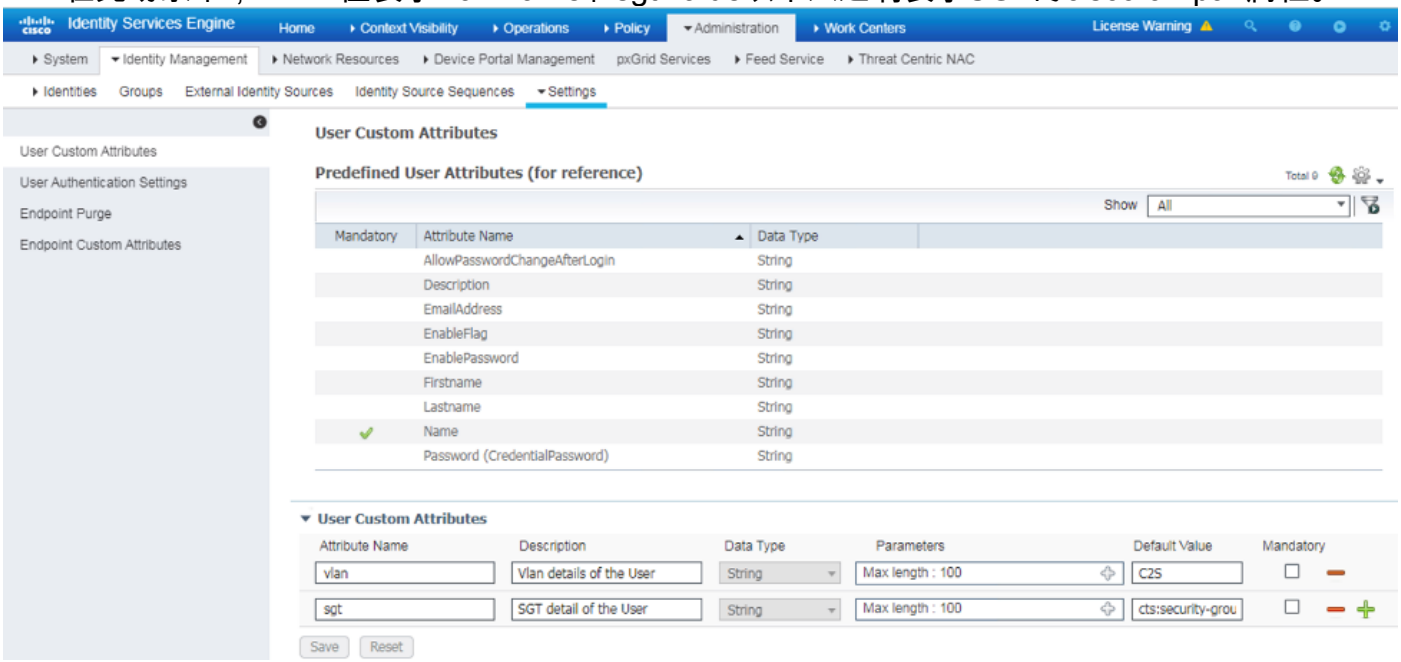
可以使用自定义用户属性为内部ID存储中的任何用户配置每用户VLAN和SGT。

步骤1.创建新用户自定义属性，以表示各自用户的VLAN和SGT值。导航到**管理>身份管理>设置>用户自定义属性。创建新用户自定义属性，如下表所示。**

此处显示了ISE数据库表以及自定义属性。

属性名称	数据类型	参数（长度）	默认值
vlan	字符串	100	C2S（默认Vlan名称）
sgt	字符串	100	cts:security-group-tag=0003-0（默认SGT值）

- 在此场景中，VLAN值表示vlan name和sgt value以十六进制表示SGT的cisco-av-pair属性。

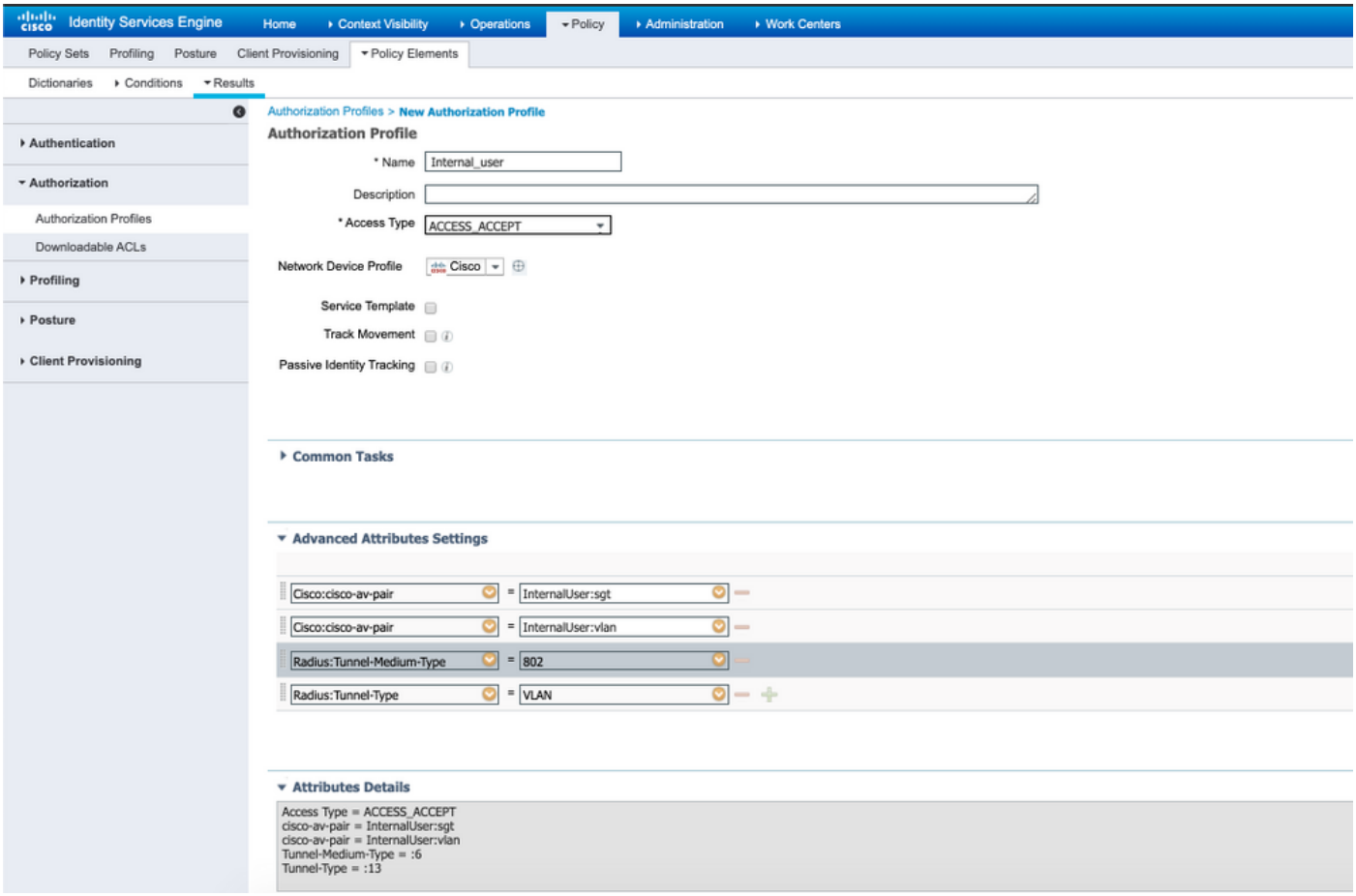


步骤2.使用用户自定义属性创建授权配置文件，以表示各自用户的vlan和sgt值。导航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add。**在Advanced Attributes Settings下添加下述属性。

此表显示内部用户的授权配置文件。

属性	价值
Cisco:cisco-av-pair	内部用户：sgt
Radius:Tunnel-Private-Group-ID	内部用户：vlan
Radius:Tunnel-Medium-Type	802
Radius：隧道类型	VLAN

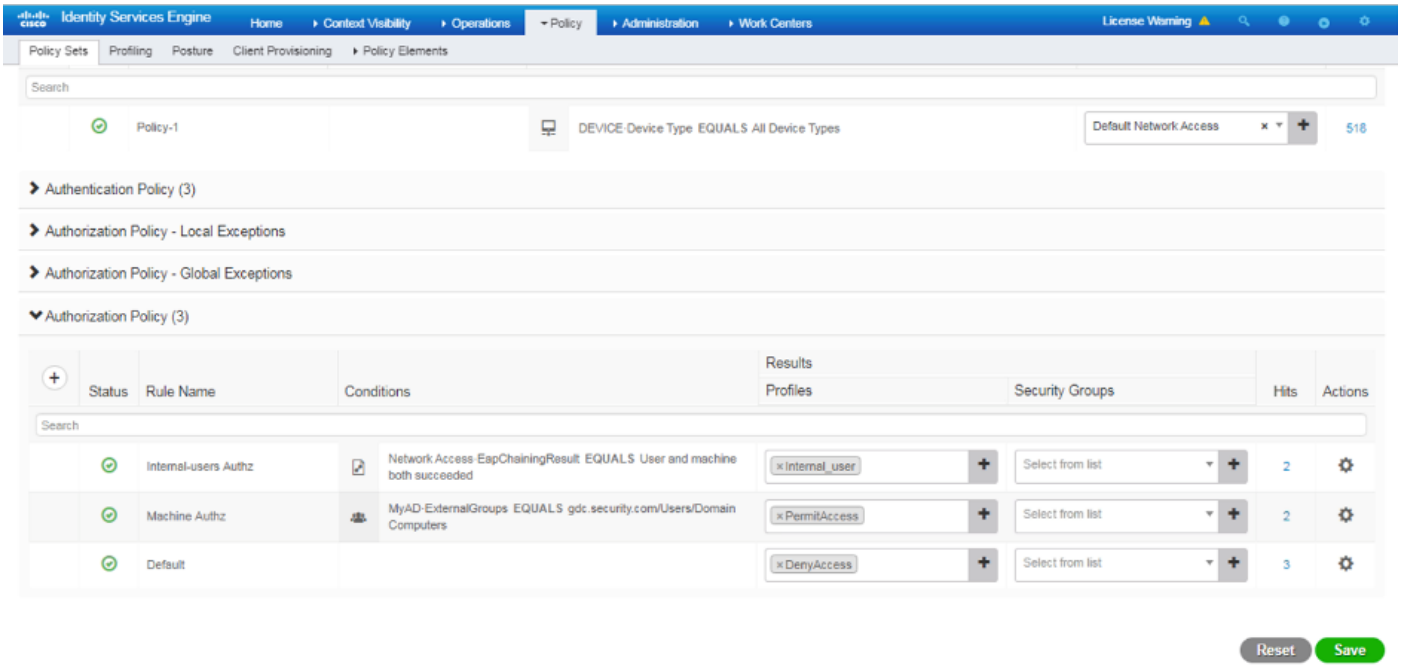
如图所示，对于内部用户，配置文件**Internal_user**配置为SGT和Vlan，分别配置为**InternalUser:sgt**和**InternalUser:vlan**。



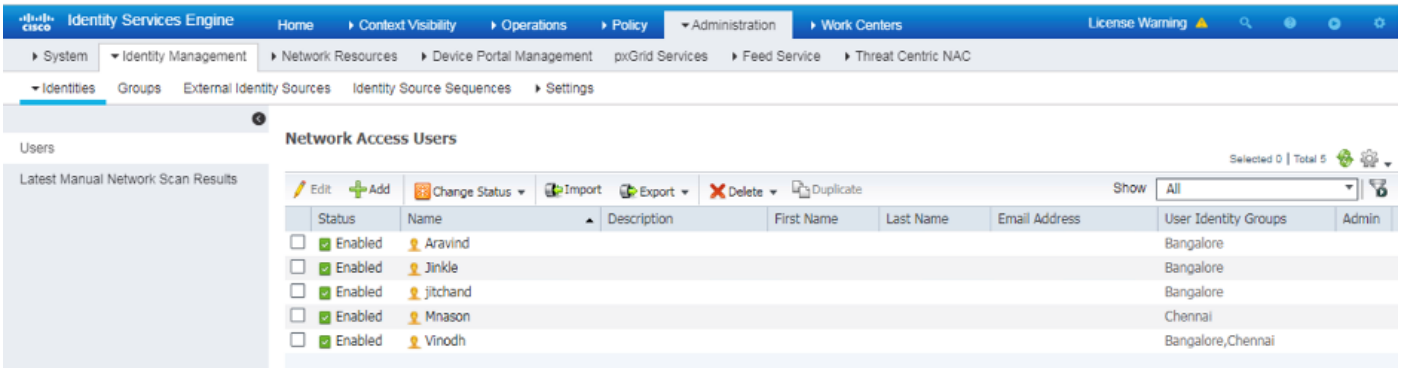
第3步：创建授权策略，导航到**Policy > Policy Sets > Policy-1 > Authorization。使用下述条件创建授权策略并将其映射到相应的授权配置文**件。

此表显示内部用户的授权策略。

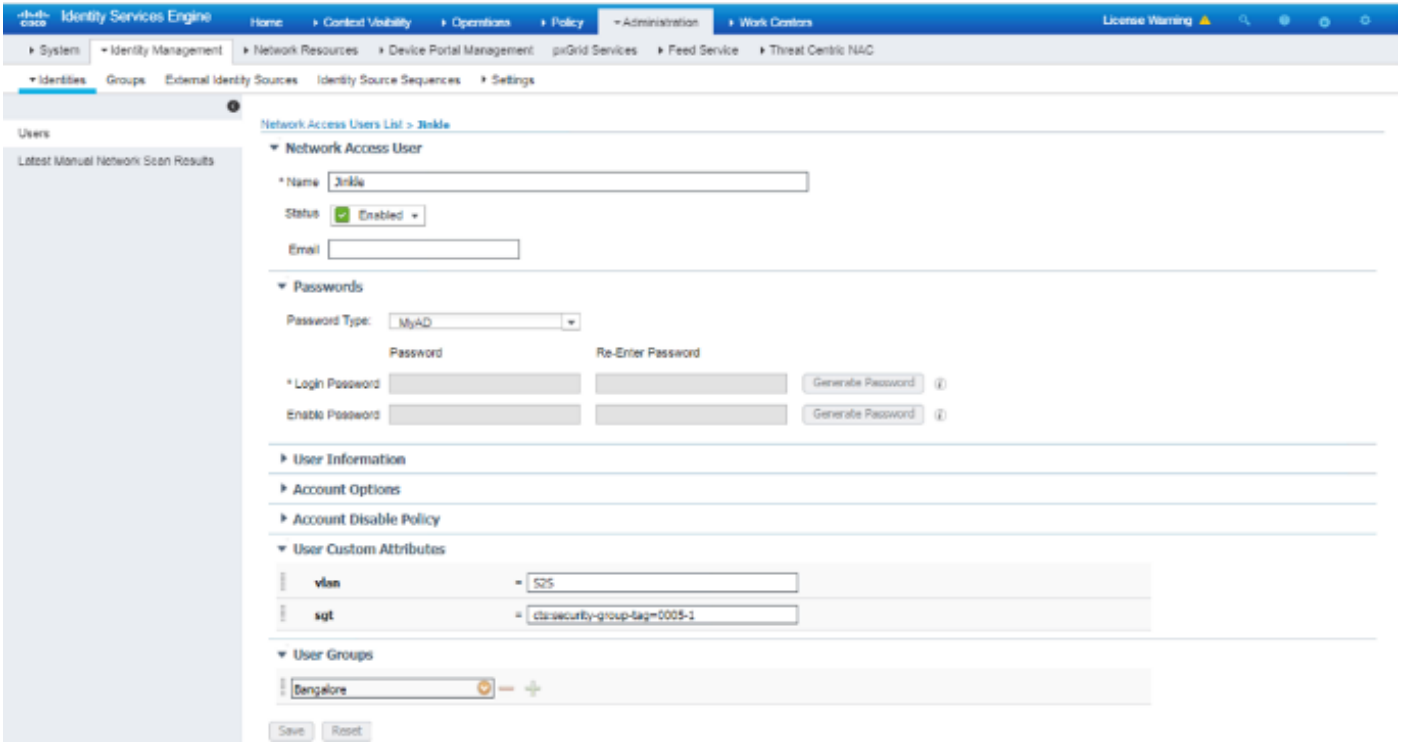
规则名称	条件	结果授权配置文件
Internal_User_Authz	如果网络访问。EapChainingResults EQUALS User and machine both succeeded	Internal_user
Machine_Only_Authz	如果MyAD.ExternalGroups等于gdc.security.com/Users/Domain计算机	允许访问



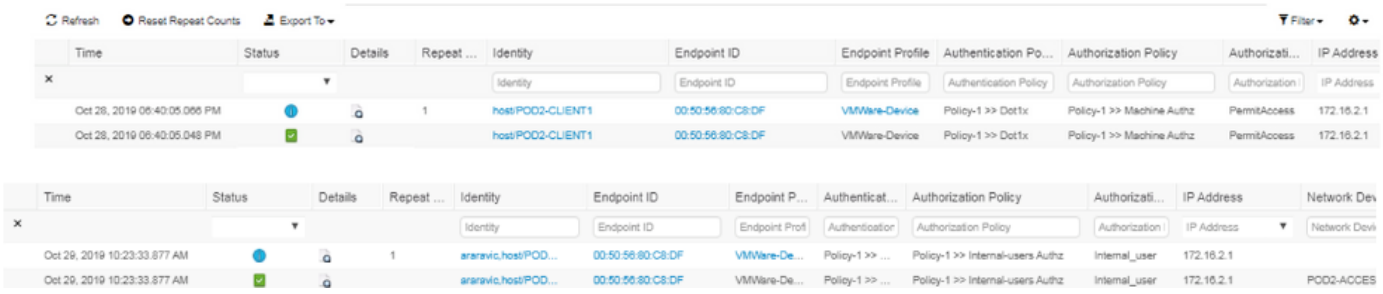
步骤4.在csv模板中使用自定义属性创建批量用户身份，其中包含用户详细信息及其各自的自定义属性。 通过导航到**Administration > Identity Management > Identities > Users > Import > Choose the file > Import**导入csv。



此图片显示了具有自定义属性详细信息的示例用户。选择用户并点击edit以查看映射到相应用户的自定义属性详细信息。



步骤 5：验证实时日志：



检查**结果**部分以验证**Vlan & SGT**属性是否作为Access-Accept的一部分发送。

结论

此解决方案允许一些大型企业客户根据他们的要求进行扩展。添加/删除用户ID时需要谨慎。如果触发错误，可能导致正版用户未经授权的访问，反之亦然。

相关信息

通过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

术语表

AAA	身份验证授权记帐
广告	Active Directory
身份验证	身份验证
身份验证	授权
DB	数据库
DOT1X	802.1X
IBN	基于身份的网络
ID	身份数据库
ISE	身份服务引擎
MnT	监控和故障排除
MsSQL	Microsoft SQL
ODBC	开放式数据库连接

PAN	策略管理节点
PSN	策略服务节点
SGT	安全组标记
SQL	结构化查询语言
VLAN	虚拟 LAN
WAN	广域网

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。