Criteri di accesso semplificati con ODBC e ISE DB (attributo personalizzato) per reti campus su larga scala

Sommario

Introduzione

In questo documento viene descritta l'installazione di un campus su larga scala senza compromettere le funzionalità e l'applicazione della sicurezza. ISE (Identity Services Engine), la soluzione di sicurezza degli endpoint di Cisco, soddisfa questo requisito con l'integrazione in una fonte di identità esterna.

Per le reti su larga scala con oltre 50 postazioni geografiche, più di 4000 profili utente diversi e 600.000 endpoint o più, le soluzioni IBN tradizionali devono essere considerate da una prospettiva diversa - più che semplici funzioni, che si adattino a tutte le funzioni. La soluzione IBN (Intent-Based Network), presente nelle tradizionali reti su larga scala, richiede una maggiore attenzione alla scalabilità e alla facilità di gestione, e non solo alle sue caratteristiche.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione Dot1x/MAB
- Cisco Identity Service Engine (Cisco ISE)
- CTS (Cisco TrustSec)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

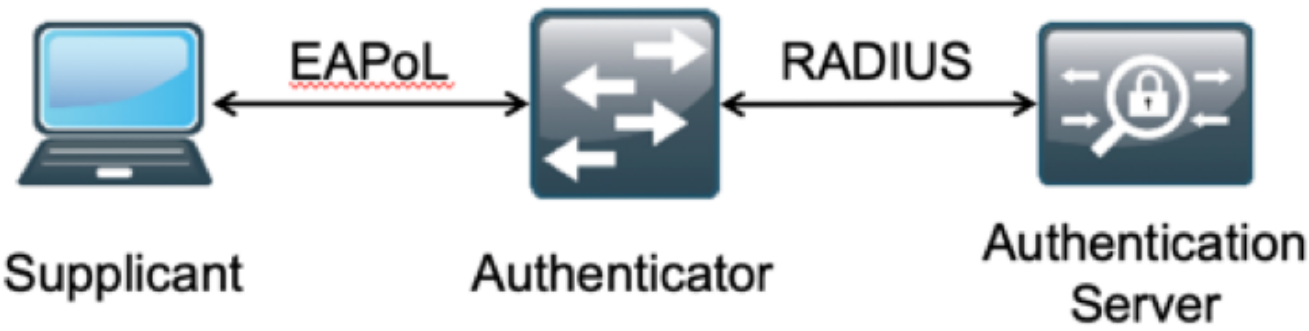
- Cisco Identity Services Engine (ISE) versione 2.6, patch 2 e versione 3.0
- Windows Active Directory (AD) Server 2008 release 2
- Microsoft SQL Server 2012

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dalla configurazione.

Premesse

In una soluzione IBN (Identity Based Network), gli elementi di base sono Supplicant, Authenticator and Authentication (AAA) Server. Il richiedente è un agente sull'endpoint che fornisce le credenziali quando viene richiesto l'accesso alla rete. L'autenticatore o NAS (Network Access Server) è il livello di accesso, che comprende switch di rete e WLC che trasferiscono le credenziali al server AAA. Il server di autenticazione convalida la richiesta di autenticazione dell'utente a fronte di un archivio ID e autorizza l'utente con un'autorizzazione di accesso o di rifiuto. L'archivio ID può trovarsi all'interno del server AAA o su un server esterno dedicato.

Nell'immagine sono illustrati gli elementi IBN di base.



RADIUS è un protocollo basato su UDP (User Datagram Protocol) con autenticazione e autorizzazione abbinate. Nella soluzione IBN di Cisco per i campus aziendali, la persona che gestisce il PSN (Policy Service Node) di ISE funge da server AAA per autenticare gli endpoint

nell'archivio di ID aziendali e concedere l'autorizzazione in base a una condizione.

In Cisco ISE, le policy di autenticazione e autorizzazione sono configurate per soddisfare questi requisiti. I criteri di autenticazione sono costituiti dal tipo di supporto, cablato o wireless, e dai protocolli EAP per la convalida utente. I criteri di autorizzazione sono costituiti da condizioni che definiscono i criteri per la corrispondenza dei vari endpoint e i risultati dell'accesso alla rete, che possono essere una VLAN, un ACL scaricabile o un SGT (Secure Group Tag). Questi sono i valori di scala massimi per le policy su cui è possibile configurare ISE.

La tabella mostra la scala delle policy Cisco ISE.

Attributo	Numero scala
Numero massimo di regole di autenticazione	1000 (modalità Policy Set)
Numero massimo di regole di autorizzazione	3.000 (modalità Policy Set) con profili 3200 Authz

Tendenze tecnologiche

La segmentazione è diventata uno degli elementi chiave della sicurezza delle reti aziendali di oggi, senza alcuna necessità di creare una vera e propria rete perimetrale. Gli endpoint possono spostarsi tra le reti interne ed esterne. La segmentazione aiuta a contenere qualsiasi attacco alla sicurezza su un particolare segmento per estendersi attraverso la rete. L'odierna soluzione Software-Defined Access (SDA), realizzata con l'aiuto del TrustSec di Cisco ISE, consente di segmentare la rete in base al modello commerciale del cliente, per evitare dipendenze da elementi di rete quali VLAN o subnet IP.

Problema

Configurazione delle policy ISE per reti aziendali su larga scala con più di 500 profili di endpoint diversi, il numero di policy di autorizzazione può aumentare fino a diventare ingestibile. Anche se Cisco ISE supporta condizioni di autorizzazione dedicate per gestire un tale volume di profili utente, c'è una sfida a gestire questo numero di policy da parte degli amministratori.

Inoltre, i clienti possono richiedere policy di autorizzazione comuni anziché regole dedicate per evitare i costi generali di gestione e disporre inoltre di un accesso di rete differenziato per gli endpoint in base ai relativi criteri.

Si consideri, ad esempio, una rete aziendale con Active Directory (AD) come **origine della verità** e il differenziatore univoco dell'endpoint è uno degli attributi di AD. In questo caso, la modalità tradizionale di configurazione dei criteri prevede più criteri di autorizzazione per ogni profilo di endpoint univoco.

In questo metodo, ogni profilo di endpoint è distinto da un attributo AD in domain.com. È quindi necessario configurare un criterio di autorizzazione dedicato.

Nella tabella vengono descritti i criteri AuthZ tradizionali.

Politica ABC	Se AnyConnect è uguale a User-AND-Machine-Both-Passed E

	Se AD-Group è uguale a domain.com/groups/ABC POI SGT:C2S-ABC E VLAN:1021
DEF-Policy	Se AnyConnect è uguale a User-AND-Machine-Both-Passed E Se AD-Group è uguale a domain.com/groups/DEF POI SGT:C2S-DEF E VLAN:1022
Criteri GHI	Se AnyConnect è uguale a User-AND-Machine-Both-Passed E Se AD-Group è uguale a domain.com/groups/GHI POI SGT:C2S-GHI E VLAN:1023
Criterio XYZ	Se AnyConnect è uguale a User-AND-Machine-Both-Passed E Se AD-Group è uguale a domain.com/groups/XYZ POI SGT:C2S-XYZ E VLAN:1024

Soluzione proposta

Per aggirare la violazione del numero massimo scalabile di policy di autorizzazione supportate su Cisco ISE, la soluzione proposta è usare un database esterno che autorizzi ciascun endpoint con i risultati dell'autorizzazione ricavati dai relativi attributi. Ad esempio, se AD viene utilizzato come database esterno per l'autorizzazione, è possibile fare riferimento a tutti gli attributi utente non utilizzati (come il codice reparto o PIN) per ottenere risultati autorizzati mappati con SGT o VLAN.

Ciò si ottiene con l'integrazione di Cisco ISE con un database esterno o all'interno del database interno di ISE configurato con attributi personalizzati. In questa sezione viene illustrata la distribuzione dei due scenari seguenti:

> **Nota:** In entrambe le opzioni, il database contiene l'**ID utente** ma non la **password** degli endpoint DOT1X. Il database viene utilizzato solo come punto di **autorizzazione**. L'autenticazione può continuare a essere l'archivio ID del cliente che nella maggior parte dei casi risiede nel server Active Directory (AD).

Configurazione con database esterno

Cisco ISE è integrato con un database esterno per la convalida delle credenziali dell'endpoint:

Questa tabella mostra le origini di identità esterne convalidate.

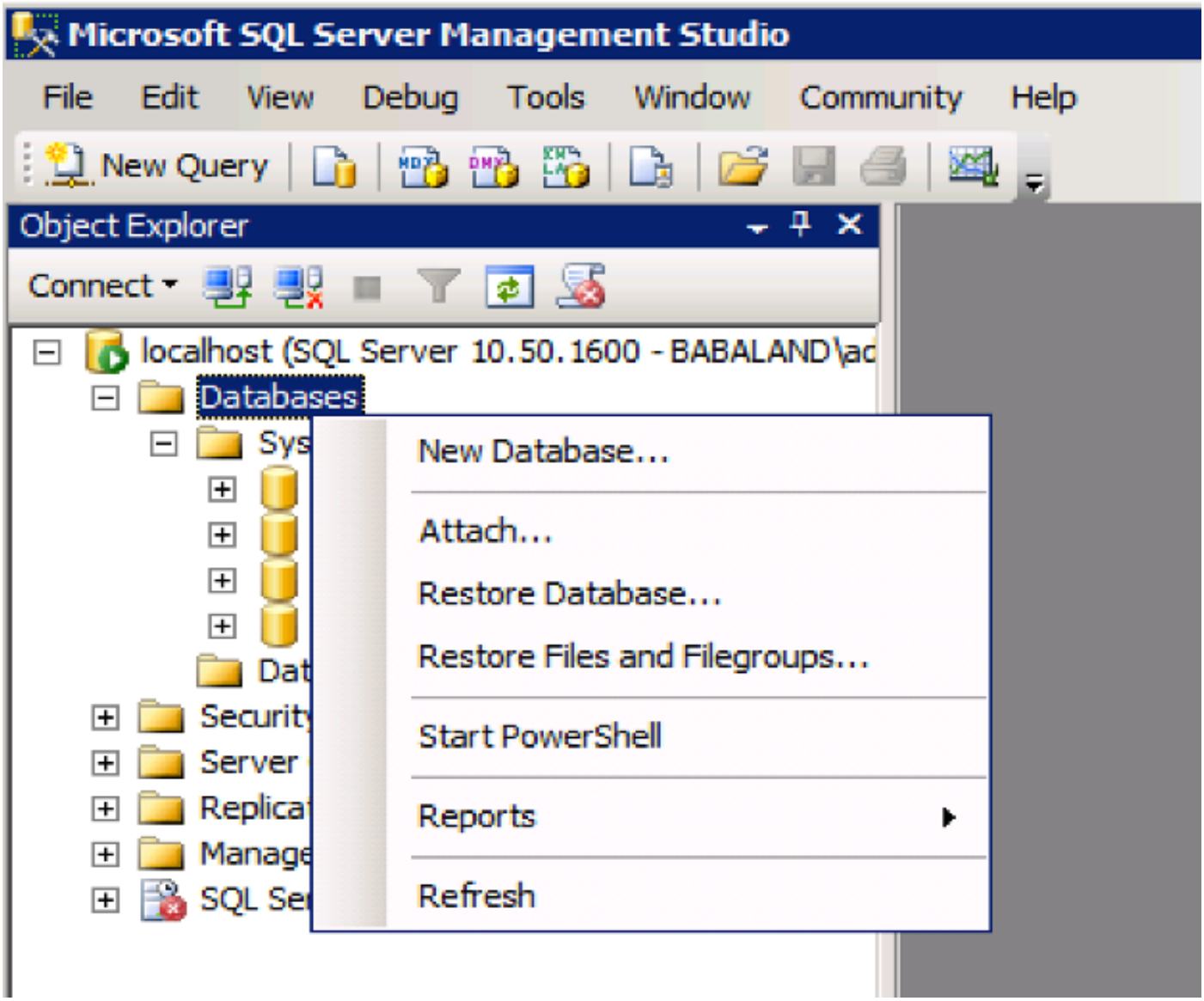
Origine identità esterna	SO/Versione
Active Directory	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—

Server LDAP	
Server di elenchi in linea LDAP SunONE	Versione 5.2
Server di elenchi in linea OpenLDAP	Versione 2.4.23
Qualsiasi server compatibile LDAP v3	—
Server Token	
RSA ACE/Server	serie 6.x
RSA Authentication Manager	serie 7.x e 8.x
Qualsiasi server token RADIUS conforme a RFC 2865	—
Single Sign-On (SSO) SAML (Security Assertion Markup Language)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Versione 11.1.2.2.0
Oracle Identity Federation (OIF)	Versione 11.1.1.2.0
PingFederate Server	Versione 6.10.0.4
PingOne Cloud	—
Secure Auth	8.1.1
Qualsiasi provider di identità conforme a SAMLv2	—
Origine identità ODBC (Open Database Connectivity)	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition release 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Social login (per account utente guest)	
Facebook	—

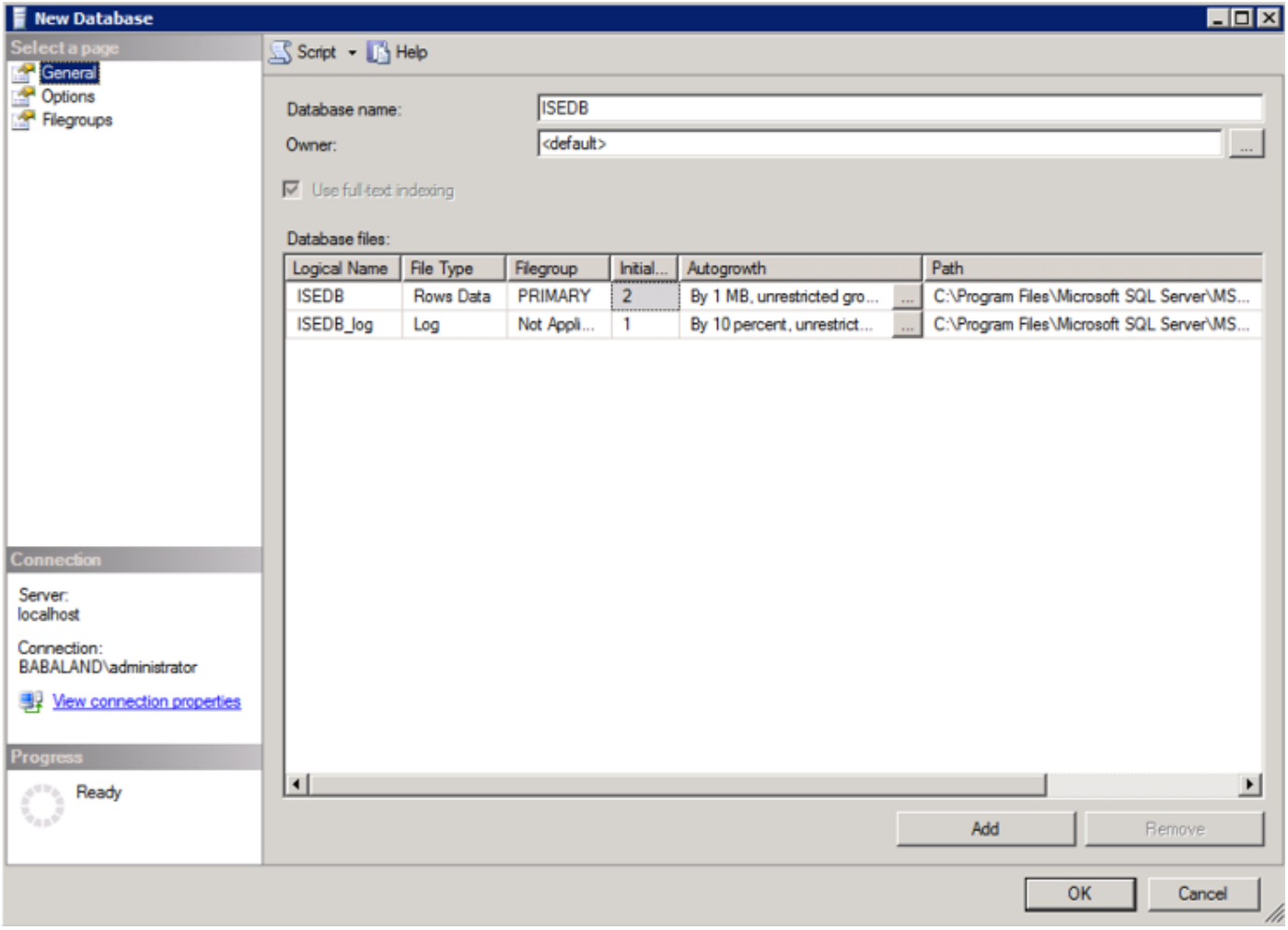
Configurazioni di esempio ODBC

Questa configurazione viene eseguita su Microsoft SQL per generare la soluzione:

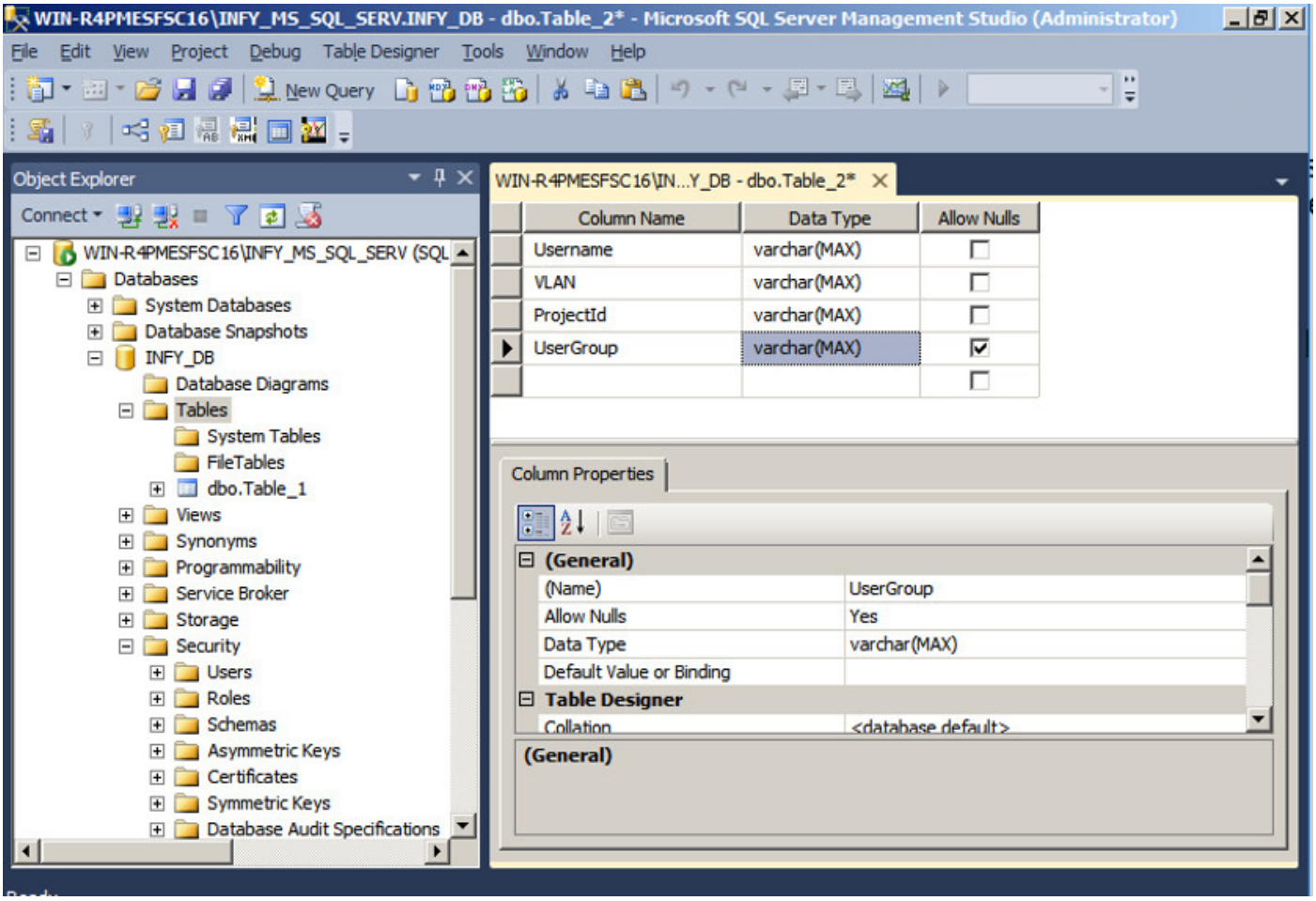
Passaggio 1. Aprire SQL Server Management Studio (**menu Start > Microsoft SQL Server**) per creare un database:



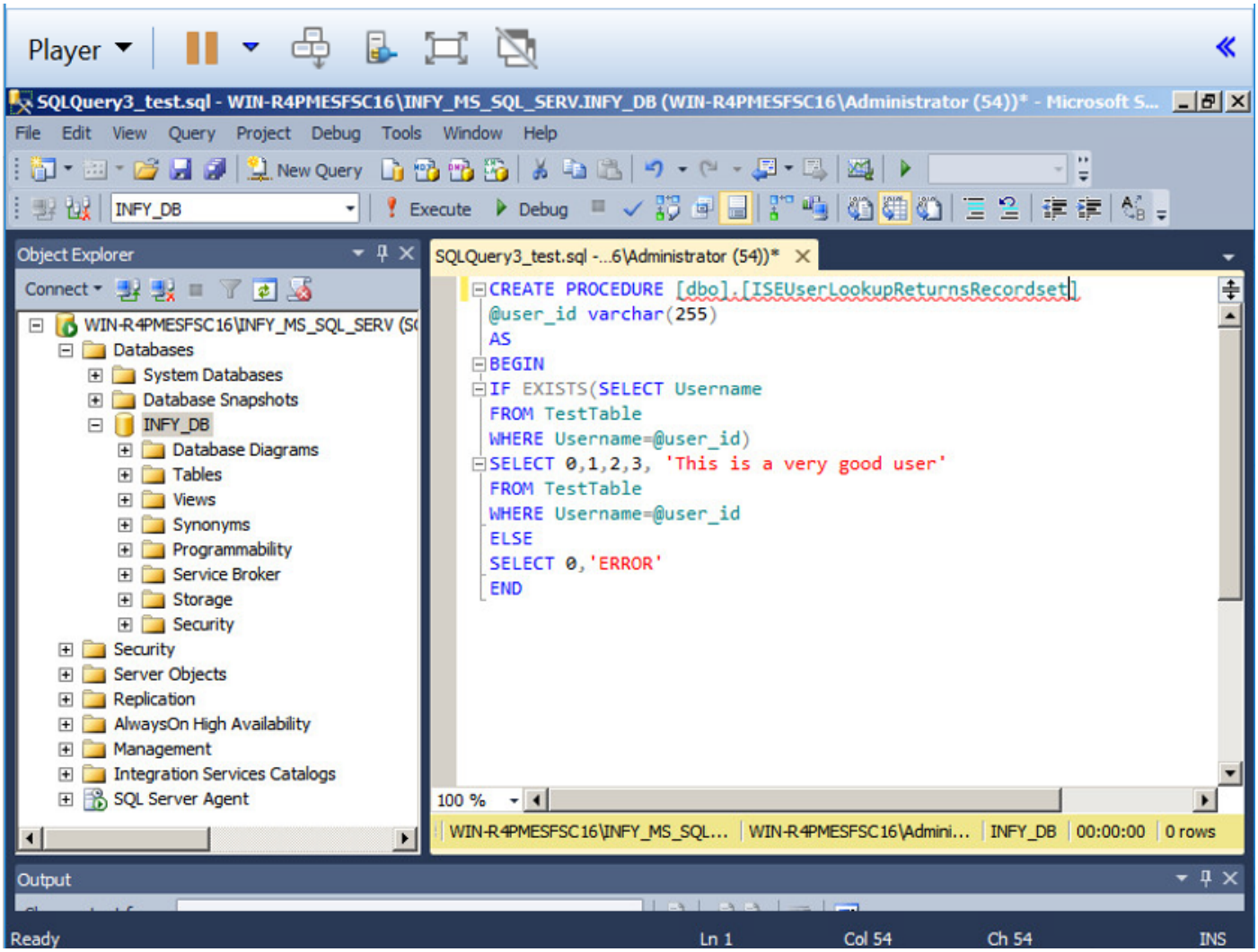
Passaggio 2. Specificare un nome e creare il database.



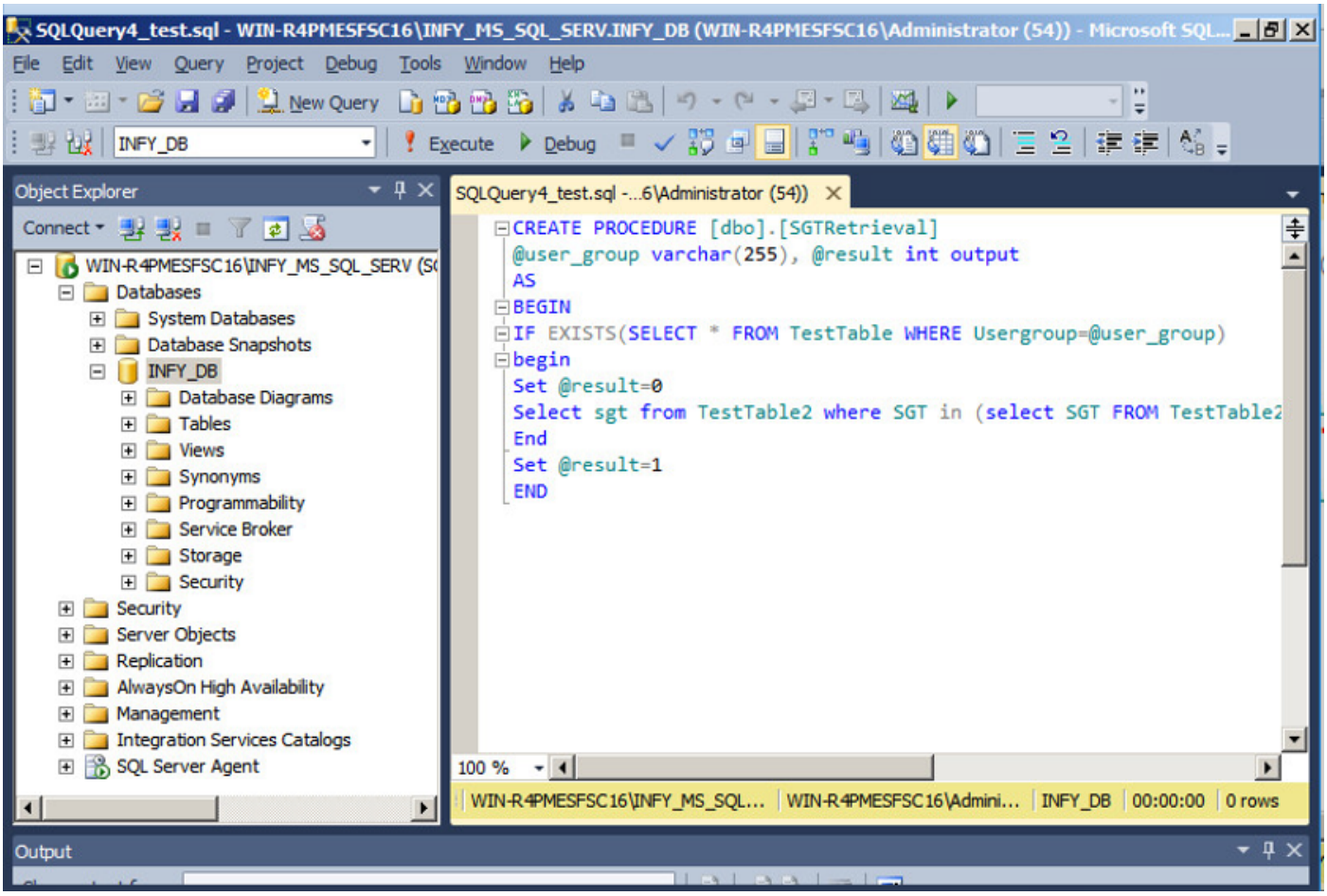
Passaggio 3. Creare una nuova tabella con le colonne obbligatorie come parametri per gli endpoint da autorizzare.



Passaggio 4. Creare una **routine** per verificare se il nome utente esiste.



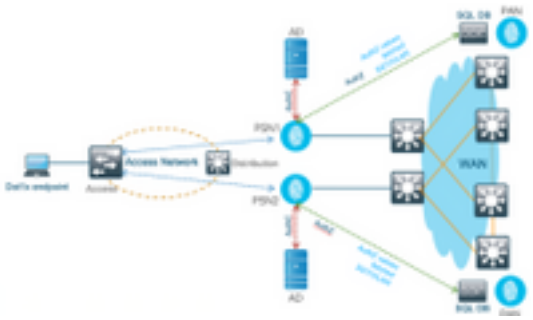
Passaggio 5. Creare una procedura per recuperare gli attributi (SGT) dalla tabella.

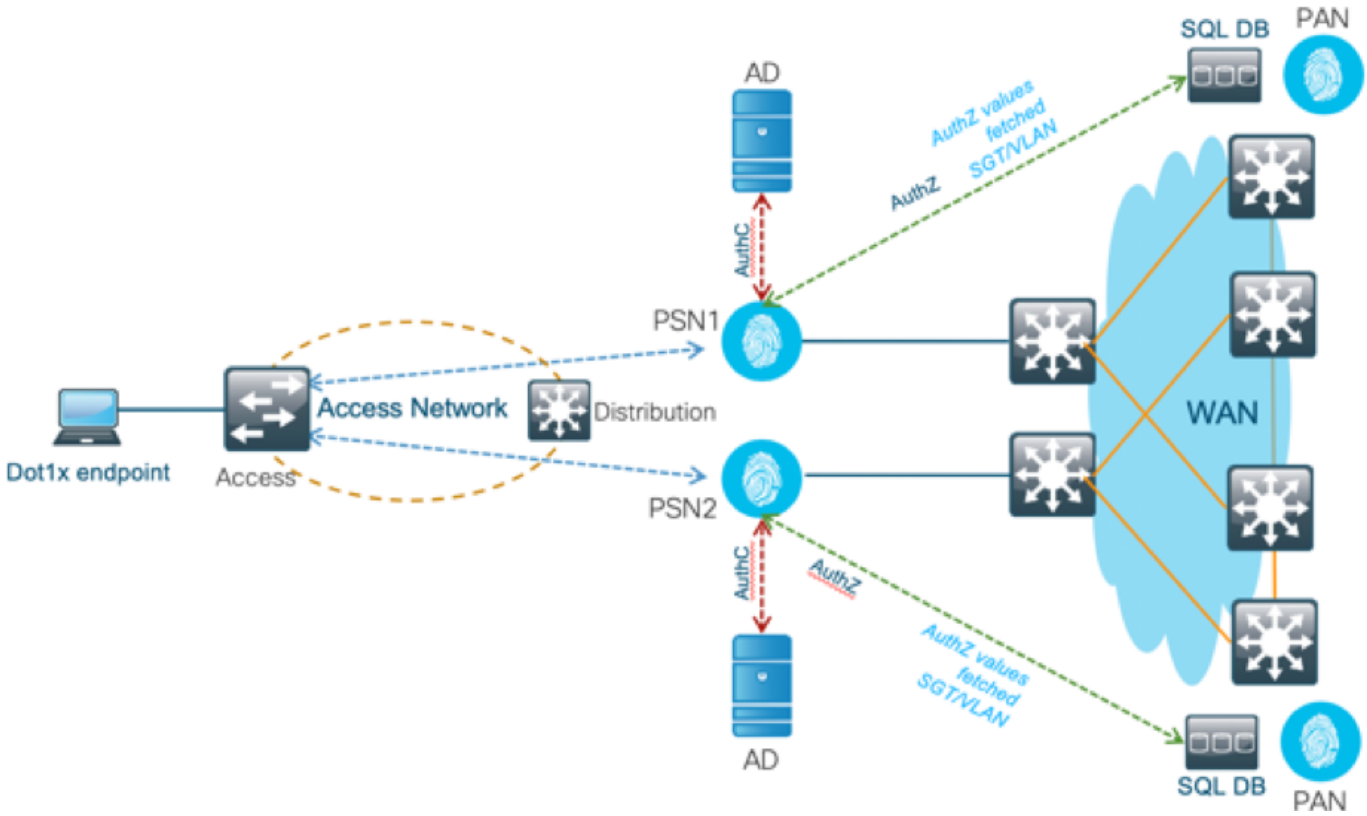


In questo documento, Cisco ISE è integrato con la soluzione Microsoft SQL per soddisfare i requisiti di scalabilità delle autorizzazioni su reti aziendali di grandi dimensioni.

Flusso di lavoro della soluzione (ISE 2.7 e precedenti)

In questa soluzione, Cisco ISE è integrato con Active Directory (AD) e Microsoft SQL. AD viene utilizzato come archivio di ID di autenticazione e MS SQL per l'autorizzazione. Durante il processo di autenticazione, il dispositivo di accesso alla rete (NAD) inoltra le credenziali dell'utente al PSN, il server AAA nella soluzione IBN. PSN convalida le credenziali dell'endpoint con l'archivio ID di Active Directory e autentica l'utente. I criteri di autorizzazione fanno riferimento al database MS SQL per recuperare i risultati autorizzati, ad esempio SGT / VLAN, per i quali viene utilizzato l'**ID utente** come riferimento.





Vantaggi

Questa soluzione presenta i seguenti vantaggi, che la rendono flessibile:

- Cisco ISE può sfruttare tutte le funzionalità aggiuntive offerte dal database esterno.
- Questa soluzione non dipende da alcun limite di scala Cisco ISE.

Svantaggi

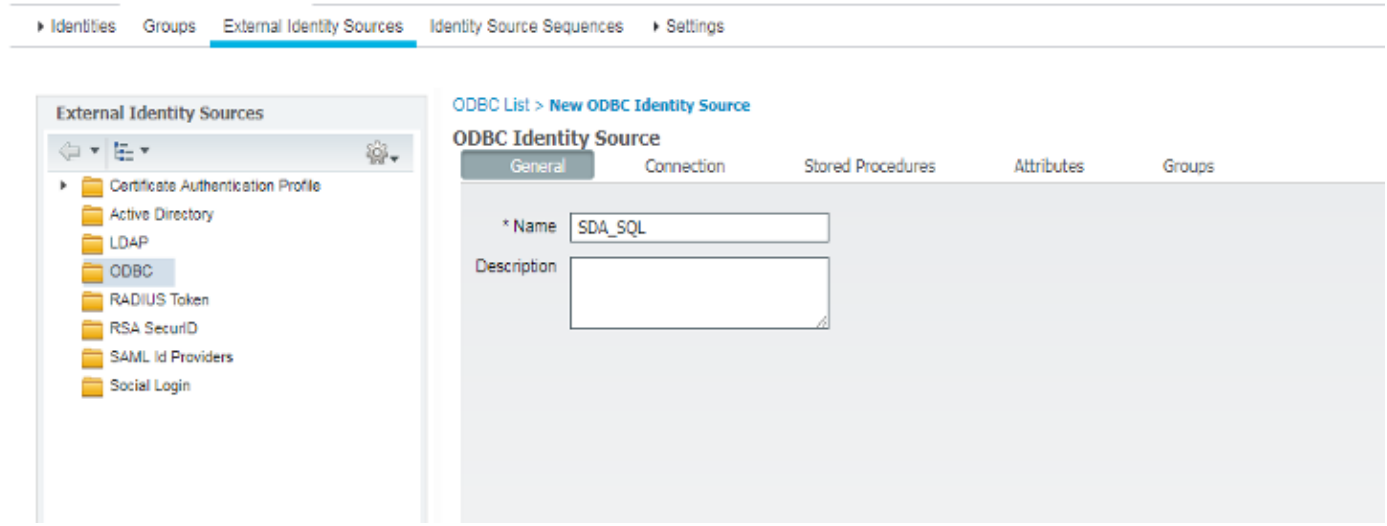
Questa soluzione presenta i seguenti svantaggi:

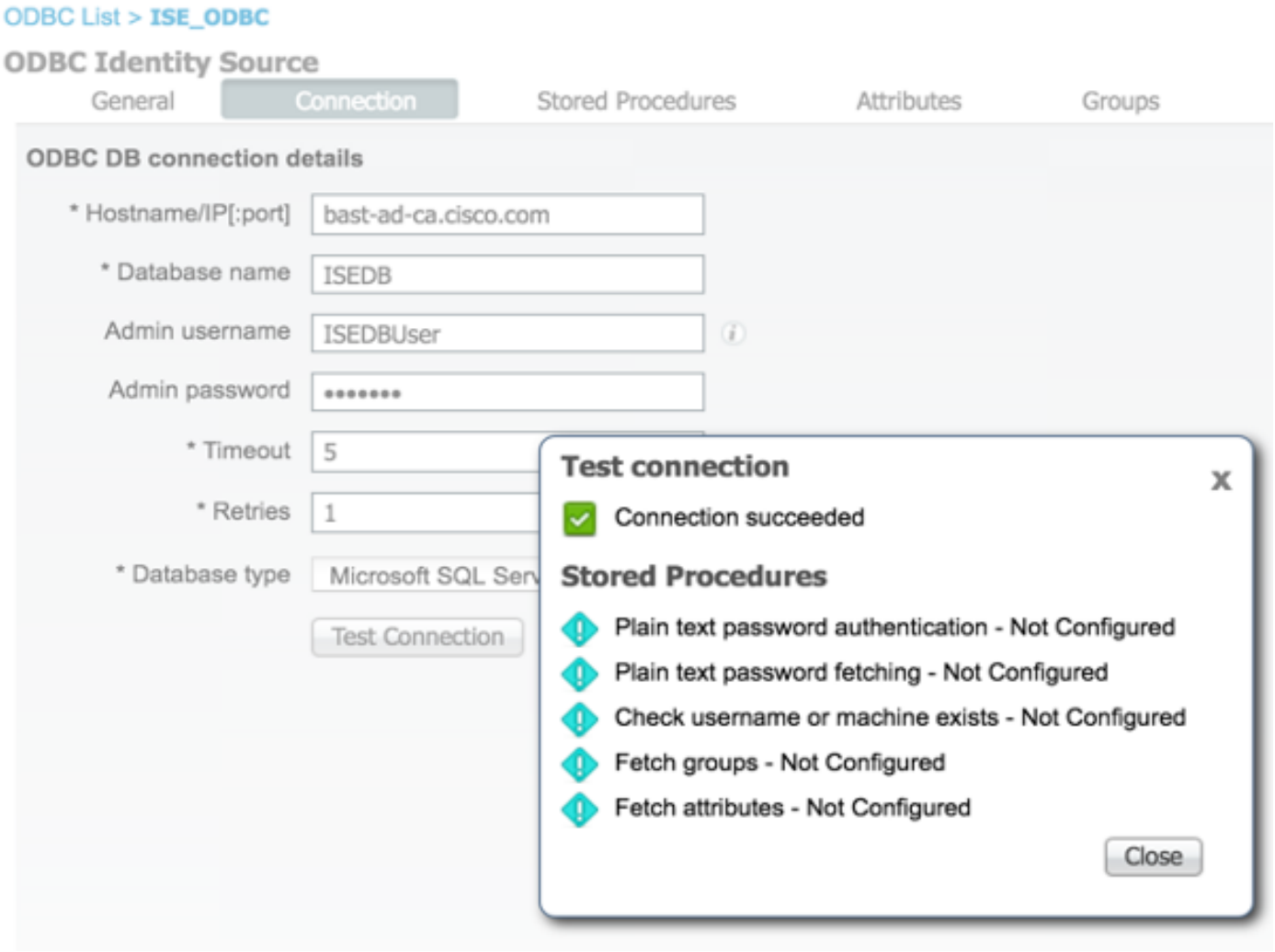
- Richiede ulteriore programmazione per popolare il database esterno con le credenziali dell'endpoint.
- Se il database esterno non è presente localmente come i PSN, questa soluzione dipende dalla WAN, che lo rende il 3° punto di errore nel flusso di dati AAA dell'endpoint.
- Richiede conoscenze aggiuntive per la gestione dei processi e delle procedure DB esterne.
- Ènecessario considerare gli errori causati dalla configurazione manuale dell'ID utente nel database.

Configurazioni di esempio del database esterno

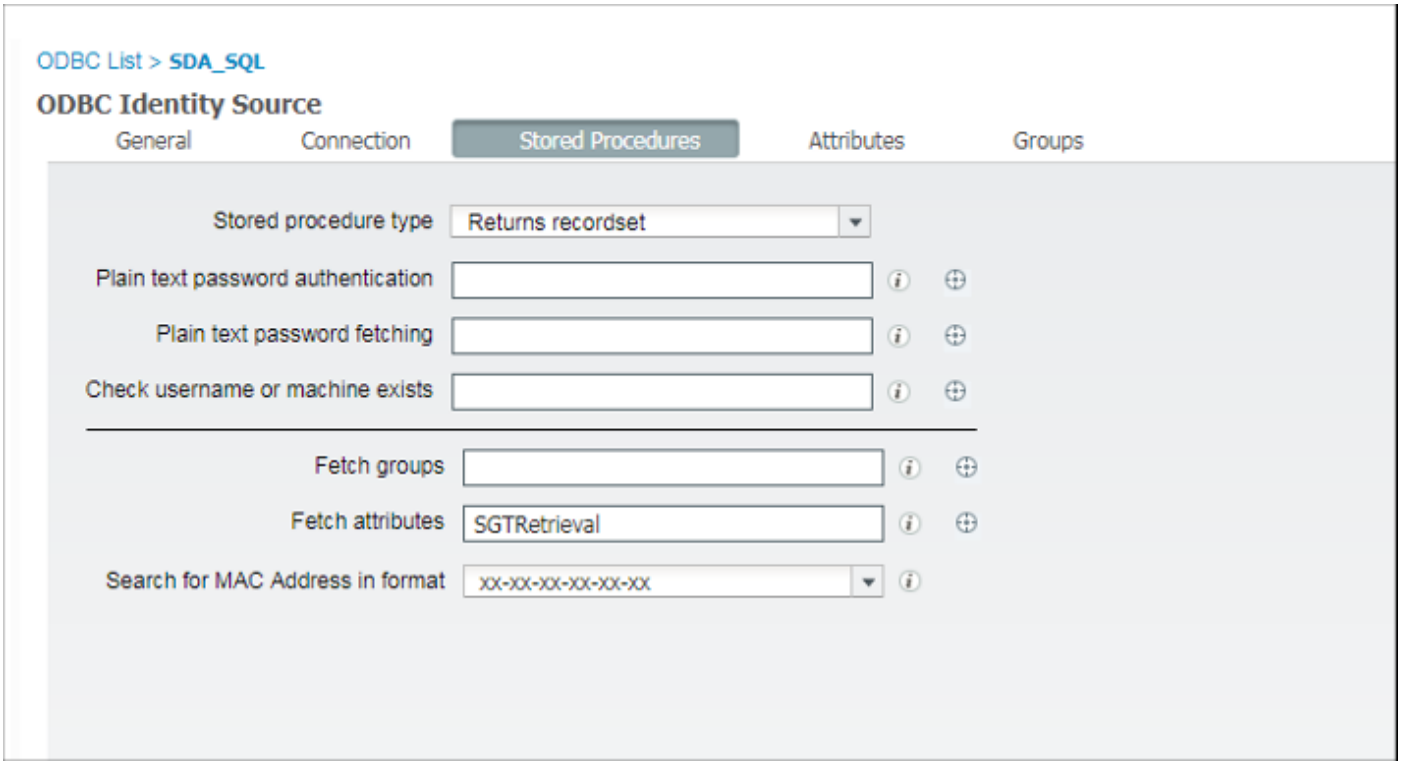
In questo documento, Microsoft SQL viene visualizzato come il database esterno utilizzato come punto di autorizzazione.

Passaggio 1. Creare un archivio identità ODBC in Cisco ISE dal menu **Amministrazione > Origine identità esterna > ODBC** e verificare le connessioni.

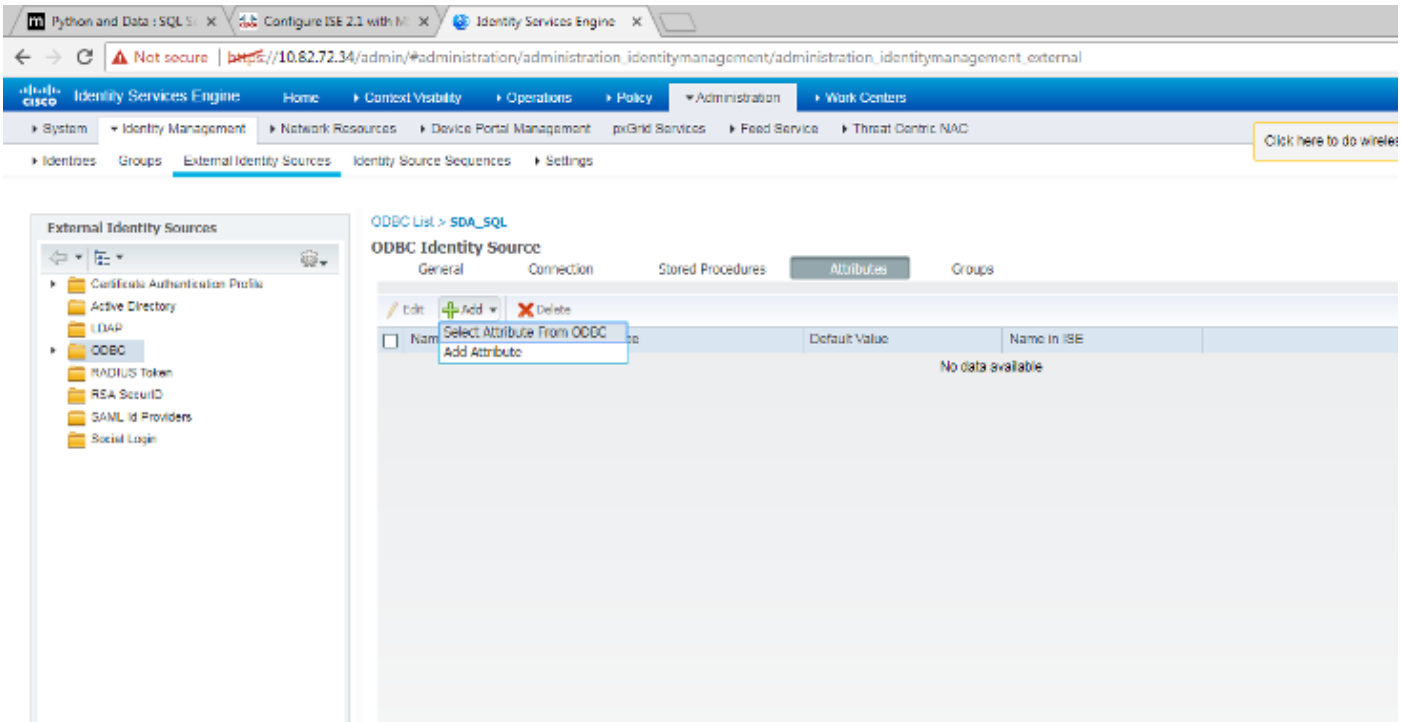


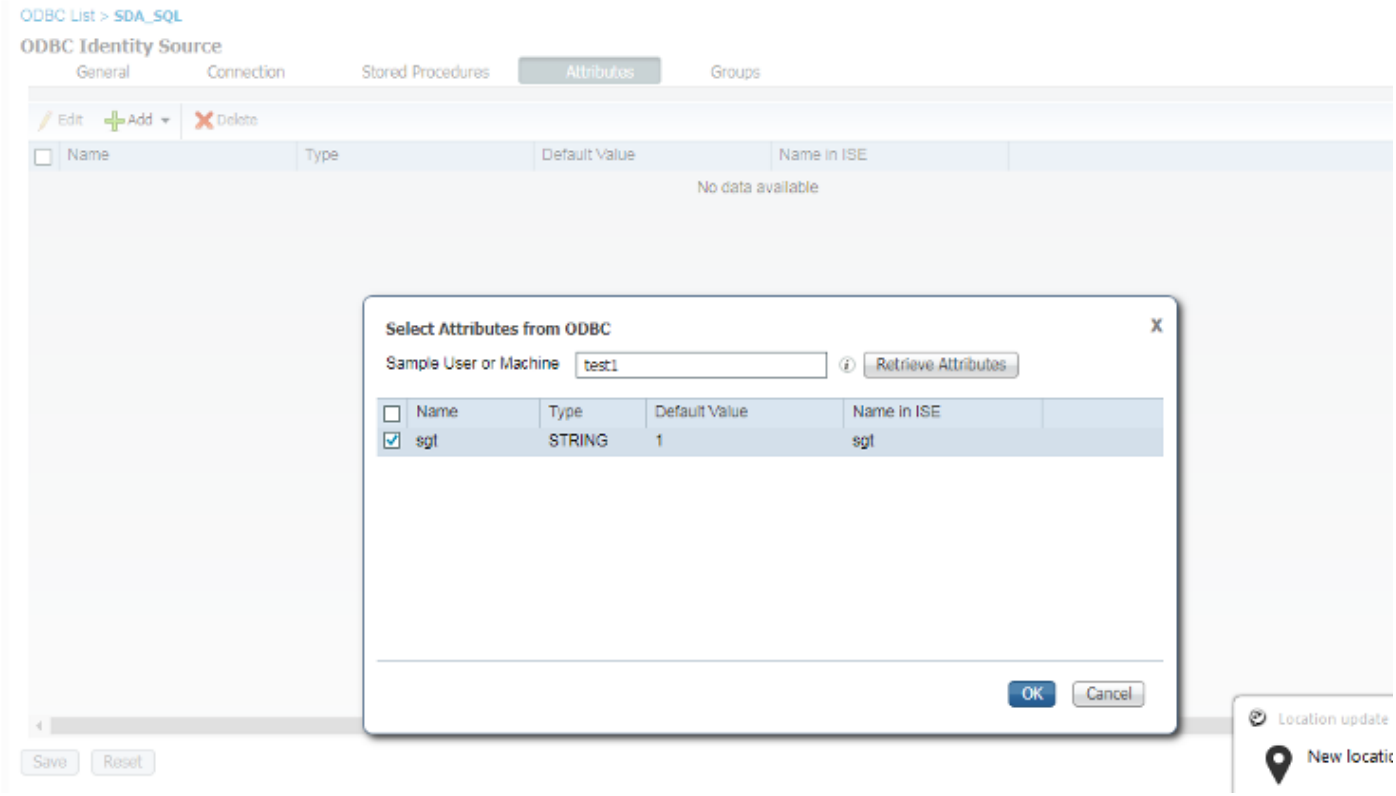


Passaggio 2. Passare alla scheda Stored procedure nella pagina ODBC per configurare le procedure create in Cisco ISE.

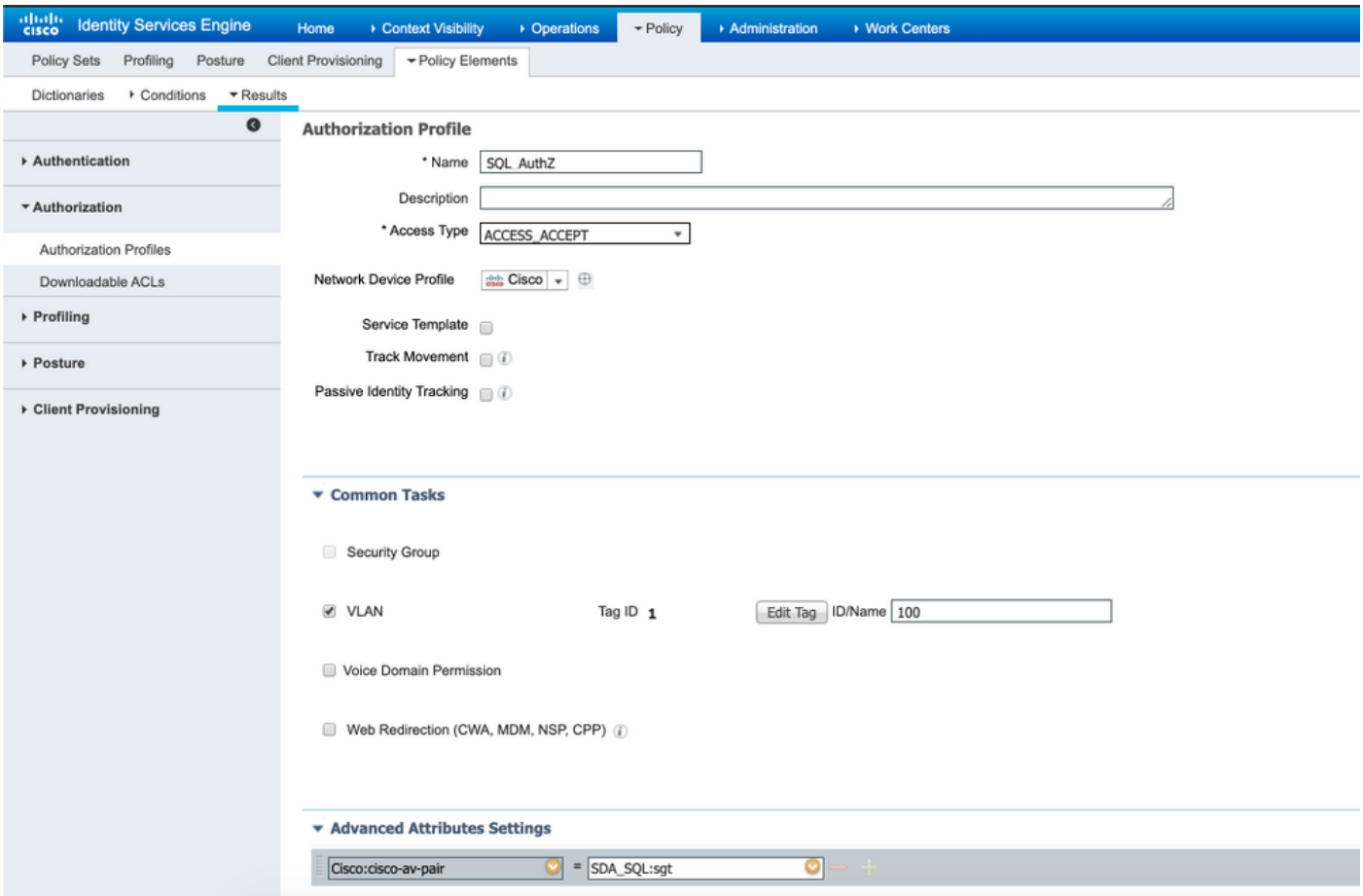


Passaggio 3. Recuperare gli attributi per l'ID utente dall'origine ID ODBC per la verifica.



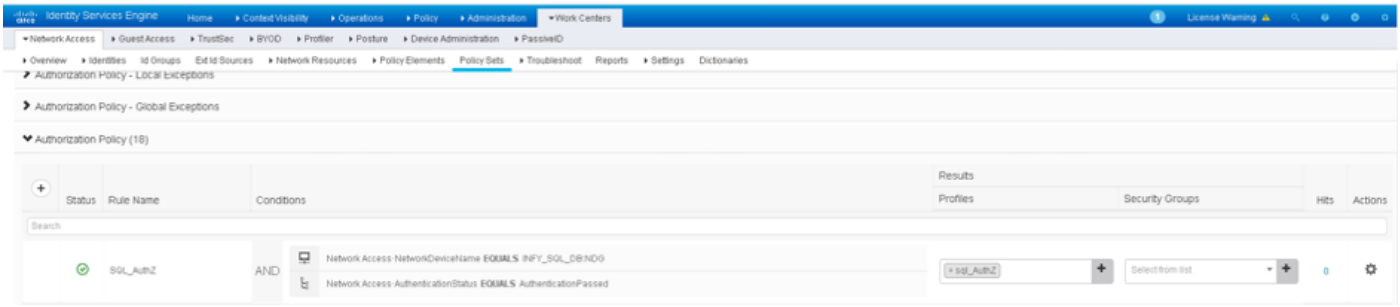


Passaggio 4. Creare un **profilo di autorizzazione** e configurarlo. In Cisco ISE, andare a **Policy > Results > Authorization profile > Advance Attributes Settings** (Criteri > Risultati > Profilo autorizzazione > Impostazioni avanzate attributi) e selezionare l'attributo **Cisco:cisco-av-pair.** Selezionare i valori come <nome del database ODBC>:sgt e salvarlo.



Passaggio 5. Creare un **criterio di autorizzazione** e configurarlo. In Cisco ISE selezionare **Policy > Policy sets > Authorization Policy > Add** (Policy > Set di criteri > Criteri di autorizzazione >

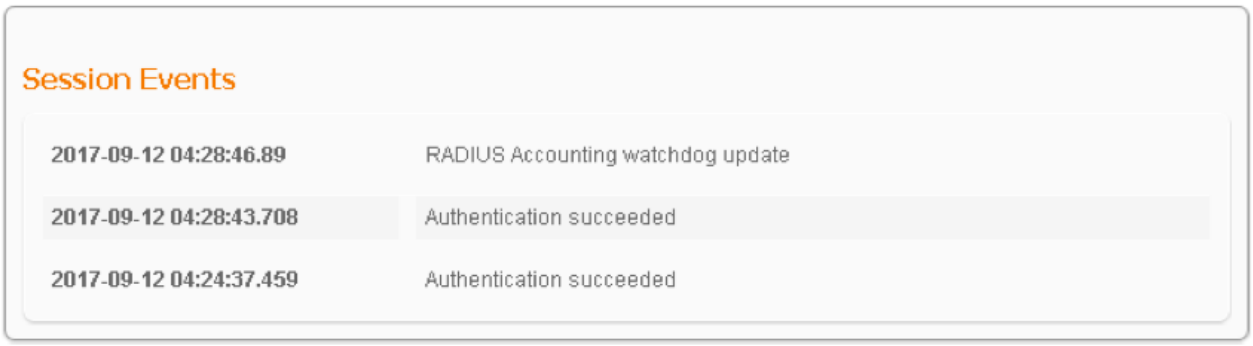
Aggiungi). Impostare la condizione come Identity Source (Origine identità) se il server SQL è. Selezionare il profilo Risultato come profilo di autorizzazione creato in precedenza.



Passaggio 6. Una volta che l'utente è autenticato e autorizzato, i registri contengono il segmento assegnato all'utente per la verifica.

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



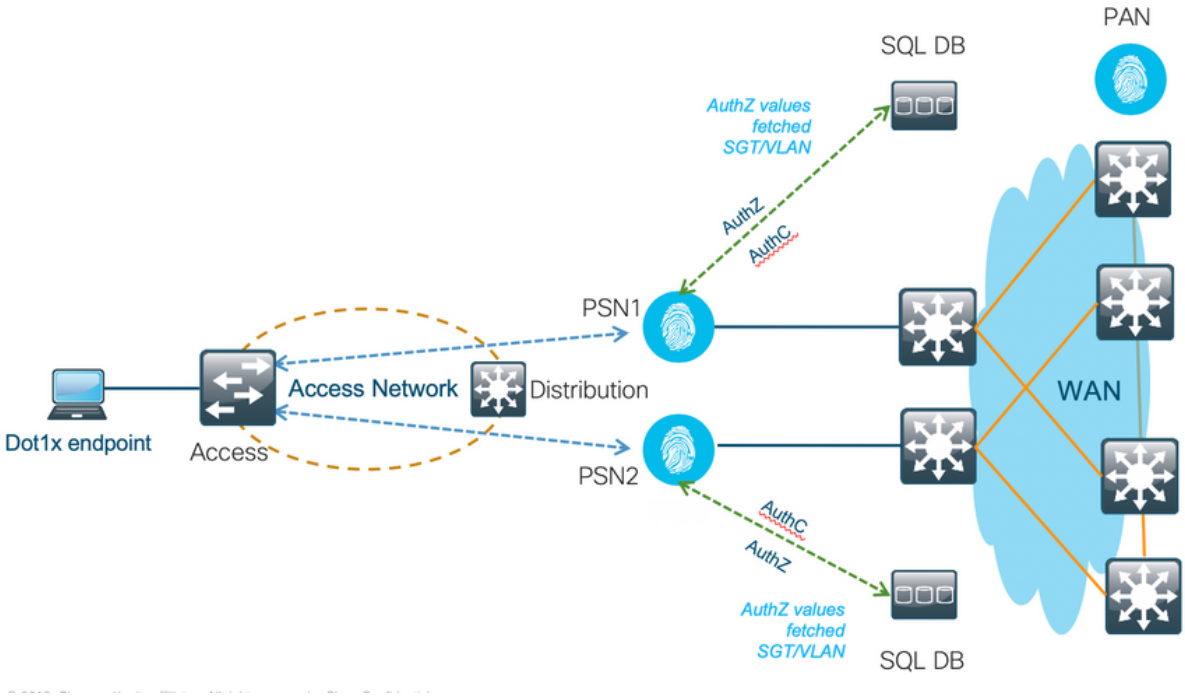
Session Events

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

Flusso di lavoro della soluzione (dopo ISE 2.7)

Dopo ISE 2.7, gli attributi di autorizzazione possono essere recuperati da ODBC come Vlan, SGT, ACL e questi attributi possono essere utilizzati nelle policy.

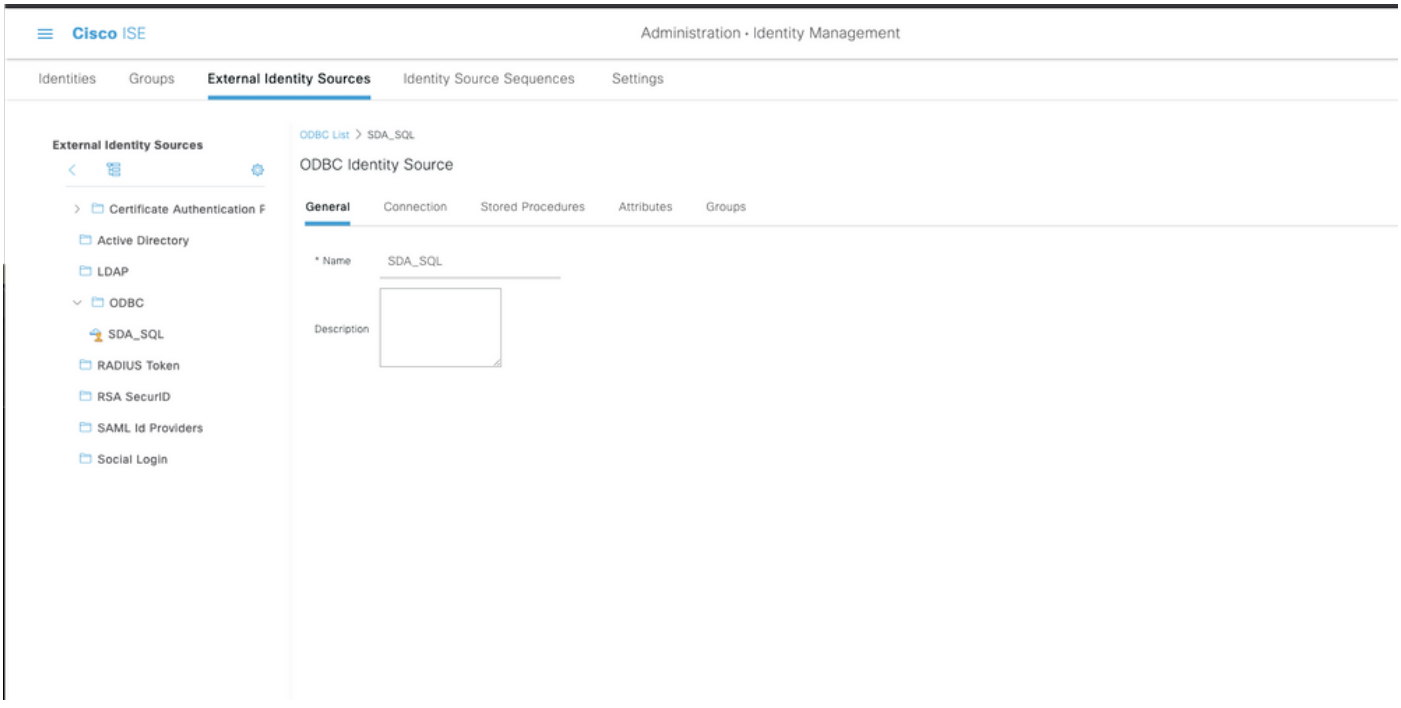
In questa soluzione, Cisco ISE è integrato con Microsoft SQL. MS SQL viene utilizzato come archivio ID per l'autenticazione e per l'autorizzazione. Quando le credenziali degli endpoint vengono fornite al PSN, vengono convalidate rispetto al database MS SQL. Il criterio di autorizzazione fa riferimento al database MS SQL per recuperare i risultati autorizzati, ad esempio SGT / VLAN, per i quali viene utilizzato l'**ID utente** come riferimento.



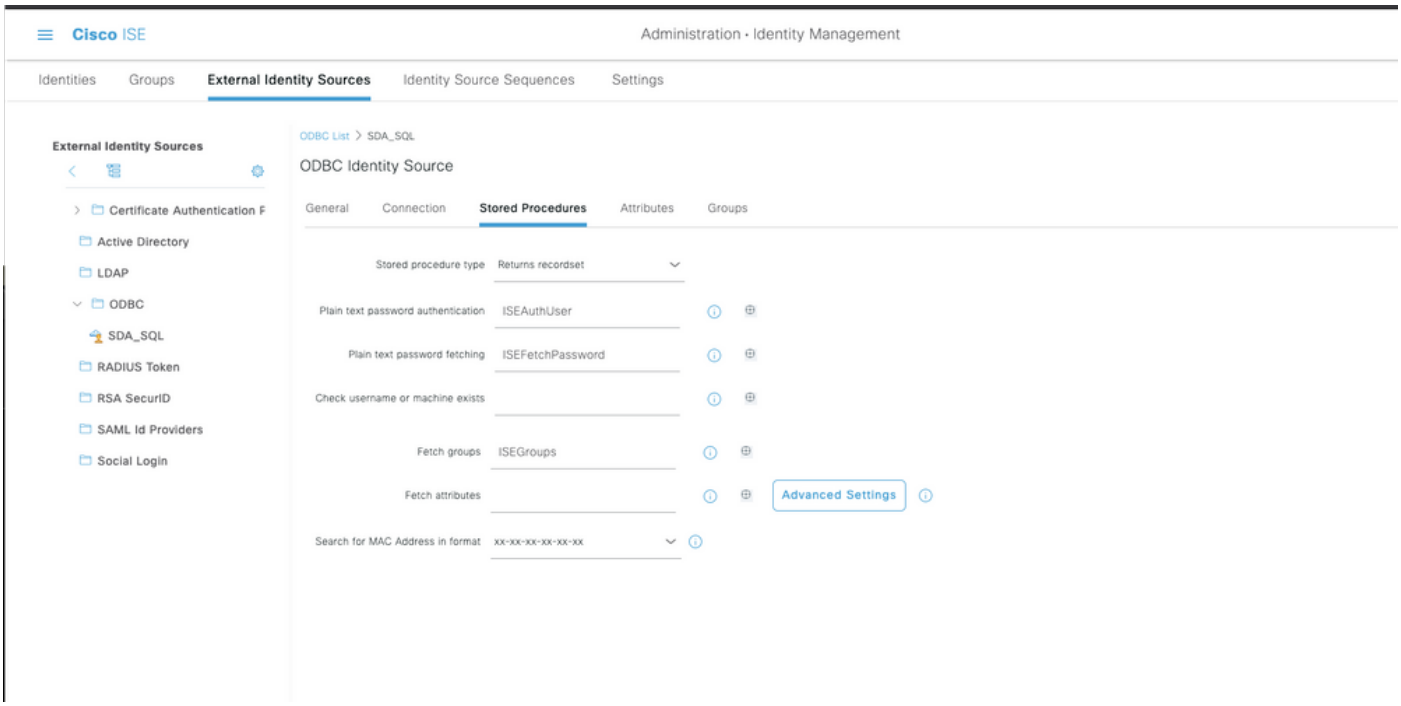
Configurazioni di esempio del database esterno

Seguire la procedura descritta in precedenza per creare il database MS SQL insieme a Nome utente, Password, ID VLAN e SGT.

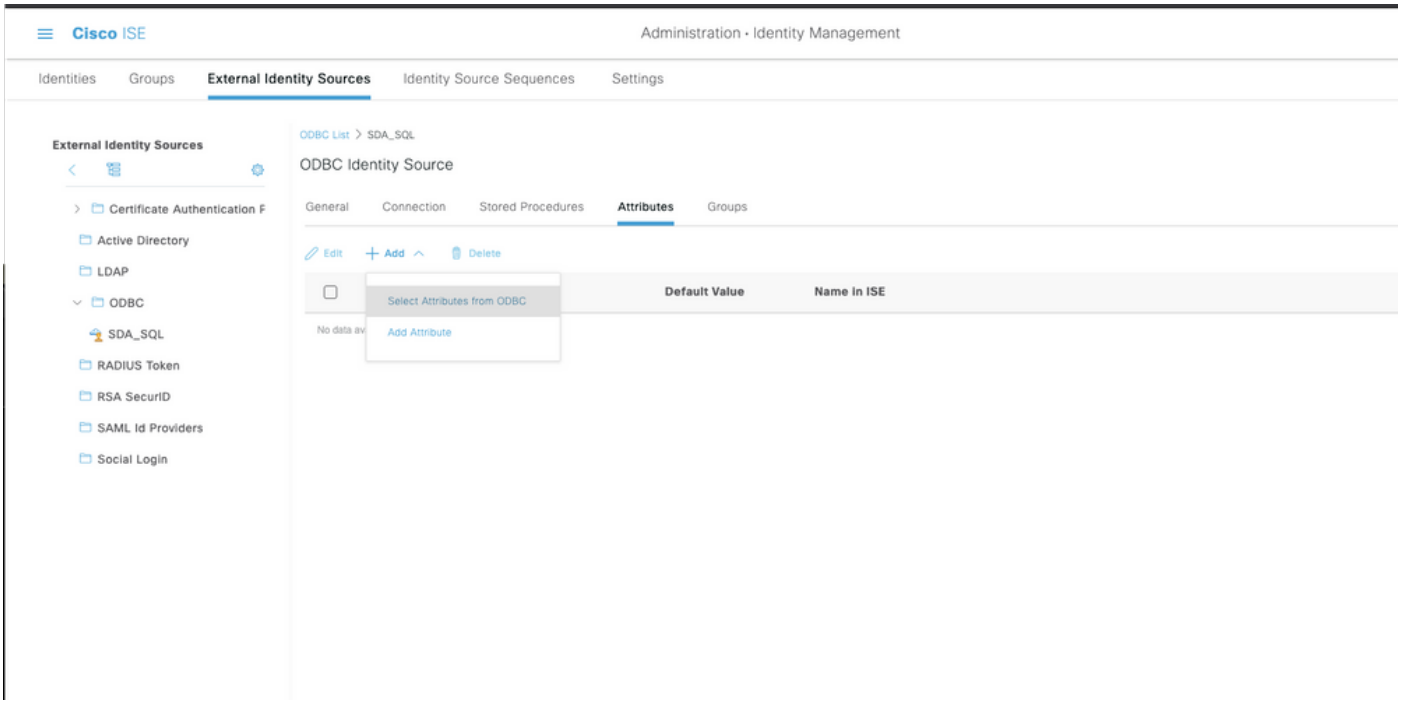
Passaggio 1. Creare un archivio identità ODBC in Cisco ISE dal menu **Amministrazione > Origine identità esterna > ODBC** e verificare le connessioni.

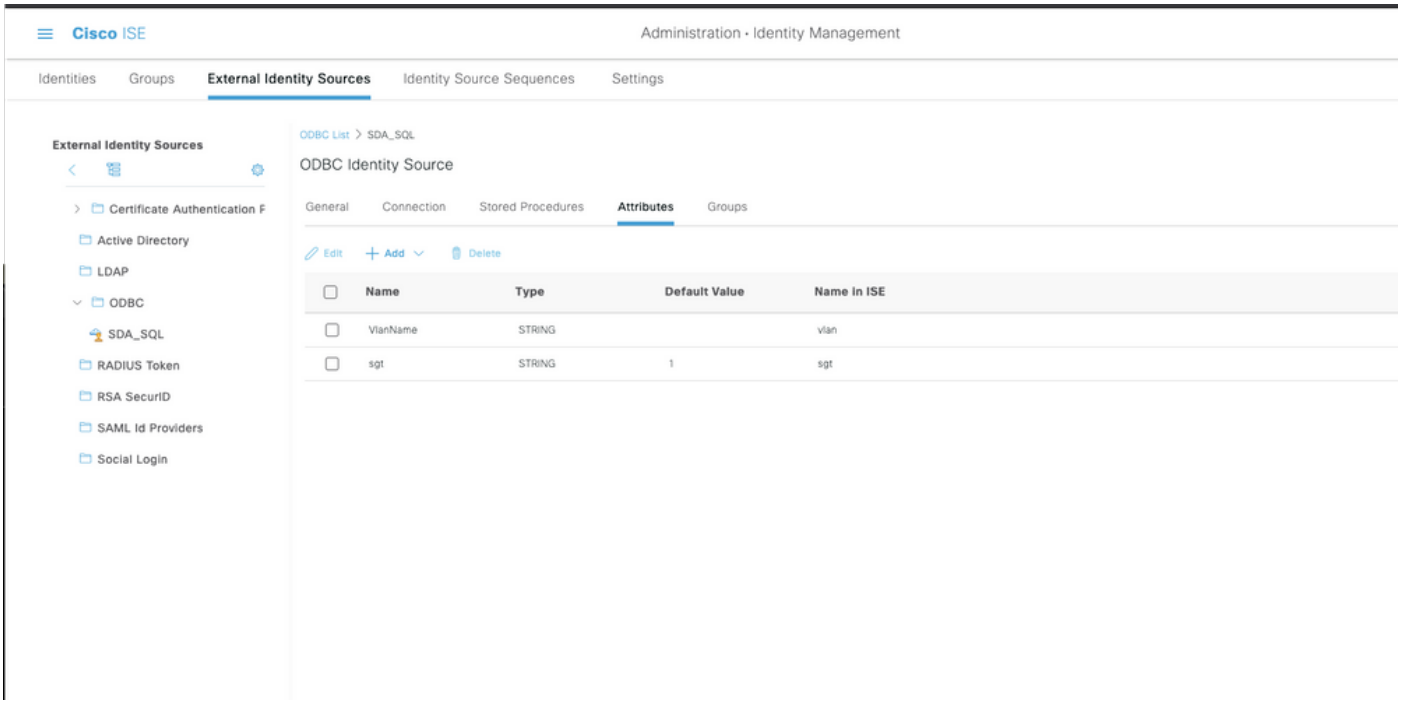


Passaggio 2. Passare alla scheda Stored procedure nella pagina ODBC per configurare le procedure create in Cisco ISE.

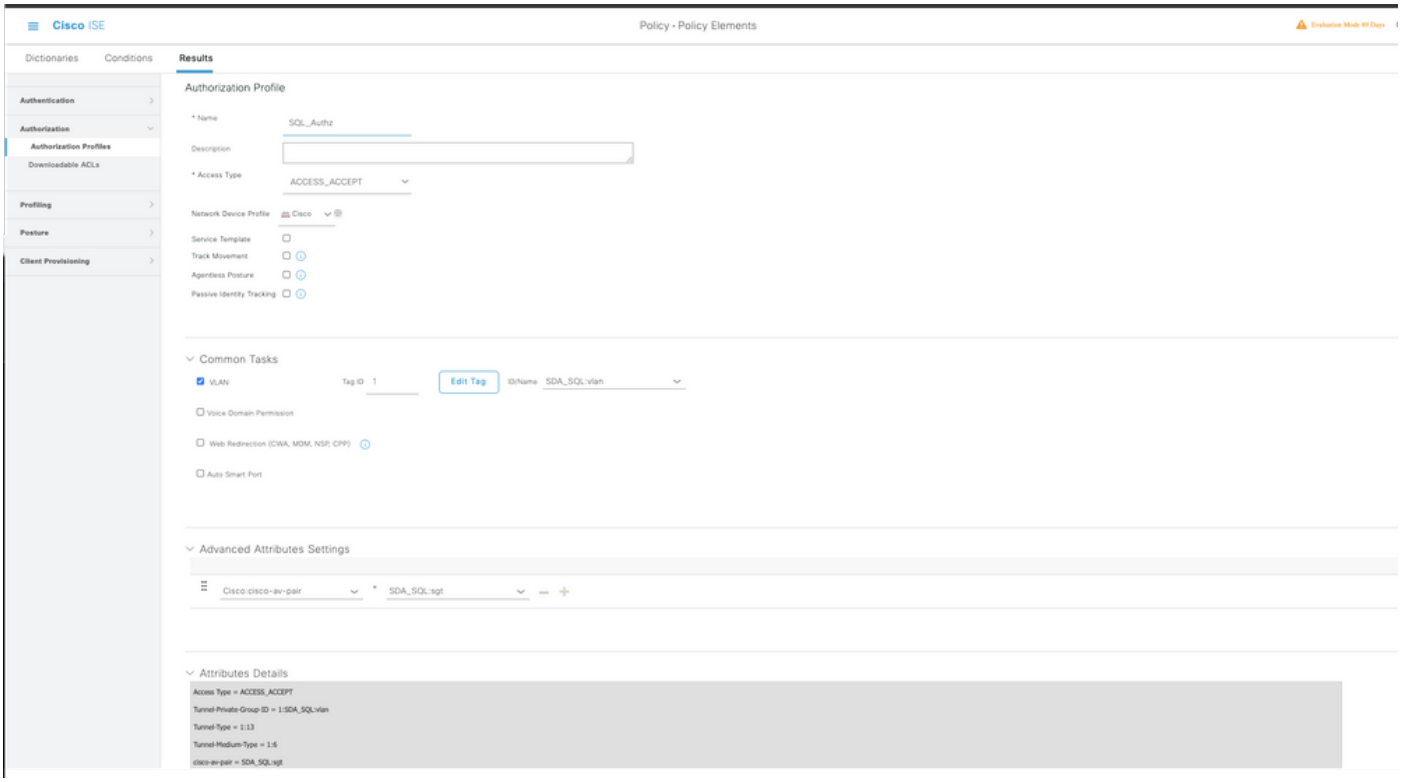


Passaggio 3. Recuperare gli attributi per l'ID utente dall'origine ID ODBC per la verifica.

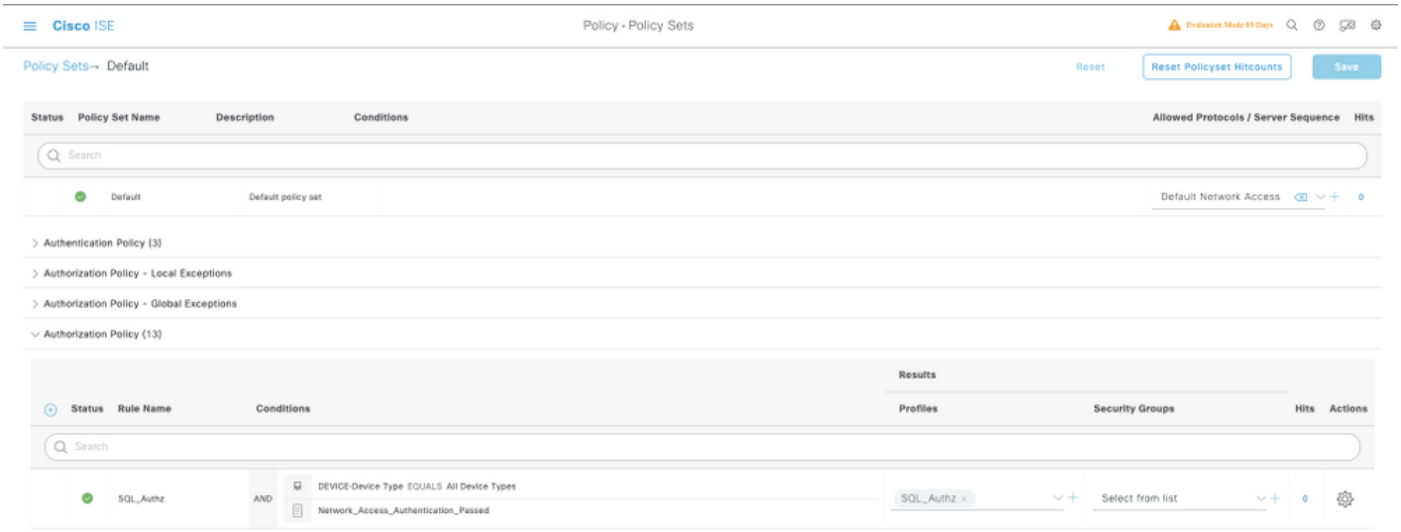




Passaggio 4. Creare un **profilo di autorizzazione** e configurarlo. In Cisco ISE, andare a **Policy > Results > Authorization profile > Advance Attributes Settings** (Criteri > Risultati > Profilo autorizzazione > Impostazioni avanzate attributi) e selezionare l'attributo **Cisco:cisco-av-pair.** Selezionare i valori come <nome del database ODBC>:sgt. In Common Tasks (Attività comuni), selezionare **VLAN** con ID/Nome come <nome del database ODBC>:vlan e salvarlo



Passaggio 5. Creare un **criterio di autorizzazione** e configurarlo. In Cisco ISE selezionare **Policy > Policy sets > Authorization Policy > Add** (Policy > Set di criteri > Criteri di autorizzazione > Aggiungi). Impostare la condizione come Identity Source (Origine identità) se il server SQL è. Selezionare il profilo Risultato come profilo di autorizzazione creato in precedenza.

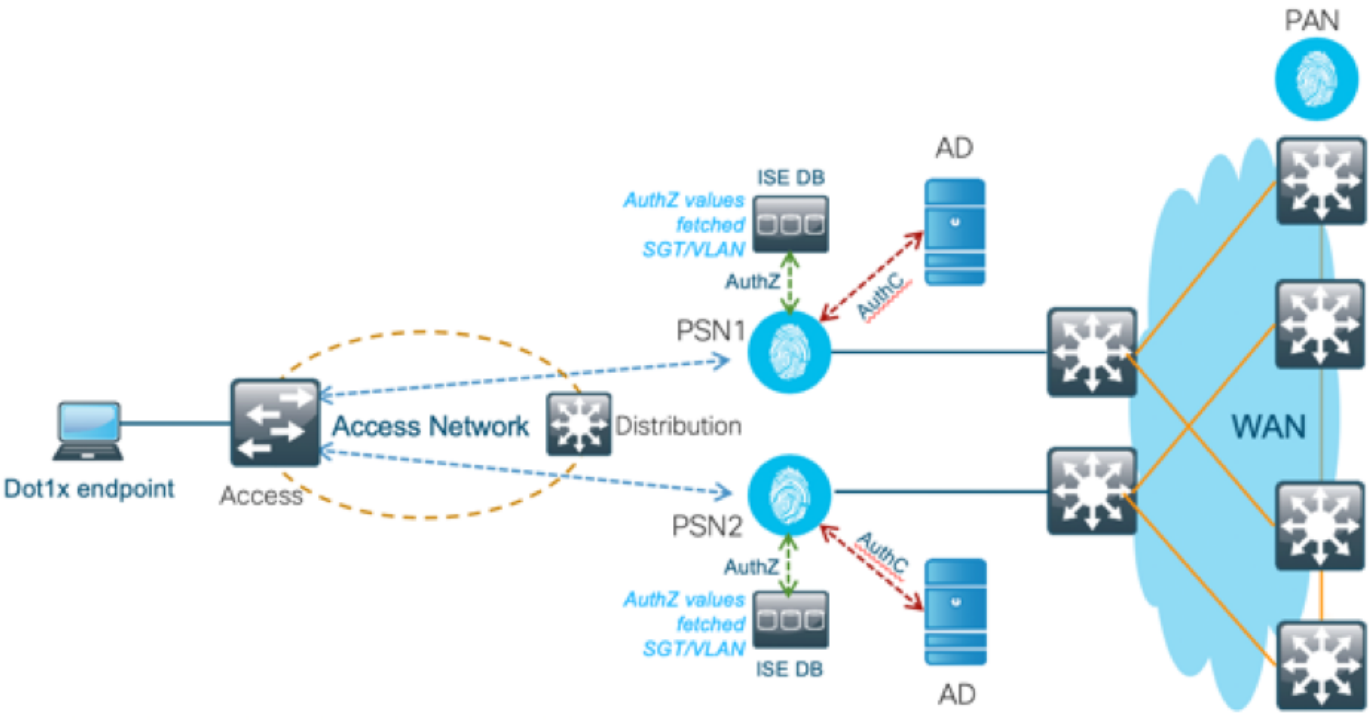


Usa DB interno

La stessa Cisco ISE ha un database integrato che può essere utilizzato per avere ID utente per l'autorizzazione.

Flusso di lavoro della soluzione

In questa soluzione, il database interno di Cisco ISE viene utilizzato come punto di autorizzazione mentre Active Directory (AD) continua a essere l'origine dell'autenticazione. L'ID utente degli endpoint è incluso in Cisco ISE DB insieme **agli attributi personalizzati** che restituiscono i risultati autorizzati, ad esempio SGT o VLAN. Quando le credenziali degli endpoint vengono fornite al PSN, verifica la validità delle credenziali degli endpoint con l'archivio ID di Active Directory e autentica l'endpoint. I criteri di autorizzazione fanno riferimento al database ISE per recuperare i risultati autorizzati, ad esempio SGT / VLAN, per cui viene usato l'ID utente come riferimento.



Vantaggi

Questa soluzione presenta i seguenti vantaggi, che la rendono una soluzione flessibile:

- Cisco ISE DB è una soluzione integrata e pertanto non presenta 3° punto di errore, a differenza della soluzione DB esterna.
- Poiché il cluster Cisco ISE assicura la sincronizzazione in tempo reale tra tutti i soggetti, non vi è dipendenza dalla WAN in quanto il PSN ha tutti gli ID utente e gli attributi personalizzati trasferiti dal PAN in tempo reale.
- Cisco ISE può sfruttare tutte le funzionalità aggiuntive offerte dal database esterno.
- Questa soluzione non dipende da alcun limite di scala Cisco ISE.

Svantaggi

Questa soluzione presenta i seguenti svantaggi:

- Il numero massimo di ID utente che Cisco ISE DB può trattenere è 300.000.
- Ènecessario considerare gli errori causati dalla configurazione manuale dell'ID utente nel database.

Configurazioni di esempio DB interne

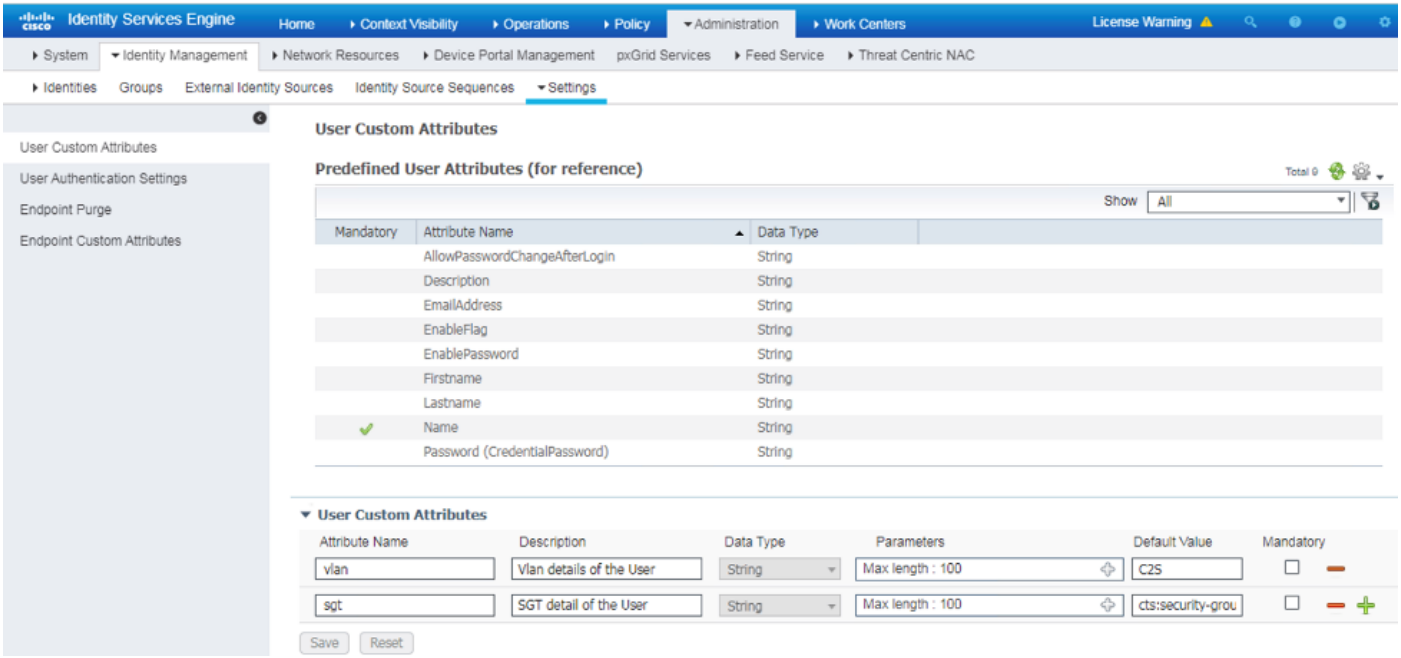
La VLAN e il servizio SGT per utente possono essere configurati per qualsiasi utente nell'archivio di ID interno con un attributo utente personalizzato.

Passaggio 1. Creare nuovi attributi personalizzati dell'utente per rappresentare il valore VLAN e SGT dei rispettivi utenti. Passare a **Amministrazione > Gestione delle identità > Impostazioni > Attributi personalizzati dell'utente.** Creare nuovi attributi personalizzati dell'utente come mostrato nella tabella.

Qui viene mostrata la tabella ISE DB con attributi personalizzati.

Nome attributo	Tipo di dati	Parametri(Lunghezza)	Valore predefinito
VLAN	Stringa	100	C2S (Nome Vlan Predefinito)
sgt	Stringa	100	cts:security-group-tag=0003-0 (valore SGT predefinito)

- In questo scenario, il valore VLAN rappresenta il nome della vlan e il valore sgt rappresenta l'attributo cisco-av-pair del protocollo SGT in formato esadecimale.

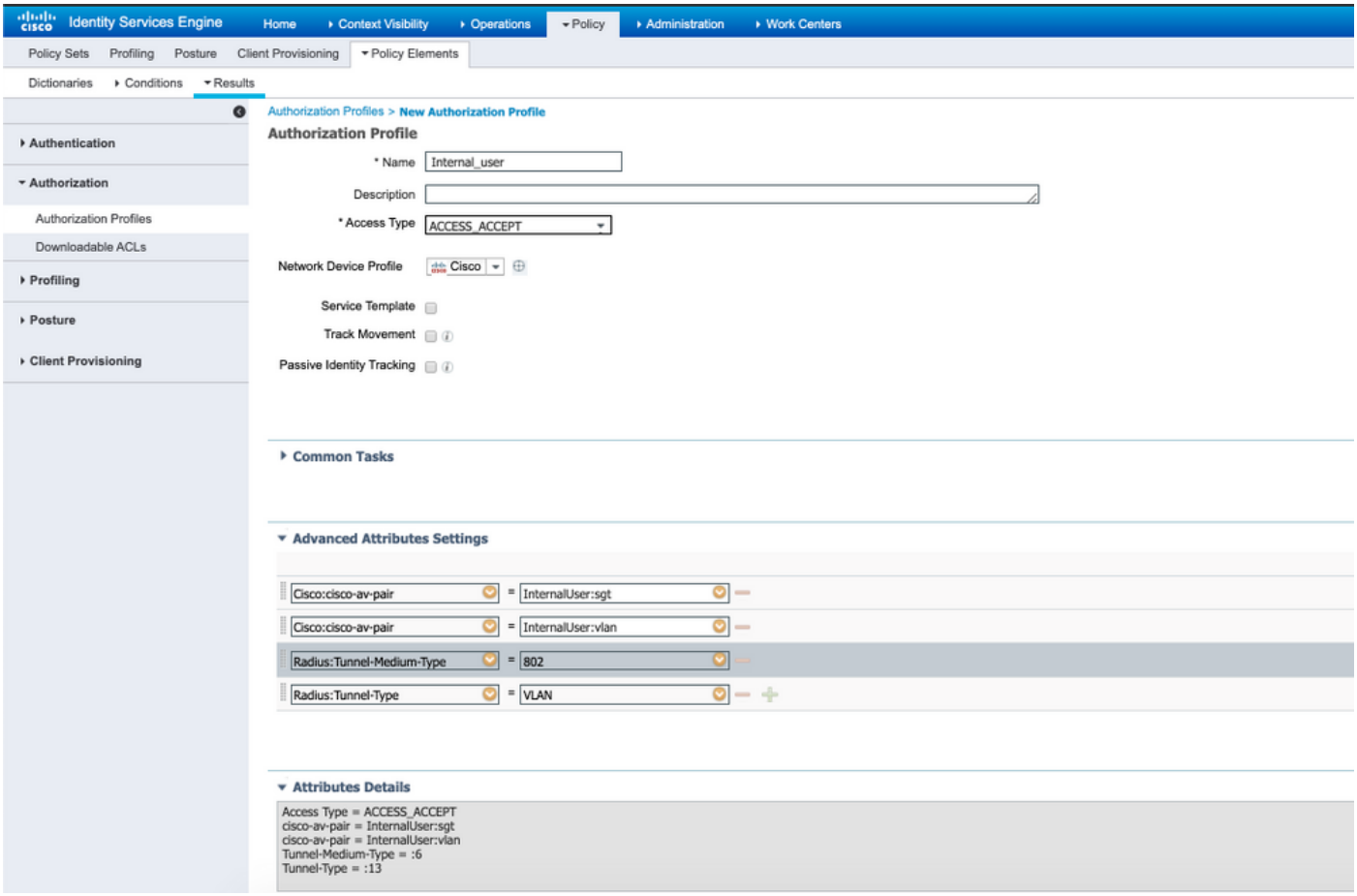


Passaggio 2. Creare un profilo di autorizzazione con attributi personalizzati dall'utente per implicare i valori vlan e sgt dei rispettivi utenti. Passare a **Criterio > Elementi dei criteri > Risultati > Autorizzazione > Profili di autorizzazione > Aggiungi.** Aggiungere gli attributi riportati di seguito in Impostazioni avanzate attributi.

Questa tabella mostra il profilo AuthZ per l'utente interno.

Attributo	Valore
Cisco:cisco-av-pair	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	Utente interno:vlan
Radius:Tunnel-Medium-Type	802
Radius:Tipo Tunnel	VLAN

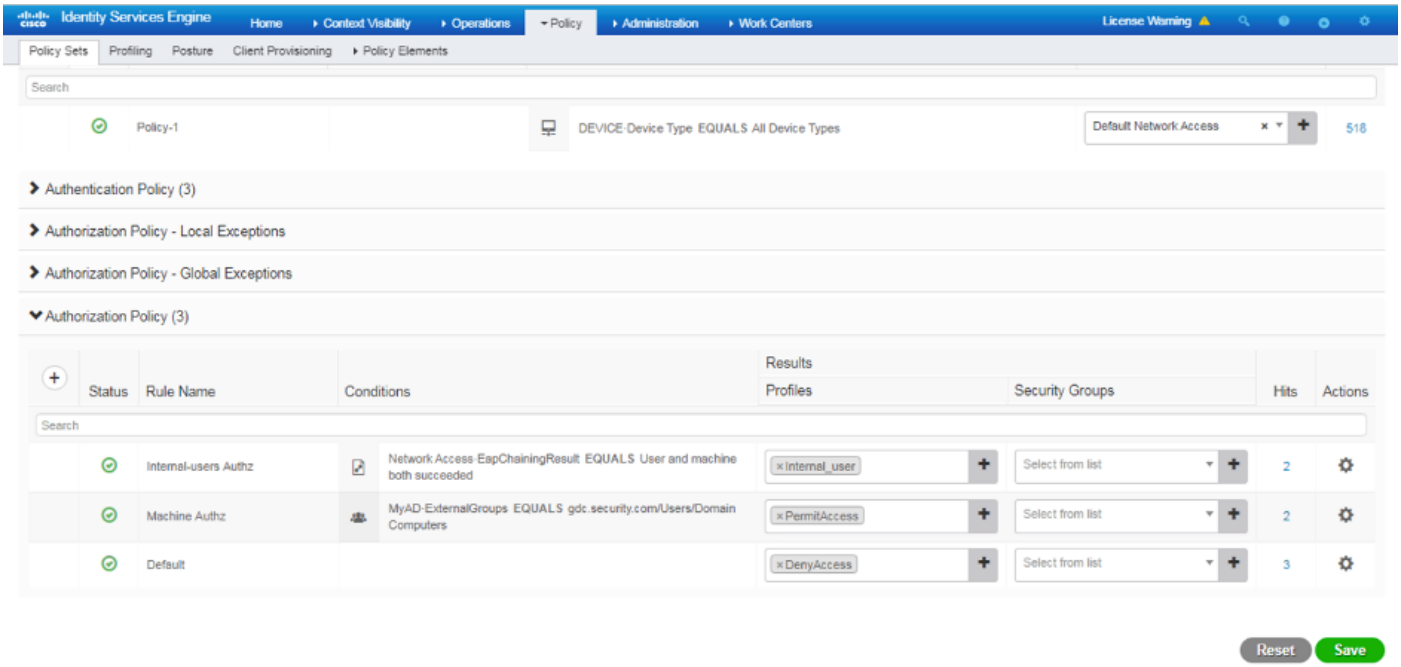
Come mostrato nell'immagine, per gli utenti interni il profilo **Internal_user** è configurato con SGT e Vlan configurati rispettivamente come **InternalUser:sgt** e **InternalUser:vlan**.



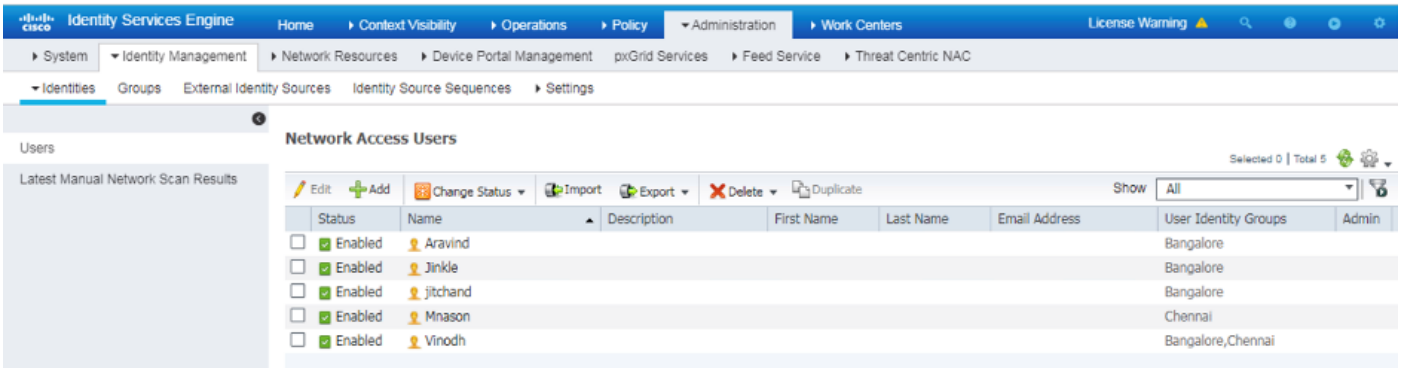
Passaggio 3. Creare il criterio di autorizzazione, passare a **Criterio > Set di criteri > Criterio-1 > Autorizzazione.** Creare i criteri di autorizzazione con le condizioni indicate di seguito e mapparli ai rispettivi profili di autorizzazione.

In questa tabella viene illustrato il criterio AuthZ per l'utente interno.

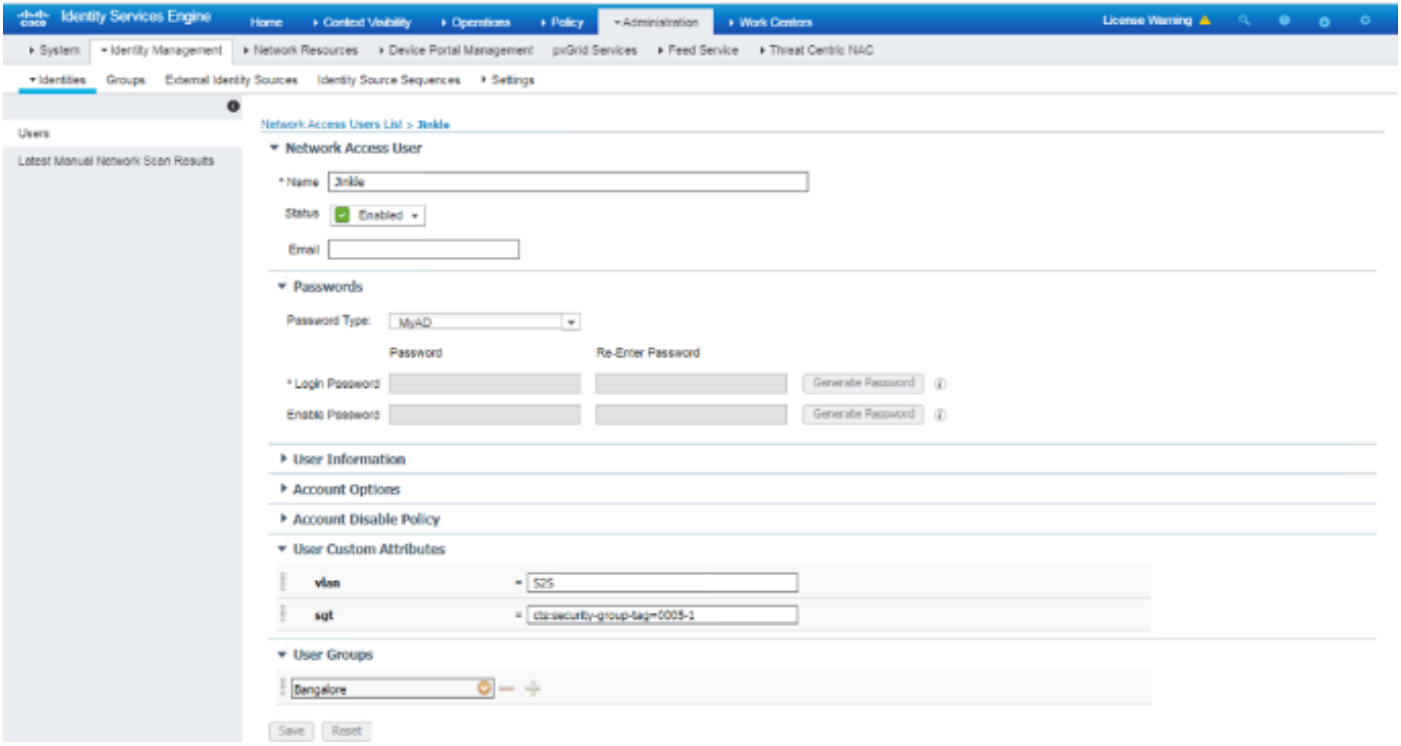
Nome regola	Condizione	Profilo di autorizzazione dei risultati
Autenticazione_utente_interno	Se Network Access.EapChainingResults è uguale a sia a utente che a computer	Utente_interno
Autorizzazione_Solo_Computer	Se MyAD.ExternalGroups è uguale a gdc.security.com/Users/Domain Computer	PermitAccess



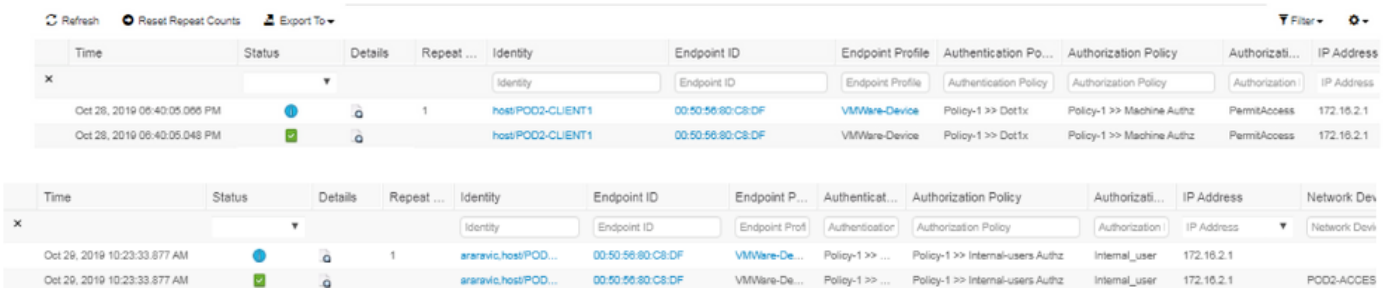
Passaggio 4. Creare identità utente in blocco con attributi personalizzati con i dettagli utente e i rispettivi attributi personalizzati nel modello CSV. Importare il file CSV selezionando **Amministrazione > Gestione identità > Identità > Utenti > Importa > Scegliere il file > Importa.**



Nell'immagine è illustrato un utente di esempio con i dettagli degli attributi personalizzati. Selezionare l'utente e fare clic su Modifica per visualizzare i dettagli degli attributi personalizzati mappati all'utente corrispondente.



Passaggio 5: Verificare i log attivi:



Controllare la sezione **Result** per verificare se l'attributo **Vlan** & **SGT** viene inviato come parte di Access-Accept.

Conclusioni

Questa soluzione consente ad alcuni dei clienti delle grandi aziende di scalare in base ai propri requisiti. L'aggiunta o l'eliminazione degli ID utente deve essere effettuata con cautela. Gli errori, se attivati, possono comportare l'accesso non autorizzato per gli utenti originali o viceversa.

Informazioni correlate

Configurare Cisco ISE con MS SQL tramite 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

Glossario

AAA	Accounting autorizzazione autenticazione
AD	Active Directory
AuthC	Autenticazione
AuthZ	Authorization
DB	Database
PUNTO1X	802.1X
IBN	Identity Based Network
ID	Database delle identità
ISE	Identity Services Engine
MnT	Monitoraggio e risoluzione dei problemi
MsSQL	Microsoft SQL

ODBC	Open DataBase Connectivity
PANORAMICA	Nodo amministrazione criteri
PSN	Policy Services Node
SGT	Tag Secure Group
SQL	Structured Query Language
VLAN	LAN virtuale
WAN	Wide Area Network

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).