

Vereenvoudigd toegangsbeleid met ODBC en ISE-database (aangepaste kenmerken) voor netwerk met grootschalige campus

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Technologische trends](#)

[Probleem](#)

[Voorgestelde oplossing](#)

[Configuratie met externe DB](#)

[ODBC-voorbeeldconfiguraties](#)

[Workflow voor oplossing \(ISE 2.7 en eerder\)](#)

[Voordelen](#)

[Nadelen](#)

[Externe DB-voorbeeldconfiguraties](#)

[Workflow voor oplossing \(na ISE 2.7\)](#)

[Externe DB-voorbeeldconfiguraties](#)

[Interne DB gebruiken](#)

[Workflow voor oplossing](#)

[Voordelen](#)

[Nadelen](#)

[Interne DB-voorbeeldconfiguraties](#)

[Conclusie](#)

[Gerelateerde informatie](#)

[Woordenlijst](#)

Inleiding

Dit document beschrijft grootschalige campusimplementatie zonder compromissen te sluiten op de functies en de beveiliging. Cisco's endpoint security oplossing, Identity Services Engine (ISE) voldoet aan deze vereiste met integratie met een externe identiteitsbron.

Voor grootschalige netwerken met meer dan 50 geo-locaties, 4000+ verschillende gebruikersprofielen en 600.000 eindpunten of meer moeten traditionele IBN-oplossingen vanuit een ander perspectief worden bekeken - meer dan alleen functies, of het nu met alle functies schaalbaar is. Intent-Based Network (IBN)-oplossing in de traditionele grootschalige netwerken van vandaag vereist extra aandacht voor schaalbaarheid en beheergemak en niet alleen voor de functies ervan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

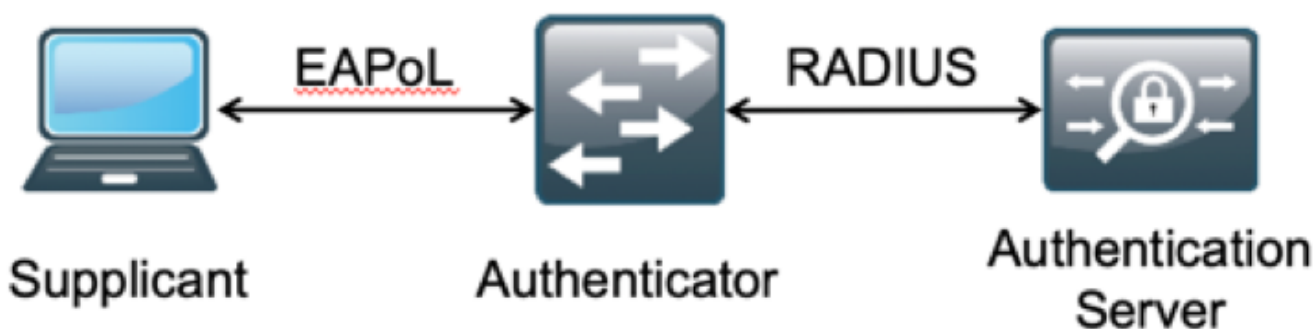
- Cisco Identity Services Engine (ISE) versie 2.6, patch 2 en versie 3.0
- Windows Active Directory (AD)-server 2008 release 2
- Microsoft SQL Server 2012

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als het netwerk actief is, moet u de mogelijke gevolgen van elke configuratie begrijpen.

Achtergrondinformatie

In een IBN-oplossing (Identity Based Network) zijn de basiselementen Supplicant, Authenticator en Verificatie (AAA) Server. De aanvrager is een agent op het eindpunt dat de referenties levert wanneer deze voor netwerktoegang worden uitgedaagd. Authenticator of NAS (Network Access Server) is de toegangslaag, die bestaat uit netwerk switches en WLC's die de referenties naar de AAA-server dragen. Verificatieserver valideert de aanvraag voor gebruikersverificatie tegen een ID-opslag en autoriseert met een toegangsgoedkeuring of een toegangswegiging. De ID-opslag kan zich bevinden op de AAA-server of op een externe speciale server.

Deze afbeelding toont de Basic IBN Elements.



RADIUS is een op User Datagram Protocol (UDP) gebaseerd protocol waarin verificatie en autorisatie aan elkaar zijn gekoppeld. In Cisco's IBN-oplossing voor ondernemingscampus fungeert de Policy Service Node (PSN) van ISE als de AAA-server die de endpoints authenticceert tegen de Enterprise ID Store en op basis van een voorwaarde autoriseert.

In Cisco ISE worden verificatie- en autorisatiebeleid geconfigureerd om aan deze vereisten te voldoen. Het verificatiebeleid bestaat uit het type media, zowel bekabeld als draadloos, en de EAP-protocollen voor gebruikersvalidatie. Het beleid van de vergunning bestaat uit voorwaarden die de criteria voor de diverse aan te passen eindpunten en het resultaat van de netwerktoegang bepalen dat VLAN of een downloadbare ACL of een Veilige Markering van de Groep kan zijn (SGT). Dit zijn maximale schaalnummers voor beleid waarmee ISE kan worden geconfigureerd.

Deze tabel toont de schaal van Cisco ISE-beleid.

Kenmerk	Schaalnummer
Maximum aantal verificatieregels	1000 (Beleidssetmodus)
Maximum aantal regels voor autorisatie	3.000 (Beleidssetmodus) met 3200 Authz profielen

Technologische trends

Segmentatie is een van de belangrijkste beveiligingselementen geworden voor de huidige bedrijfsnetwerken, zonder dat er behoefte is aan een echt edge-netwerk. De eindpunten mogen tussen interne en externe netwerken zwerven. De segmentering helpt om elke security aanval op een bepaald segment te beperken om zich over het netwerk uit te breiden. De oplossing van vandaag voor softwaregedefinieerde toegang (SDA) met behulp van Cisco ISE-TrustSec biedt een manier om te segmenteren op basis van het bedrijfsmodel van de klant om afhankelijkheid van netwerkelementen zoals VLAN's of IP-subnetten te voorkomen.

Probleem

ISE-beleidsconfiguratie voor grootschalige ondernemingsnetwerken met meer dan 500 verschillende endpointprofielen kan het aantal autorisatiebeleid toenemen tot een niet te beheren punt. Zelfs als Cisco ISE speciale autorisatievoorwaarden ondersteunt om zo'n groot aantal gebruikersprofielen te verwerken, is er een uitdaging om die vele beleidsnummers van beheerders te beheren.

Bovendien kunnen klanten een gemeenschappelijk autorisatiebeleid nodig hebben in plaats van een specifiek beleid om overheadkosten voor beheer te vermijden en bovendien gedifferentieerde netwerktoegang voor endpoints te hebben op basis van hun criteria.

Neem bijvoorbeeld een ondernemingsnetwerk met Active Directory (AD) als **bron van waarheid** en de unieke differentiator van het eindpunt is een van de kenmerken in AD. In een dergelijk geval heeft de traditionele manier van beleidsconfiguratie meer autorisatiebeleid voor elk uniek endpointprofiel.

In deze methode wordt elk eindpuntprofiel onderscheiden met een AD-kenmerk onder domain.com. Daarom moet er een speciaal vergunningsbeleid worden opgesteld.

Deze tabel toont het Traditionele AuthZ-beleid.

	Als AnyConnect gelijk is aan gebruiker en machine-beide doorgegeven
ABC-beleid	EN Als AD-groep gelijk is aan domain.com/groups/ABC DAN SGT:C2S-ABC EN VLAN:1021

Als AnyConnect gelijk is aan gebruiker en machine-beide doorgegeven
 EN
 DEF-beleid Als AD-groep gelijk is aan domain.com/groups/DEF
 DAN
 SGT:C2S-DEF EN VLAN:1022
 Als AnyConnect gelijk is aan gebruiker en machine-beide doorgegeven
 EN
 GHI-beleid Als AD-groep gelijk is aan domain.com/groups/GHI
 DAN
 SGT:C2S-GHI EN VLAN:1023
 Als AnyConnect gelijk is aan gebruiker en machine-beide doorgegeven
 EN
 XYZ-Policy Als AD-groep gelijk is aan domain.com/groups/XYZ
 DAN
 SGT:C2S-XYZ EN VLAN:1024

Voorgestelde oplossing

Om de inbreuk op het maximaal schaalbare aantal ondersteunde autorisatiebeleid op Cisco ISE te omzeilen, wordt voorgesteld een externe DB te gebruiken die elk eindpunt autoriseert en het autorisatieresultaat uit de eigenschappen haalt. Als AD bijvoorbeeld wordt gebruikt als externe DB voor autorisatie, kan naar alle ongebruikte gebruikerskenmerken (zoals Department- of Pincode) worden verwezen om geautoriseerde resultaten te leveren die met SGT of VLAN in kaart zijn gebracht.

Dit wordt bereikt met de integratie van Cisco ISE met een externe DB of binnen de interne DB van ISE geconfigureerd met aangepaste kenmerken. In dit deel wordt de inzet van deze 2 scenario's toegelicht:

Opmerking: In beide opties bevat de DB de **gebruikers-id** maar niet het **wachtwoord** van de DOT1X-eindpunten. De DB wordt alleen als **autorisatiepunt** gebruikt. Verificatie kan nog steeds de ID-opslag van de klant zijn, die in de meeste gevallen zich op de Active Directory (AD)-server bevindt.

Configuratie met externe DB

Cisco ISE is geïntegreerd met een externe DB voor endpointverificatie van referenties:

Deze tabel toont de gevalideerde externe identiteitsbronnen.

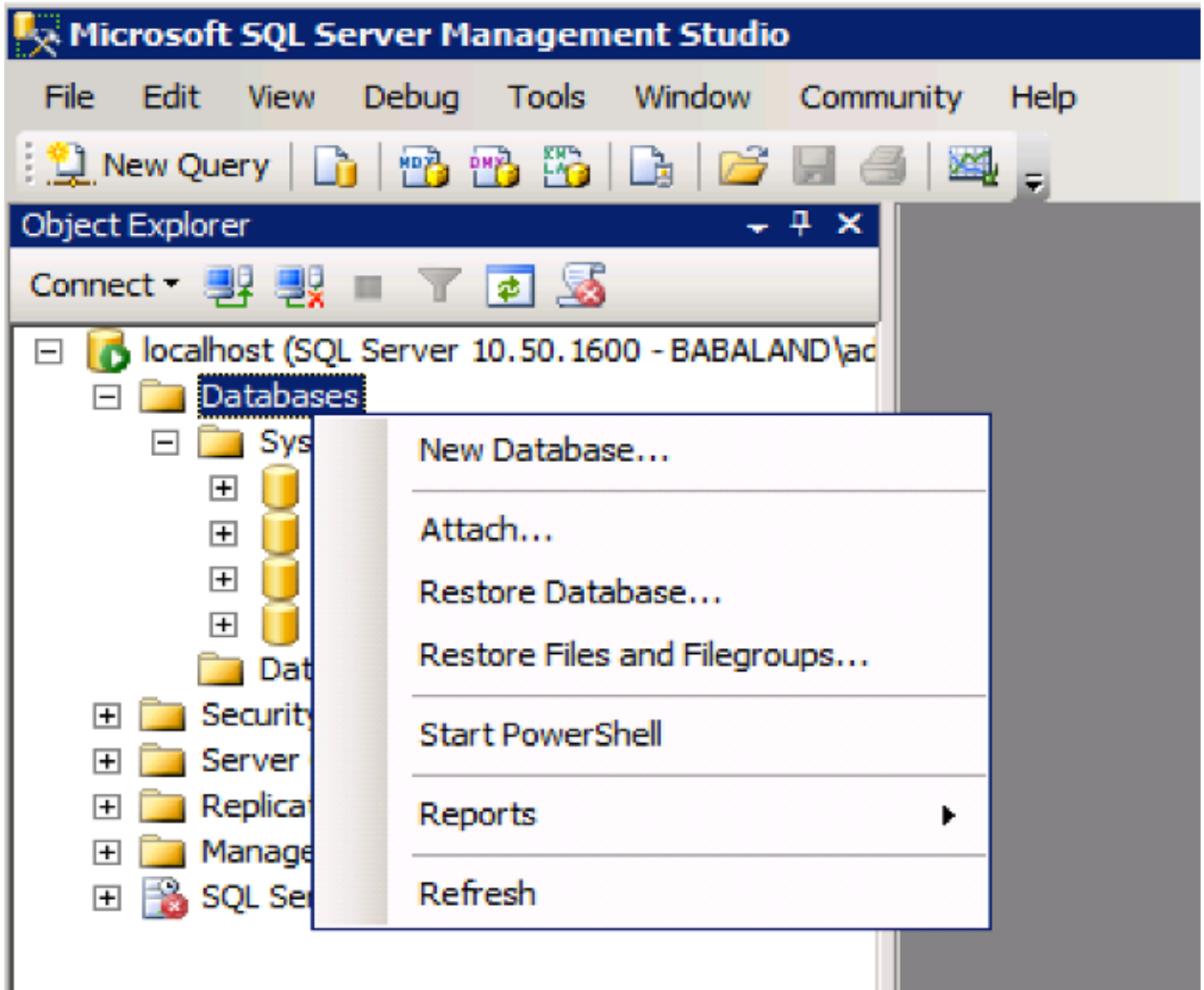
Externe identiteitsbron	IOS/versie
Active Directory	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—
Microsoft Windows Active Directory 2008 R2	—
Microsoft Windows Active Directory 2012	—
Microsoft Windows Active Directory 2012 R2	—
Microsoft Windows Active Directory 2016	—
LDAP-servers	
SunONE LDAP-adressserver	Versie 5.2

OpenLDAP-adressserver	Versie 2.4.23
Alle LDAP v3-conforme servers	—
Token servers	
RSA ACE/server	6.x reeks
RSA-verificatiebeheer	7.x en 8.x reeks
Elke RADIUS RFC 2865-conforme token server	—
Security Assertion Markup Language (SAML) single-aanmelding (SSO)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Versie 11.1.2.2.0
Oracle Identity Federation (OIF)	Versie 11.1.2.0
PingFederate Server	Versie 6.10.0.4
PingOne-cloud	—
Beveiligde autorisatie	8.1.1
Any SAMLv2-conforme identiteitsprovider	—
Identiteitsbron voor Open Database Connectiviteit (ODBC)	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Social Login (voor gastgebruikersaccounts)	
Facebook	—

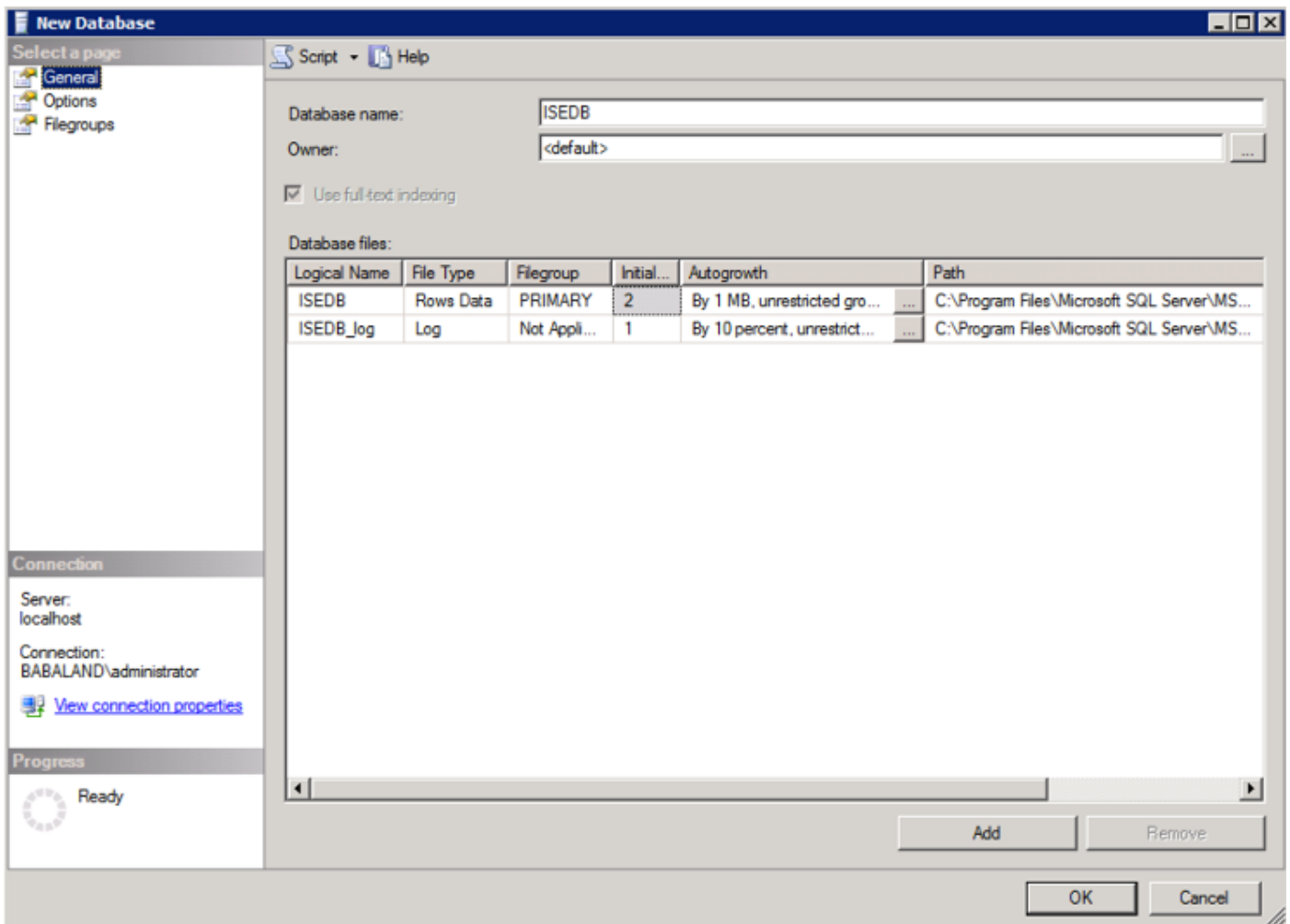
ODBC-voorbeeldconfiguraties

Deze configuratie wordt uitgevoerd op Microsoft SQL om de oplossing te bouwen:

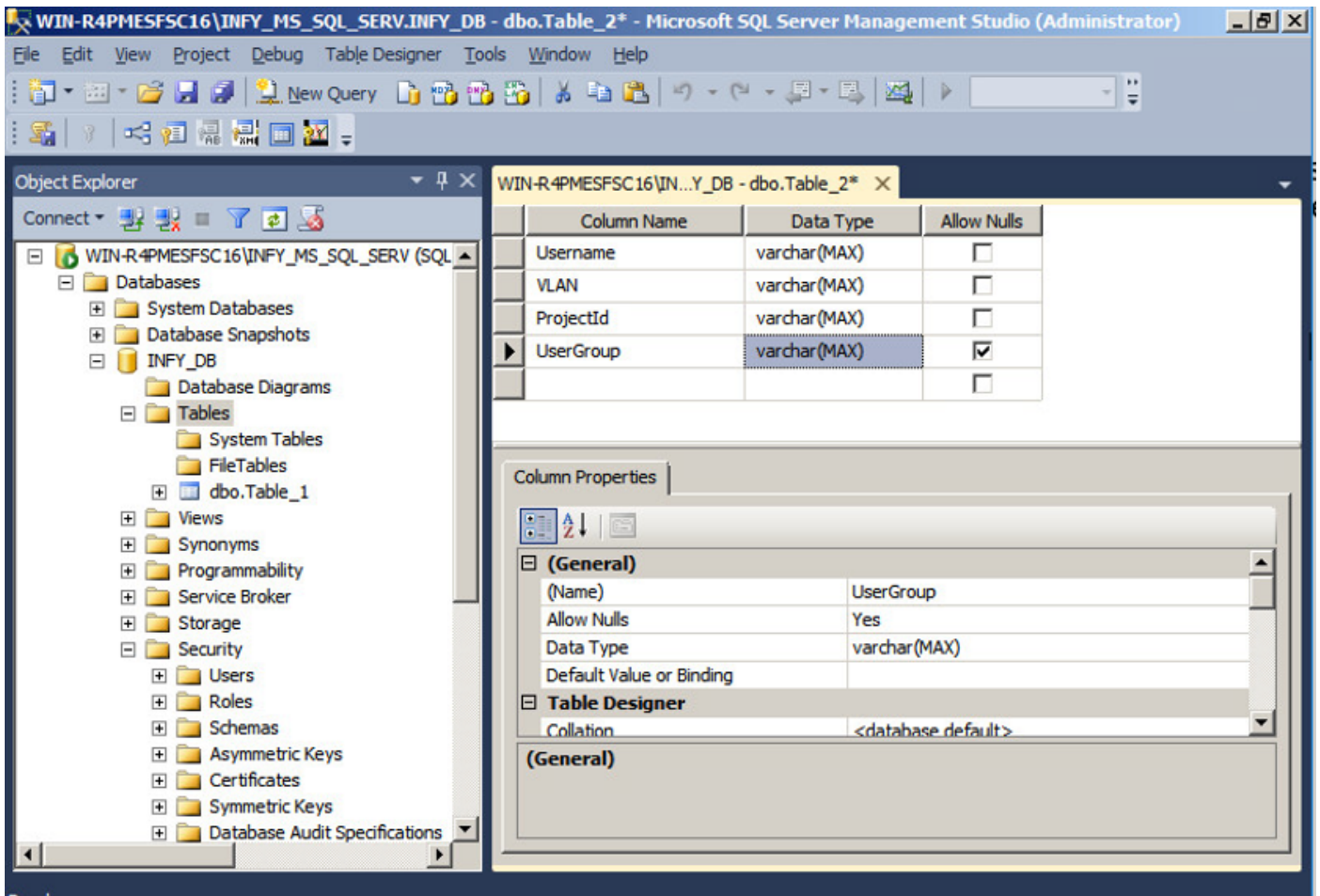
Stap 1. Open SQL Server Management Studio (**Start menu > Microsoft SQL Server**) om een database te maken:



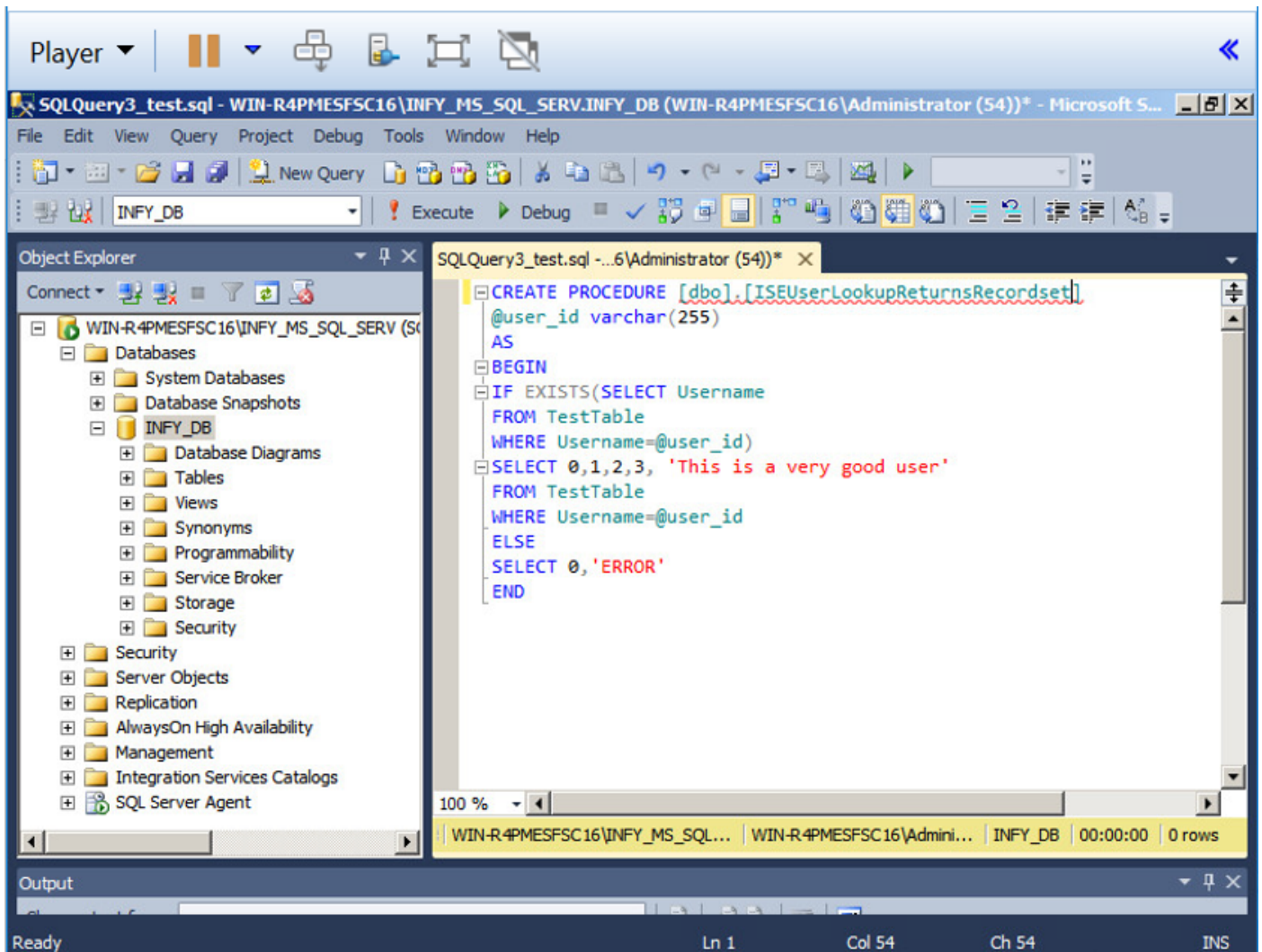
Stap 2. Geef een naam op en maak de database.



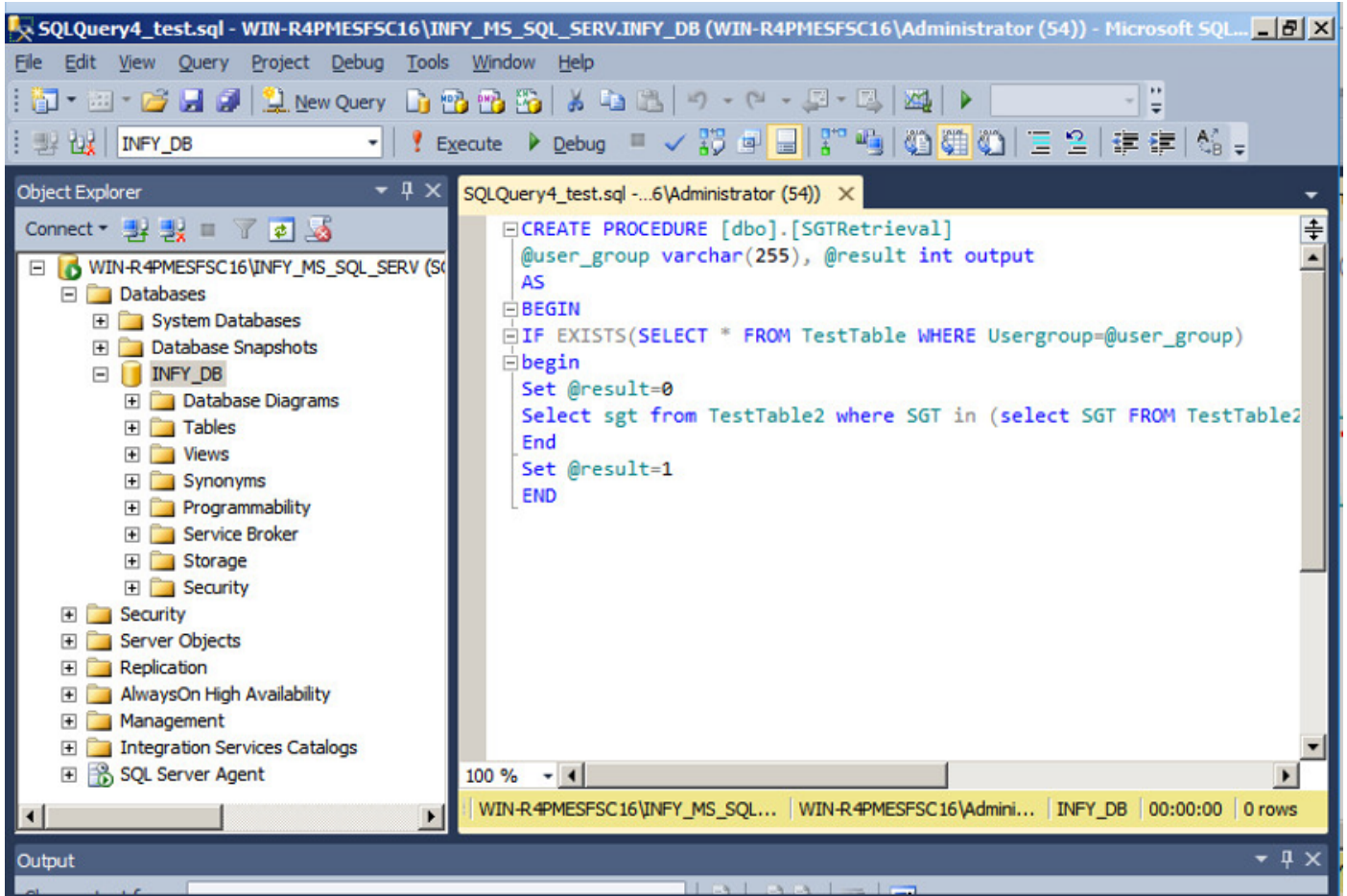
Stap 3. Maak een nieuwe tabel met de vereiste kolommen als parameters voor eindpunten om te worden geautoriseerd.



Stap 4. Maak een **procedure** om te controleren of de gebruikersnaam bestaat.



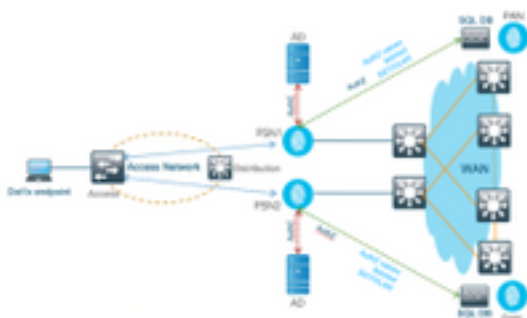
Stap 5. Maak een procedure om kenmerken (SGT) uit de tabel te halen.

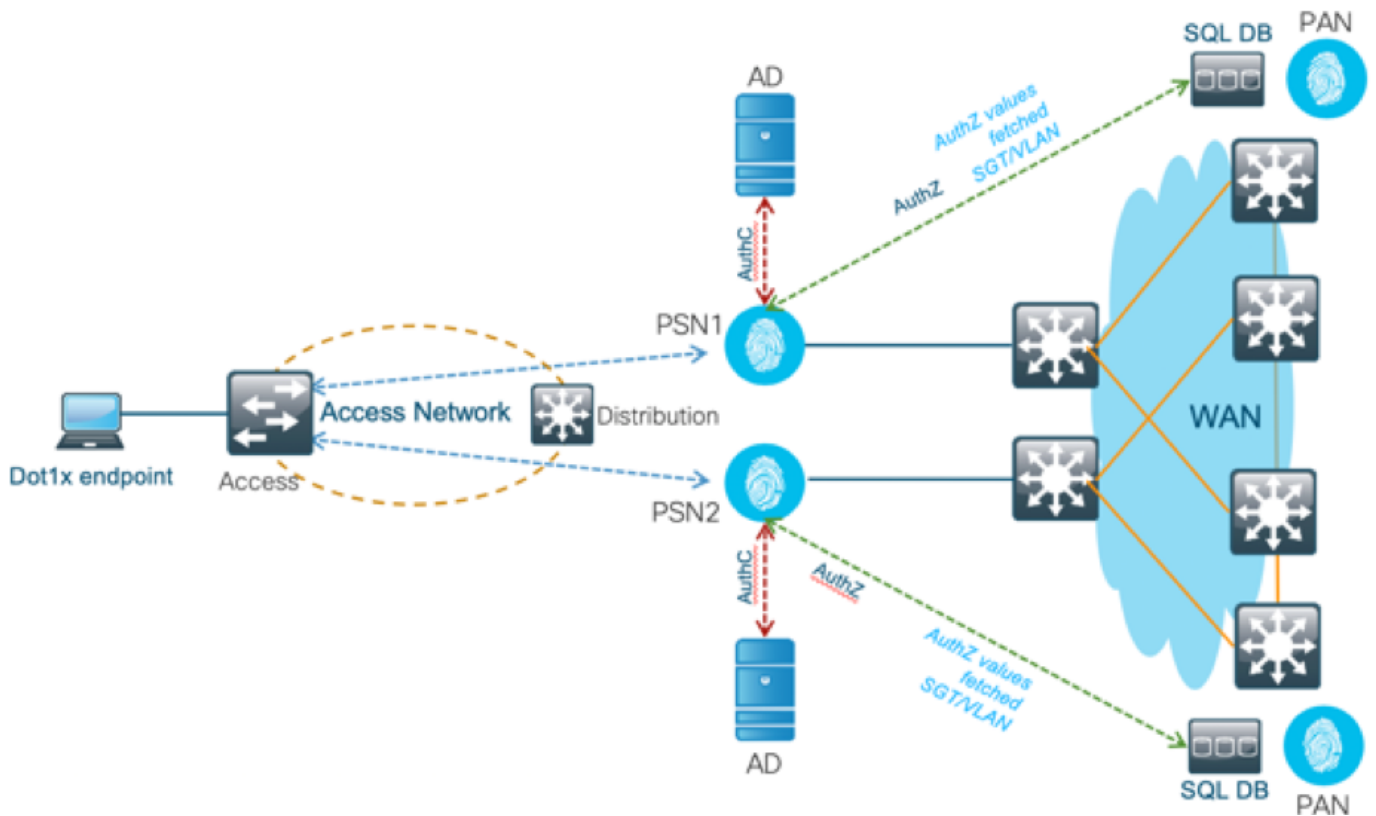


In dit document is Cisco ISE geïntegreerd met Microsoft SQL-oplossing om te voldoen aan de vereisten voor autorisatieschalen op grote ondernemingsnetwerken.

Workflow voor oplossing (ISE 2.7 en eerder)

In deze oplossing is Cisco ISE geïntegreerd met een Active Directory (AD) en Microsoft SQL. AD wordt gebruikt als een verificatie-ID-opslag en MS SQL voor autorisatie. Tijdens het verificatieproces stuurt de Network Access Device (NAD) de gebruikersreferenties naar de PSN - de AAA-server in de IBN-oplossing. PSN valideert de endpointreferenties met de Active Directory ID-opslag en verifieert de gebruiker. Het autorisatiebeleid verwijst naar de MS SQL DB voor het ophalen van de geautoriseerde resultaten zoals SGT / VLAN waarvoor user-id als referentie wordt gebruikt.





Voordelen

Deze oplossing biedt de volgende voordelen:

- Cisco ISE kan gebruikmaken van alle mogelijke extra functies die de externe DB biedt.
- Deze oplossing is niet afhankelijk van enige Cisco ISE-schaallimieten.

Nadelen

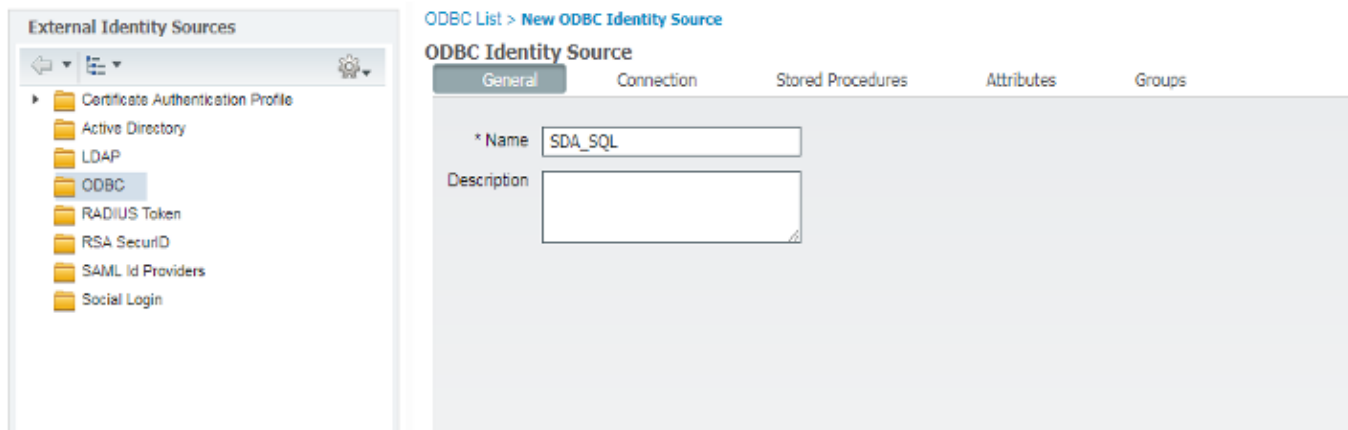
Deze oplossing heeft deze nadelen:

- Vereist extra programmering om de externe DB met endpointreferenties te vullen.
- Als de externe DB niet lokaal aanwezig is zoals PSN's, is deze oplossing afhankelijk van WAN, waardoor het het 3^e punt van mislukking in de AAA-gegevensstroom.
- Vereist extra kennis om externe DB processen en procedures te onderhouden.
- Er moet rekening worden gehouden met fouten die zijn veroorzaakt door de handmatige configuratie van gebruikers-id naar DB.

Externe DB-voorbeeldconfiguraties

In dit document wordt Microsoft SQL weergegeven als de externe DB die als autorisatiepunt wordt gebruikt.

Stap 1. Maak een ODBC Identity Store in Cisco ISE aan vanuit het menu **Beheer > Externe Identity Source > ODBC** en test de verbindingen.



ODBC List > ISE_ODBC

ODBC Identity Source

General Connection Stored Procedures Attributes Groups

ODBC DB connection details

* Hostname/IP[:port]: bast-ad-ca.cisco.com

* Database name: ISEDB

Admin username: ISEDBUser

Admin password:

* Timeout: 5

* Retries: 1

* Database type: Microsoft SQL Serv

Test Connection

Test connection

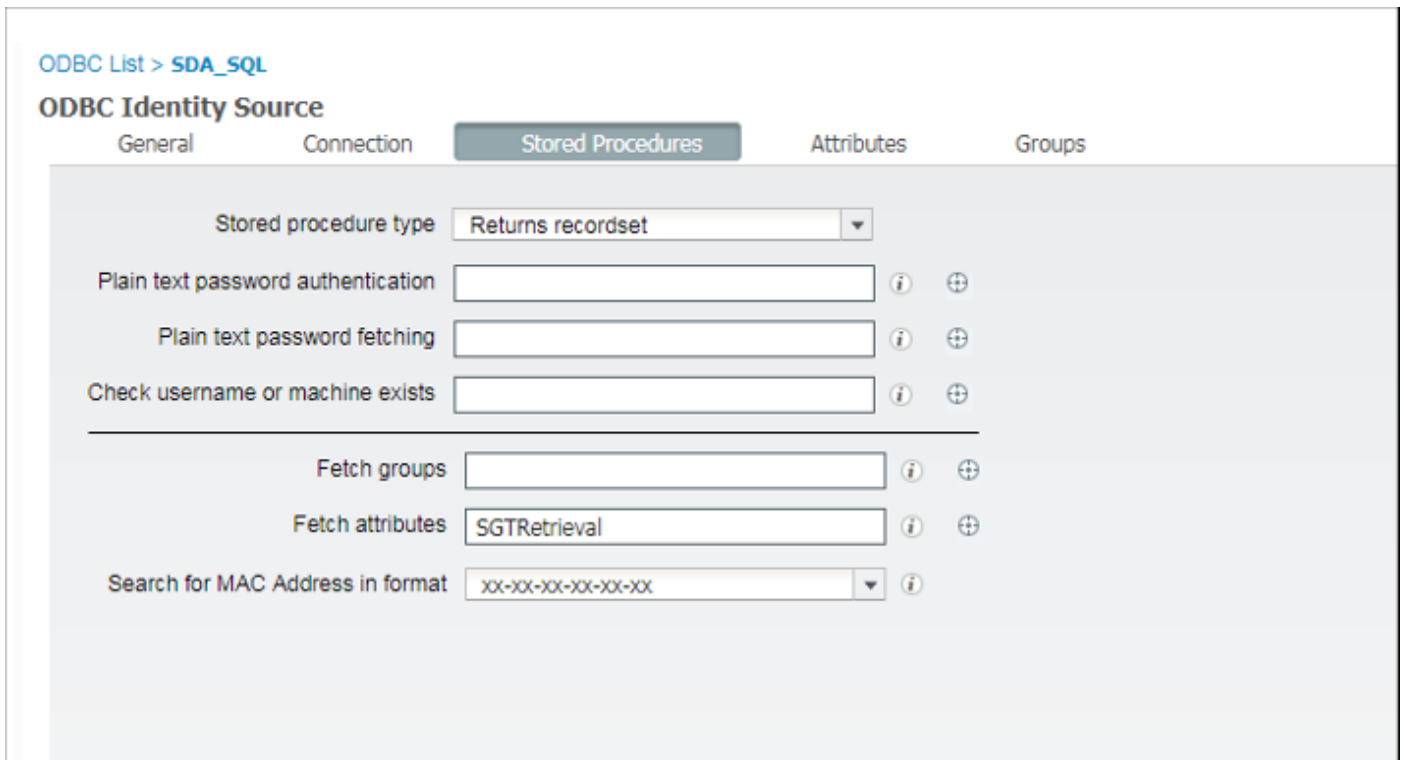
Connection succeeded

Stored Procedures

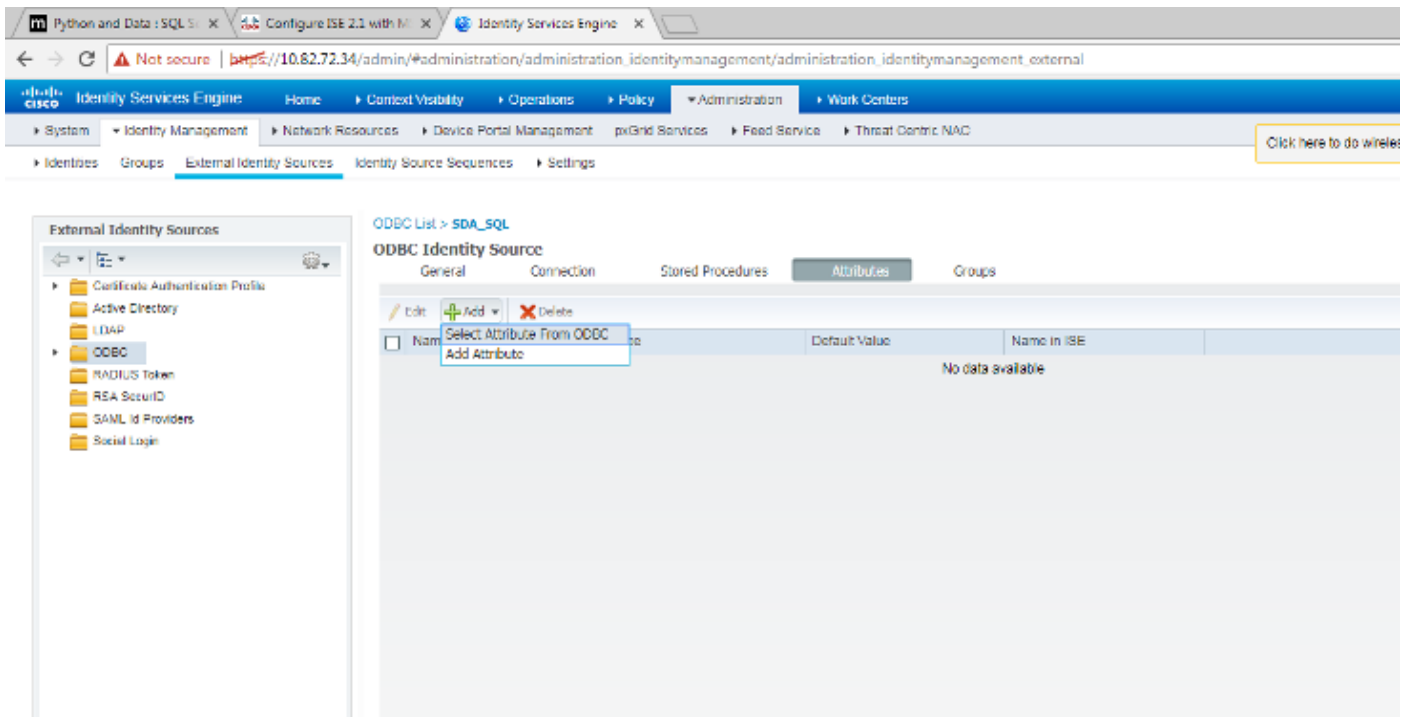
- Plain text password authentication - Not Configured
- Plain text password fetching - Not Configured
- Check username or machine exists - Not Configured
- Fetch groups - Not Configured
- Fetch attributes - Not Configured

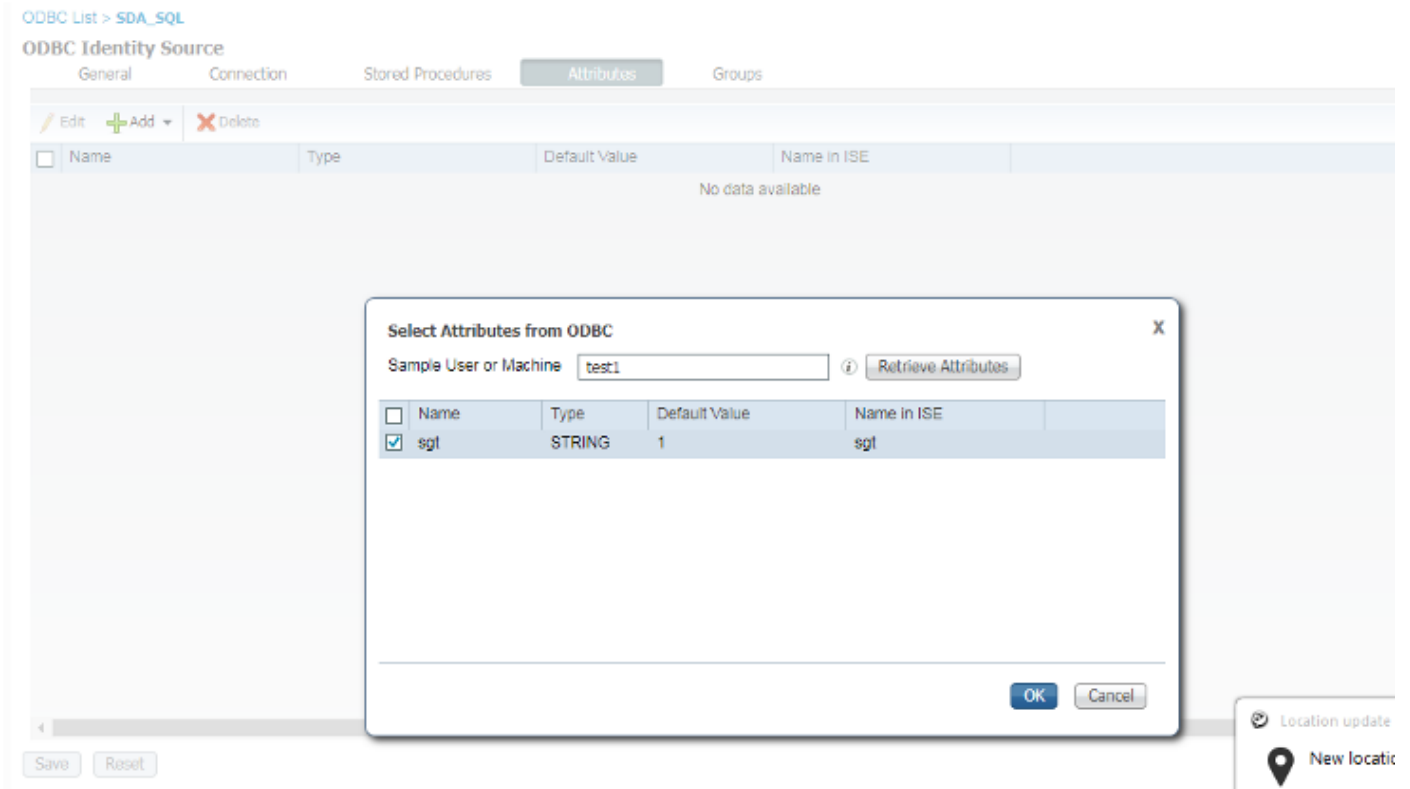
Close

Step 2. Navigeer naar het tabblad Opgeslagen procedures op de ODBC-pagina om de gemaakte procedures in Cisco ISE te configureren.

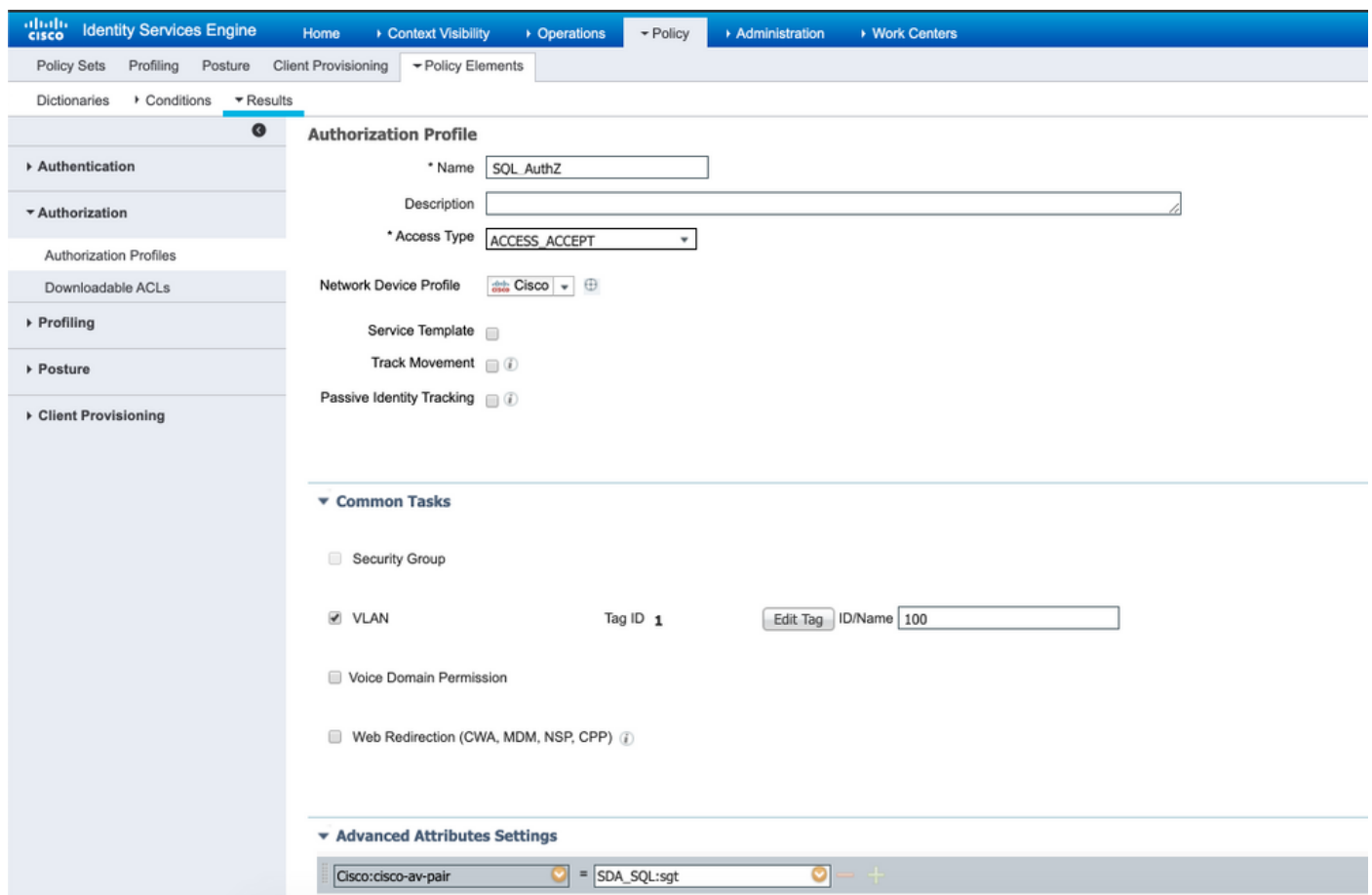


Stap 3. Haal de kenmerken voor de gebruikers-id uit de ODBC-ID-bron voor verificatie.

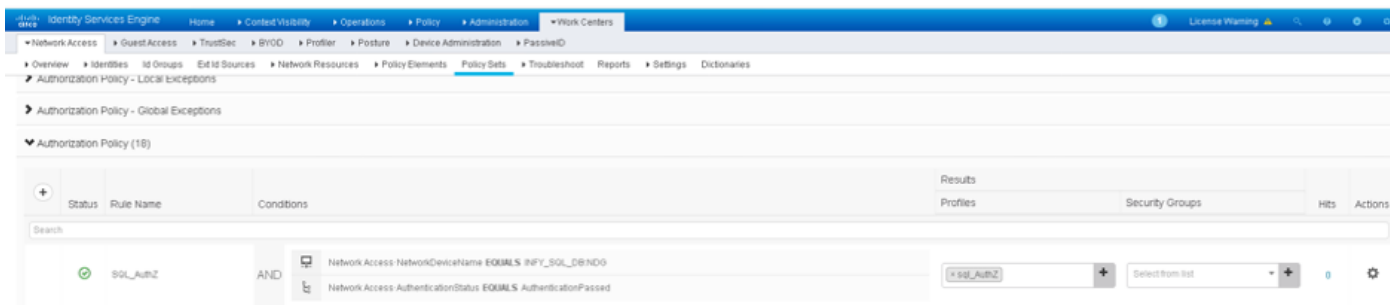




Stap 4. Maak een **autorisatieprofiel** en configureer het. In Cisco ISE gaat u naar **Policy > Results > Autorisatieprofiel > Advanced Attributes Settings** en selecteert u het kenmerk als **Cisco:cisco-av-pair**. Selecteer de waarden als <naam van ODBC-database>:sgt en sla deze vervolgens op.



Stap 5. Maak een **autorisatiebeleid** en configureer het. In Cisco ISE, navigeer naar **Policy > Policy sets > Authorisation Policy > Add**. Zet de voorwaarde als Identity Source is de SQL server. Selecteer het profiel Resultaat als het profiel Autorisatie dat eerder is gemaakt.



Stap 6. Zodra de gebruiker is geauthenticeerd en geautoriseerd, bevatten de logbestanden het aan de gebruiker toegewezen zicht, ter verificatie.

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

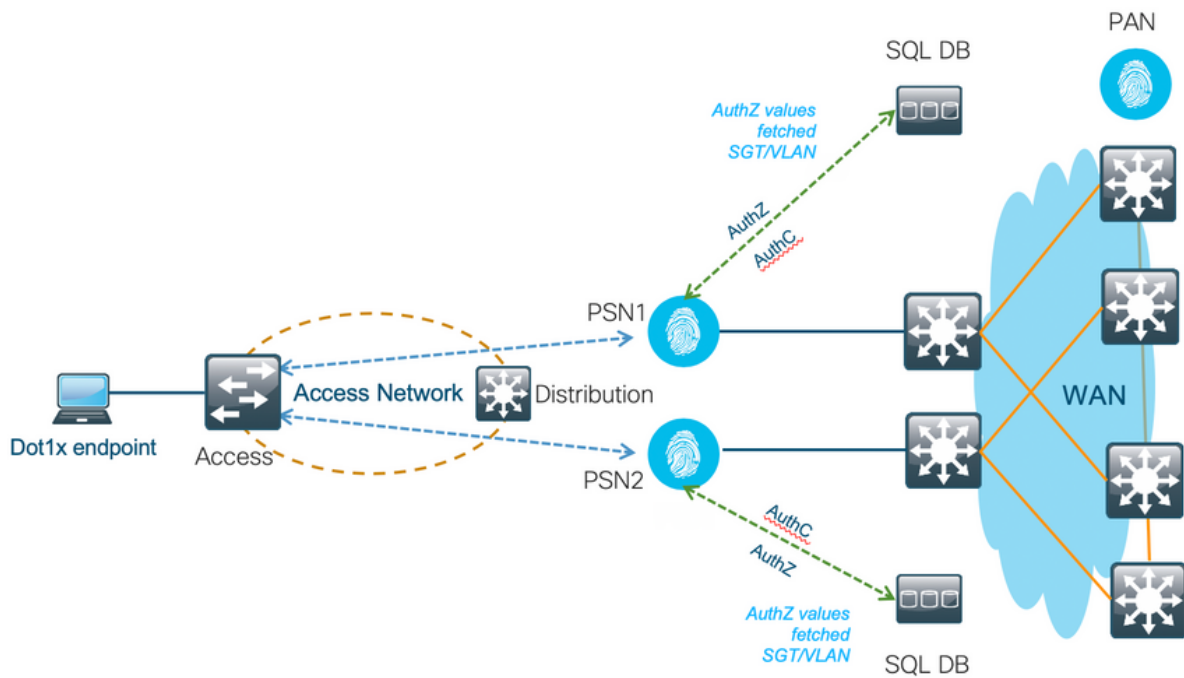
2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

Workflow voor oplossing (na ISE 2.7)

Post ISE 2.7, kenmerken van autorisatie kunnen worden gehaald van ODBC zoals VLAN, SGT, ACL en deze eigenschappen kunnen worden verbruikt in beleid.

In deze oplossing is Cisco ISE geïntegreerd met Microsoft SQL. MS SQL wordt gebruikt als een ID-opslag voor verificatie en voor autorisatie. Wanneer de referenties van eindpunten aan PSN worden verstrekt, valideert het de referenties tegen de MS SQL DB. Het autorisatiebeleid verwijst

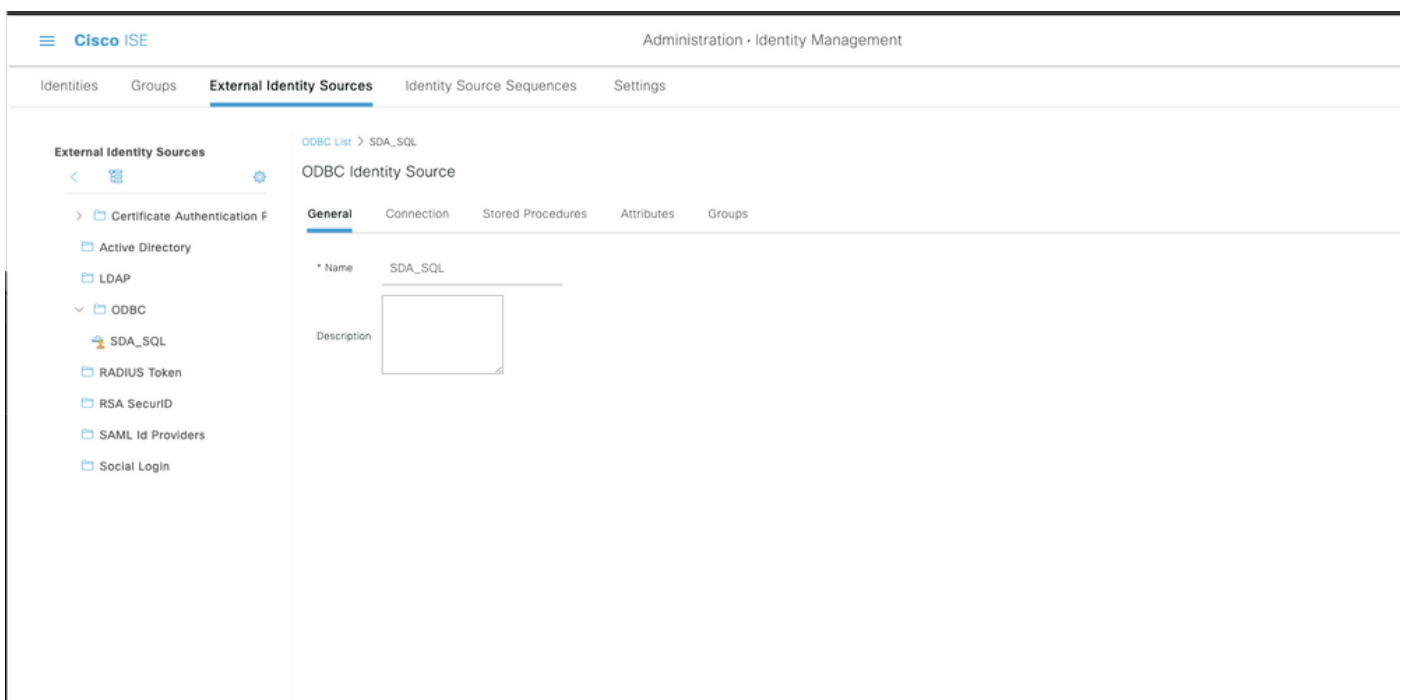
naar de MS SQL DB voor het ophalen van de geautoriseerde resultaten zoals SGT / VLAN waarvoor **user-id** als referentie wordt gebruikt.



Externe DB-voorbeeldconfiguraties

Volg de procedure die eerder in dit document is opgegeven om MS SQL DB samen met Gebruikersnaam, Wachtwoord, VLAN-id en SGT te maken.

Stap 1. Maak een ODBC Identity Store in Cisco ISE aan vanuit het menu **Beheer > Externe Identity Source > ODBC** en test de verbindingen.



Stap 2. Navigeer naar het tabblad Opgeslagen procedures op de ODBC-pagina om de gemaakte procedures in Cisco ISE te configureren.

Cisco ISE Administration - Identity Management

External Identity Sources > ODBC List > SDA_SQL

ODBC Identity Source

General Connection **Stored Procedures** Attributes Groups

Stored procedure type Returns recordset

Plain text password authentication ISEAuthUser ⓘ ⓘ

Plain text password fetching ISEFetchPassword ⓘ ⓘ

Check username or machine exists ⓘ ⓘ

Fetch groups ISEGroups ⓘ ⓘ

Fetch attributes ⓘ ⓘ [Advanced Settings](#) ⓘ

Search for MAC Address in format xx-xx-xx-xx-xx-xx ⓘ

Stap 3. Haal de kenmerken voor de gebruikers-id uit de ODBC-ID-bron voor verificatie.

Cisco ISE Administration - Identity Management

External Identity Sources > ODBC List > SDA_SQL

ODBC Identity Source

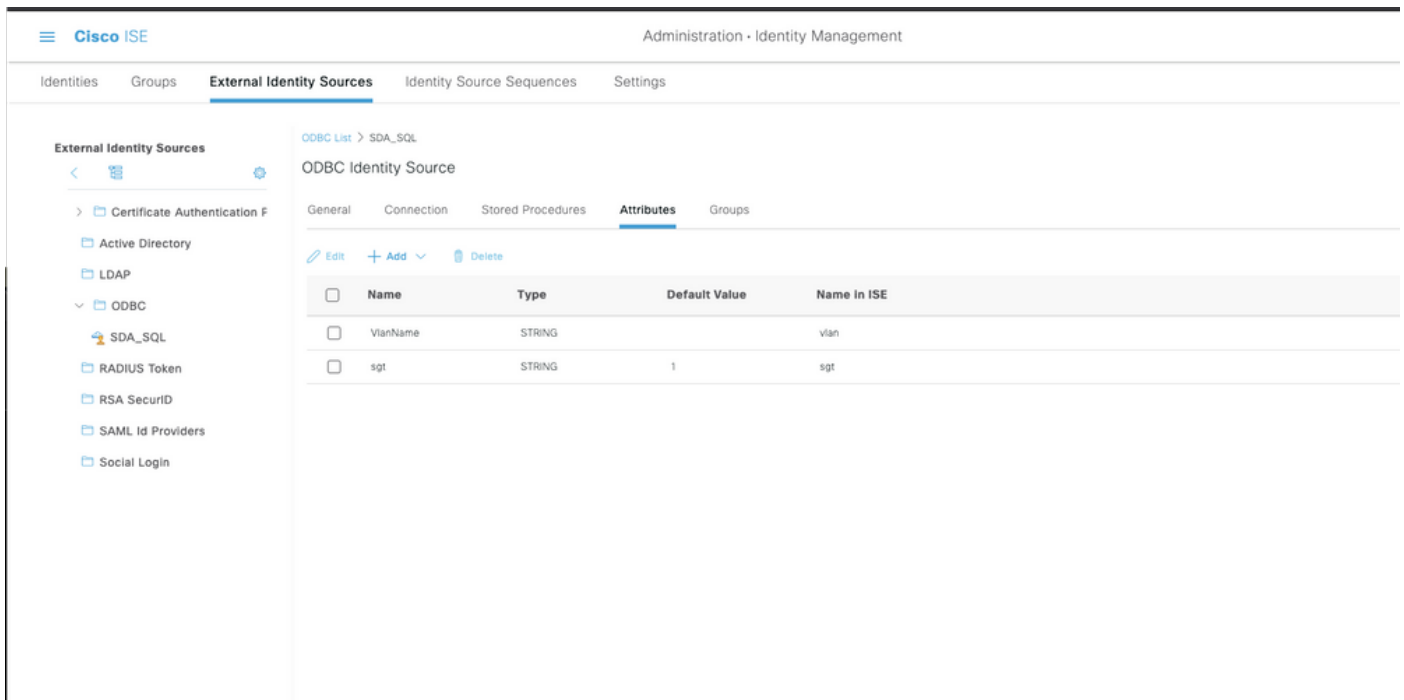
General Connection Stored Procedures **Attributes** Groups

[Edit](#) [+ Add](#) [Delete](#)

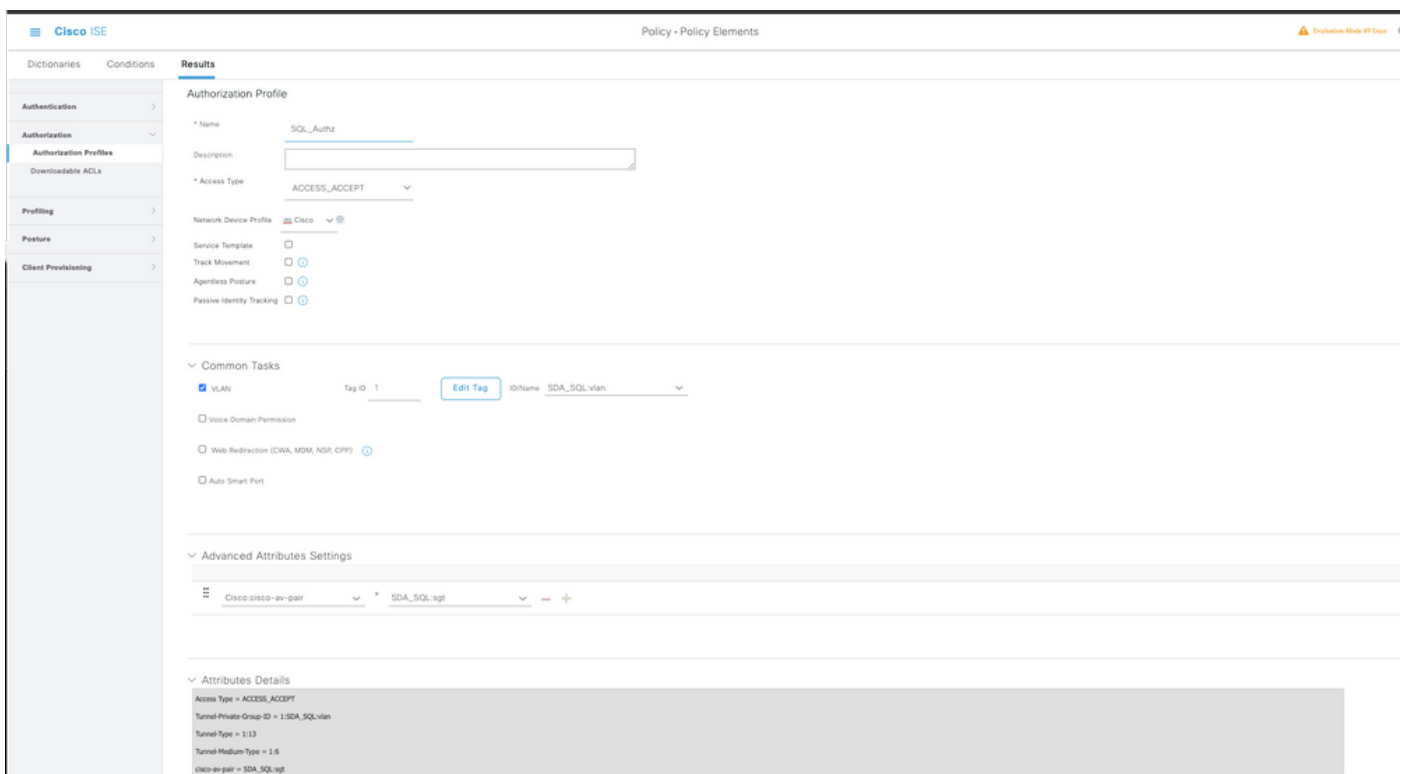
	Default Value	Name in ISE
No data available		

Select Attributes from ODBC

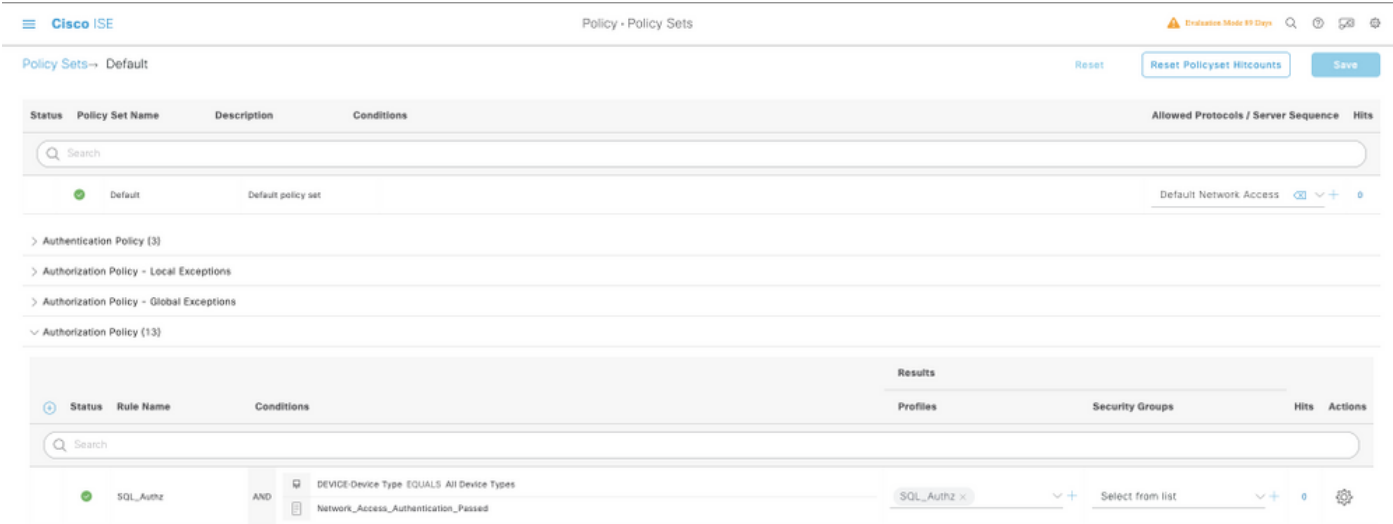
Add Attribute



Stap 4. Maak een **autorisatieprofiel** en configureer het. In Cisco ISE gaat u naar **Policy > Results > Authorisation profile > Advanced Attributes Settings** en selecteert u het kenmerk als **Cisco:cisco-av-pair**. Selecteer de waarden als <naam van ODBC-database>:sgt. Selecteer onder Common Tasks de optie **VLAN** met id/name als <naam van ODBC-database>:VLAN en sla het op



Stap 5. Maak een **autorisatiebeleid** en configureer het. In Cisco ISE, navigeer naar **Policy > Policy sets > Authorisation Policy > Add**. Zet de voorwaarde als Identity Source is de SQL server. Selecteer het profiel Resultaat als het profiel Autorisatie dat eerder is gemaakt.

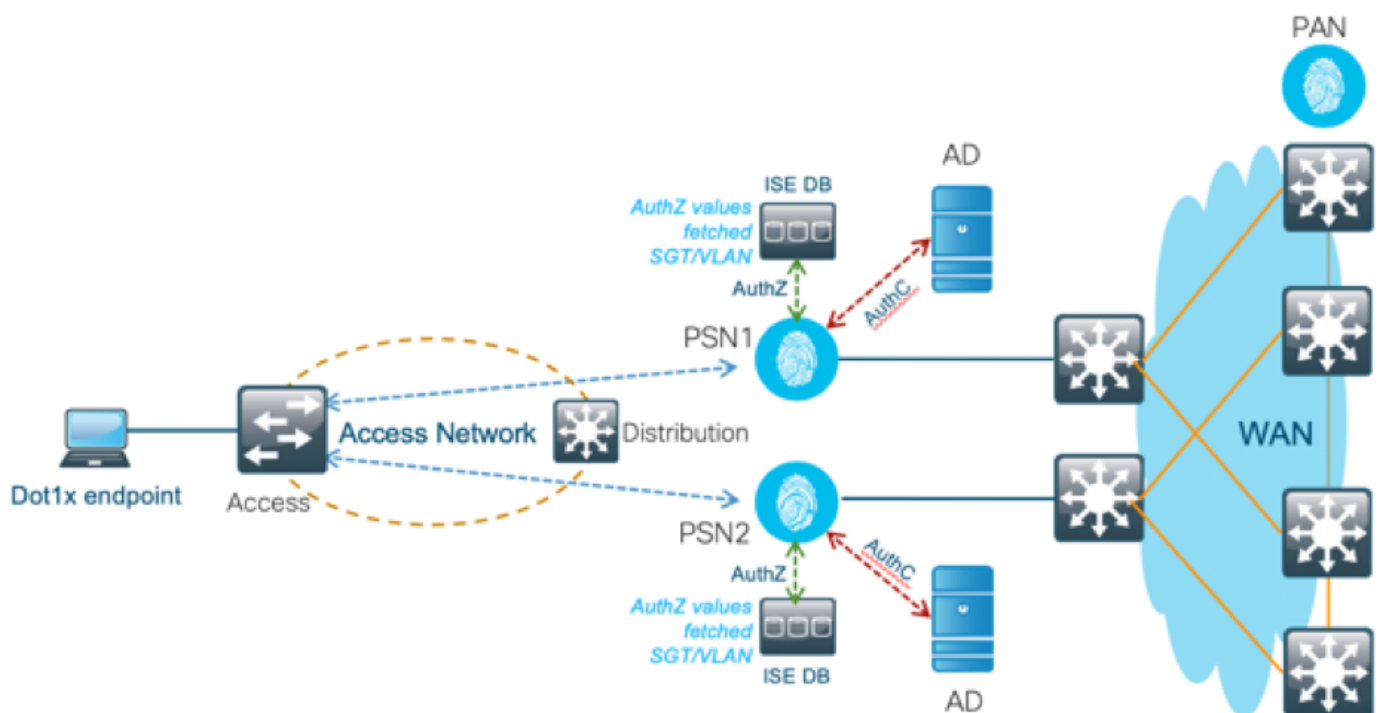


Interne DB gebruiken

Cisco ISE zelf heeft een ingebouwde DB die kan worden gebruikt om gebruikers-id's voor autorisatie te hebben.

Workflow voor oplossing

In deze oplossing wordt de interne DB van Cisco ISE gebruikt als autorisatiepunt terwijl Active Directory (AD) de verificatiebron blijft. Gebruiker-ID van eindpunten is opgenomen in Cisco ISE-database samen met **aangepaste kenmerken** die de geautoriseerde resultaten zoals SGT of VLAN ophalen. Wanneer de referenties van eindpunten aan PSN worden verstrekt, controleert het de geldigheid van de endpoints' referenties met de Active Directory ID-opslag en verifieert het eindpunt. Het autorisatiebeleid verwijst naar de ISE-database om de geautoriseerde resultaten te halen, zoals SGT / VLAN, waarvoor de user-id als referentie wordt gebruikt.



Voordelen

Deze oplossing biedt de volgende voordelen, waardoor het een flexibele oplossing is:

- Cisco ISE DB is een ingebouwde oplossing en heeft daarom geen 3^e punt van mislukking, in tegenstelling tot de externe DB-oplossing.
- Aangezien het Cisco ISE-cluster zorgt voor real-time synchronisatie tussen alle personen, is er geen WAN-afhankelijkheid omdat het PSN alle gebruikers-id's en aangepaste kenmerken heeft die in real-time van PAN worden gedrukt.
- Cisco ISE kan gebruikmaken van alle mogelijke extra functies die de externe DB biedt.
- Deze oplossing is niet afhankelijk van enige Cisco ISE-schaallimieten.

Nadelen

Deze oplossing heeft deze nadelen:

- Het maximale aantal gebruikers-id's dat Cisco ISE DB kan inhouden is 300.000.
- Er moet rekening worden gehouden met fouten die zijn veroorzaakt door de handmatige configuratie van gebruikers-id naar DB.

Interne DB-voorbeeldconfiguraties

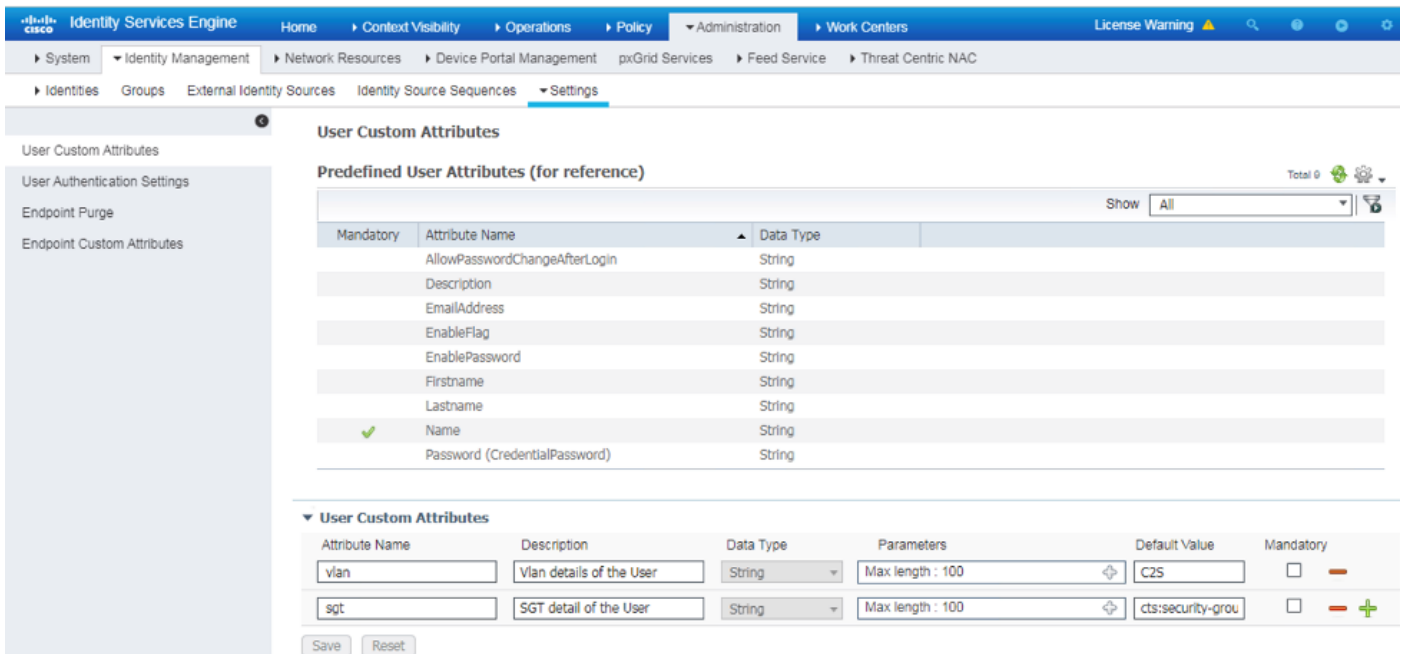
Per-gebruiker VLAN & SGT kan worden geconfigureerd voor elke gebruiker in de interne ID-winkel met een aangepast gebruikerskenmerk.

Stap 1. Maak nieuwe aangepaste gebruikerskenmerken om de VLAN- en SGT-waarde van de respectieve gebruikers weer te geven. Navigeer naar **Beheer > Identity Management > Instellingen > Aangepaste gebruikerskenmerken**. Maak nieuwe aangepaste gebruikerskenmerken zoals in deze tabel.

Hier wordt de ISE DB-tabel weergegeven met Aangepaste kenmerken.

Naam kenmerk	Gegevenstype	Parameters (lengte)	Standaardwaarde
vlan	String	100	C2S (standaard VLAN-naam)
sekte	String	100	cts:security-group-tag=0003-0 (standaard SGT-waarde)

- In dit scenario vertegenwoordigt de VLAN-waarde de VLAN-naam en de SGT-waarde het cisco-av-paar attribuut van SGT in Hex.



Stap 2. Maak een autorisatieprofiel met aangepaste gebruikerskenmerken om de VLAN- en sgt-waarden van de respectieve gebruikers te impliceren. Navigeer naar **Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen > Toevoegen**. Voeg de onderstaande kenmerken toe onder Geavanceerde attributeninstellingen.

Deze tabel toont het AuthZ-profiel voor interne gebruiker.

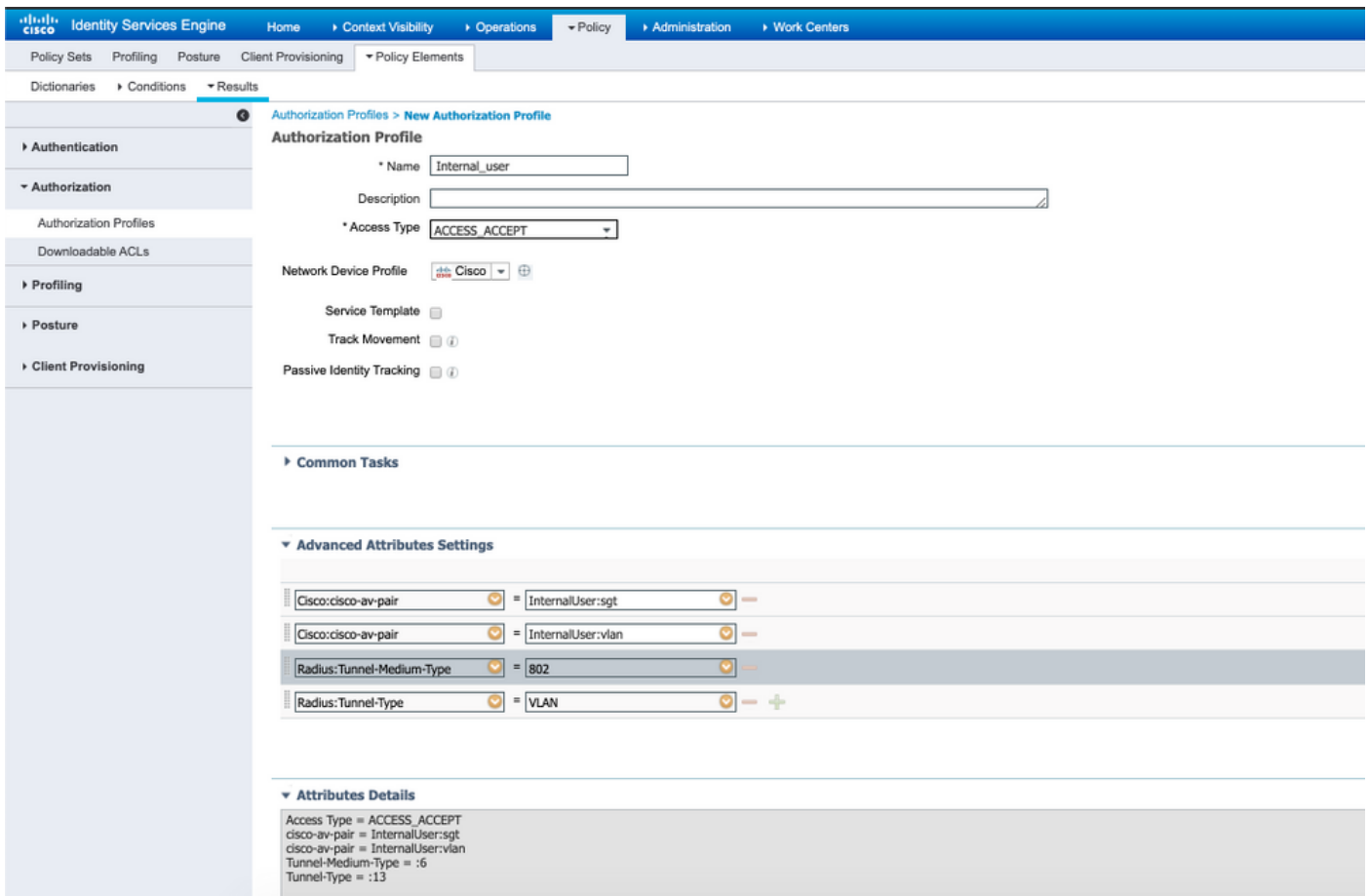
Kenmerk

Cisco 1500:cisco-av-paar
 RADIUS:Tunnel-Private-Group-ID
 Straal:Tunnel-gemiddeld-type
 Straal:tunneltype

Waarde

Interne gebruiker:sgt
 Interne gebruiker:VLAN
 802
 VLAN

Zoals getoond in de afbeelding, wordt voor de interne gebruikers het profiel **Internal_user** geconfigureerd met SGT & VLAN geconfigureerd als **InternalUser:sgt** & **InternalUser:vlan** respectievelijk.



Stap 3. Maak een machtigingsbeleid, Navigeer naar **Beleid > Policy Sets > Policy-1 > Autorisatie**. Maak een machtigingsbeleid met de onderstaande voorwaarden en geef dit aan de respectieve autorisatieprofielen.

Deze tabel toont het AuthZ-beleid voor interne gebruiker.

Regelnaam	Voorwaarde	Profiel resultaatverificatie
Intern_Gebruiker_Auteur	Als Network Access.EapChainingResults gelijk maakt aan gebruiker en machine beide geslaagd	Intern_gebruiker
Alleen machine_Auteur	Als MyAD.ExternalGroups GELIJK is aan gdc.security.com/Users/Domain Computers	Toegangsrechten

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Search

Policy-1

DEVICE Device Type EQUALS All Device Types

Default Network:Access x + 518

Authentication Policy (3)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
	✓	Internal-users Authz	Network:Access-EspChainingResult EQUALS User and machine both succeeded	x Internal_user +	Select from list +	2	⚙️
	✓	Machine Authz	MyAD-ExternalGroups EQUALS gdc.security.com/Users/Domain Computers	x PermitAccess +	Select from list +	2	⚙️
	✓	Default		x DenyAccess +	Select from list +	3	⚙️

Reset Save

Stap 4. Maak bulkgebruikersidentiteiten met aangepaste kenmerken met gebruikersdetails en hun respectieve aangepaste kenmerken in de csv-sjabloon. Importeer de csv door Navigate to **Administration > Identity Management > Identiteiten > Gebruikers > Importeren > Bestand > Importeren**.

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Network Access Users

Selected 0 | Total 5

Edit + Add Change Status Import Export Delete Duplicate Show All

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
✓ Enabled	Aravind					Bangalore	Admin
✓ Enabled	Jinkle					Bangalore	
✓ Enabled	jitchand					Bangalore	
✓ Enabled	Mnason					Chennai	
✓ Enabled	Vinodh					Bangalore,Chennai	

Dit beeld toont een voorbeeldgebruiker met aangepaste attribuutdetails. Selecteer de gebruiker en klik op bewerken om de aangepaste attribuutdetails te bekijken die aan de betreffende gebruiker zijn toegewezen.

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Center

System > Identity Management > Network Resources > Device Portal Management > piGrid Services > Feed Service > Threat Center NAC

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

Network Access Users List > Jinkle

Network Access User

Name: Jinkle

Status: Enabled

Email:

Passwords

Password Type: MyAD

Logn Password: [] [] [Generate Password]

Enable Password: [] [] [Generate Password]

User Information

Account Options

Account Disable Policy

User Custom Attributes

vlan = S25

sgt = ciscosecurity-group-tag=0005-1

User Groups

Bengalore

Save Reset

Stap 5: Controleer de bewegende logs:

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Po...	Authorization Policy	Authorizati...	IP Address
Oct 28, 2019 06:40:05.066 PM	Success		1	hostPOD2-CLIENT1	00:50:56:80:C8:DF	VMWare-Device	Policy-1 >> Dot1x	Policy-1 >> Machine Authz	PermtAccess	172.16.2.1
Oct 28, 2019 06:40:05.048 PM	Success			hostPOD2-CLIENT1	00:50:56:80:C8:DF	VMWare-Device	Policy-1 >> Dot1x	Policy-1 >> Machine Authz	PermtAccess	172.16.2.1

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address	Network Dev
Oct 29, 2019 10:23:33.877 AM	Success		1	araravic.hostPOD...	00:50:56:80:C8:DF	VMWare-De...	Policy-1 >> ...	Policy-1 >> Internal-users Authz	Internal_user	172.16.2.1	
Oct 29, 2019 10:23:33.877 AM	Success			araravic.hostPOD...	00:50:56:80:C8:DF	VMWare-De...	Policy-1 >> ...	Policy-1 >> Internal-users Authz	Internal_user	172.16.2.1	POD2-ACCES

Controleer in het gedeelte **Resultaat** om te controleren of het kenmerk **VLAN & SGT** als deel van **Access-Accept** wordt verzonden.

Result

User-Name	araravic
Class	CACS:AC1002320000E5E815DA26BA:pod2ise8/361122903/4422
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) C2S
EAP-Key-Name	2b:c0:55:87:a3:0a:ac:a1:a2:ee:29:66:6e:b2:0e:b5:26:94:23:5d:75:45:c6:10:e0:8f:d8:bc:bc:e7:b0:71:cc:de:c3:79:c2:85:62:4c:01:04:7e:95:fe:a7:66:0a:8b:7d:f3:8b:4a:b0:e1:c5:9b:bb:e0:c5:73:32:d1:ad:48
cisco-av-pair	cts:security-group-tag=0004-00
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Conclusie

Deze oplossing stelt enkele grote zakelijke klanten in staat om op te schalen naar hun behoeften. Voorzichtigheid is geboden bij het toevoegen of verwijderen van gebruikers-id's. Als fouten worden geactiveerd, kunnen ze leiden tot ongeoorloofde toegang voor echte gebruikers of andersom.

Gerelateerde informatie

Cisco ISE configureren met 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>

Woordenlijst

AAA	Accounting van verificatieautorisatie
AD	Active Directory
AuthC	Verificatie
Automatis ch Z	Authorization
DB	Gegevensbank
DOT1X	802.1X
IBN	Op identiteit gebaseerd netwerk
identiteits bewijs	Identiteitsdatabase
ISE	Identity Services Engine

MnT	Monitoring en probleemoplossing
MSSQL	Microsoft SQL
ODBC	Open DataBase-connectiviteit
PAN	Policy Admin-knooppunt
PSN	Knooppunt voor beleidsservices
SGT	Secure-groepstag
SQL	Gestructureerde zoektaal
VLAN	Virtual LAN
WAN	Wide Area Network

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.