Política de acesso simplificada usando ODBC e ISE DB (atributo personalizado) para rede de campus em larga escala

Contents

Introduction

Este documento descreve a implantação em larga escala do campus sem comprometer seus recursos e a aplicação da segurança. A solução de segurança de endpoint da Cisco, o Identity Services Engine (ISE), atende a esse requisito com integração a uma fonte de identidade externa.

Para redes de grande escala com mais de 50 geolocalizações, mais de 4000 perfis de usuário diferentes e 600.000 terminais ou mais, as soluções IBN tradicionais precisam ser examinadas de uma perspectiva diferente - mais do que apenas recursos, sejam escaláveis com todos os recursos. A solução de rede baseada em intenção (IBN) nas redes tradicionais de grande escala atuais requer foco adicional na escalabilidade e facilidade de gerenciamento, e não apenas em seus recursos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

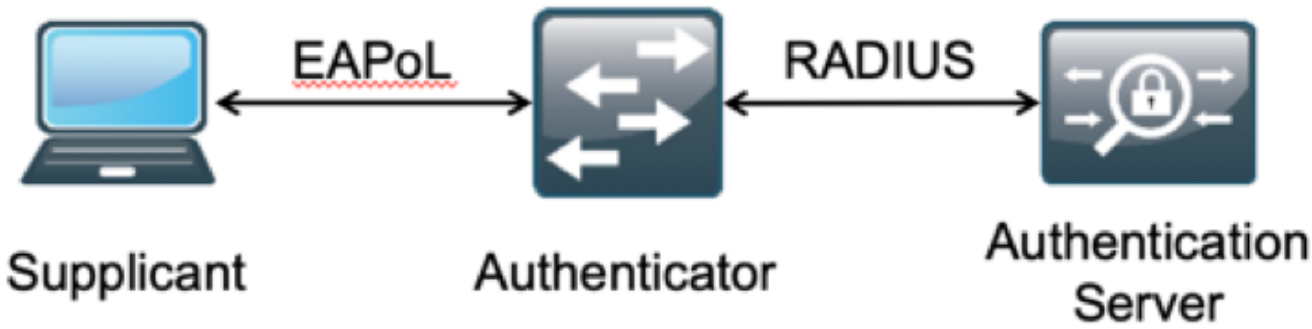
- Cisco Identity Services Engine (ISE) versão 2.6, patch 2 e versão 3.0
- Windows Ative Diretory (AD) Server 2008 versão 2
- Microsoft SQL Server 2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de entender o impacto potencial de qualquer configuração.

Informações de Apoio

Em uma solução de rede baseada em identidade (IBN), os elementos básicos são suplicante, autenticador e servidor de autenticação (AAA). O Requerente é um agente no endpoint que fornece as credenciais quando desafiado para acesso à rede. Authenticator ou NAS (Network Access Server) é a camada de acesso, que compreende switches de rede e WLCs que transportam as credenciais para o servidor AAA. O Servidor de autenticação valida a solicitação de autenticação do usuário em relação a um armazenamento de ID e autoriza com um access-accept ou access-reject. O armazenamento de ID pode estar dentro do servidor AAA ou em um servidor dedicado externo.

Esta imagem mostra os elementos IBN básicos.



O RADIUS é um protocolo baseado no User Datagram Protocol (UDP) com autenticação e autorização combinadas. Na solução IBN da Cisco para campus empresarial, a persona Policy Service Node (PSN) do ISE atua como o servidor AAA que autentica os endpoints em relação ao Enterprise ID Store e autoriza com base em uma condição.

No Cisco ISE, as políticas de autenticação e autorização são configuradas para atender a esses requisitos. As políticas de autenticação consistem no tipo de mídia, com ou sem fio, e nos protocolos EAP para validação do usuário. As políticas de autorização consistem em condições que definem os critérios para que os vários pontos finais correspondam e o resultado de acesso à rede que pode ser uma VLAN, uma ACL para download ou uma SGT (Secure Group Tag, Tag de grupo seguro). Esses são números de escala máxima para políticas com as quais o ISE pode ser configurado.

Esta tabela mostra a Escala de políticas do Cisco ISE.

Atributo	Número da escala
Número máximo de regras de autenticação	1000 (modo de definição de política)
Número máximo de regras de autorização	3.000 (modo de definição de política) com perfis 3200 Authz

Tendências em tecnologia

A segmentação tornou-se um dos principais elementos de segurança das redes corporativas atuais sem a necessidade de uma rede edge real. Os endpoints têm permissão para fazer roaming entre redes internas e externas. A segmentação ajuda a conter qualquer ataque à segurança em um segmento específico para se estender pela rede. A solução atual de acesso definido por software (SDA) com a ajuda do TrustSec do Cisco ISE oferece uma maneira de segmentar com base no modelo de negócios do cliente para evitar dependências em elementos de rede, como VLANs ou sub-redes IP.

Problema

Configuração de política do ISE para redes corporativas de grande escala com mais de 500 perfis de endpoint diferentes, o número de políticas de autorização pode aumentar até um ponto não gerenciável. Mesmo que o Cisco ISE ofereça suporte a condições de autorização dedicadas para atender a esse volume de perfis de usuário, existe um desafio para gerenciar esses vários números de políticas por administradores.

Além disso, os clientes podem exigir políticas de autorização comuns em vez de políticas dedicadas para evitar sobrecargas de gerenciamento e também ter acesso diferenciado à rede para terminais com base em seus critérios.

Por exemplo, considere uma rede corporativa com Ative Diretory (AD) como a **fonte da verdade** e o diferenciador exclusivo do endpoint é um dos atributos no AD. Nesse caso, a forma tradicional de configuração de política tem mais políticas de autorização para cada perfil de endpoint exclusivo.

Neste método, cada perfil de endpoint é diferenciado com um atributo do AD em domain.com. Portanto, uma política de autorização dedicada precisa ser configurada.

Esta tabela mostra as políticas de AuthZ tradicionais.

Política ABC	Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed E

DEF-Policy	Se AD-Group FOR IGUAL A domain.com/groups/ABC EM SEGUIDA SGT:C2S-ABC E VLAN:1021 Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed E Se AD-Group FOR IGUAL A domain.com/groups/DEF EM SEGUIDA SGT:C2S-DEF E VLAN:1022
Política GHI	Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed E Se AD-Group FOR IGUAL A domain.com/groups/GHI EM SEGUIDA SGT:C2S-GHI E VLAN:1023
Política XYZ	Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed E Se AD-Group FOR IGUAL A domain.com/groups/XYZ EM SEGUIDA SGT:C2S-XYZ E VLAN:1024

Solução proposta

Para contornar a violação do número máximo escalável de políticas de autorização suportadas no Cisco ISE, a solução proposta é usar um BD externo que autorize cada endpoint com o resultado da autorização extraído de seus atributos. Por exemplo, se o AD for usado como um BD externo para autorização, qualquer atributo de usuário não utilizado (como Departamento ou código Pin) poderá ser consultado para fornecer resultados autorizados mapeados com SGT ou VLAN.

Isso é obtido com a integração do Cisco ISE com um BD externo ou dentro do BD interno do ISE configurado com atributos personalizados. Esta seção explica a implantação desses dois cenários:

> **Note**: Em ambas as opções, o DB contém o **user-id** mas não a **senha** dos pontos finais DOT1X. O DB é usado apenas como o ponto de **autorização**. A autenticação ainda pode continuar sendo o armazenamento de ID do cliente que, na maioria dos casos, reside no servidor do Ative Diretory (AD).

Configuração com BD externo

O Cisco ISE é integrado a um BD externo para validação de credenciais de endpoint:

Esta tabela mostra as Origens de Identidade Externas Validadas.

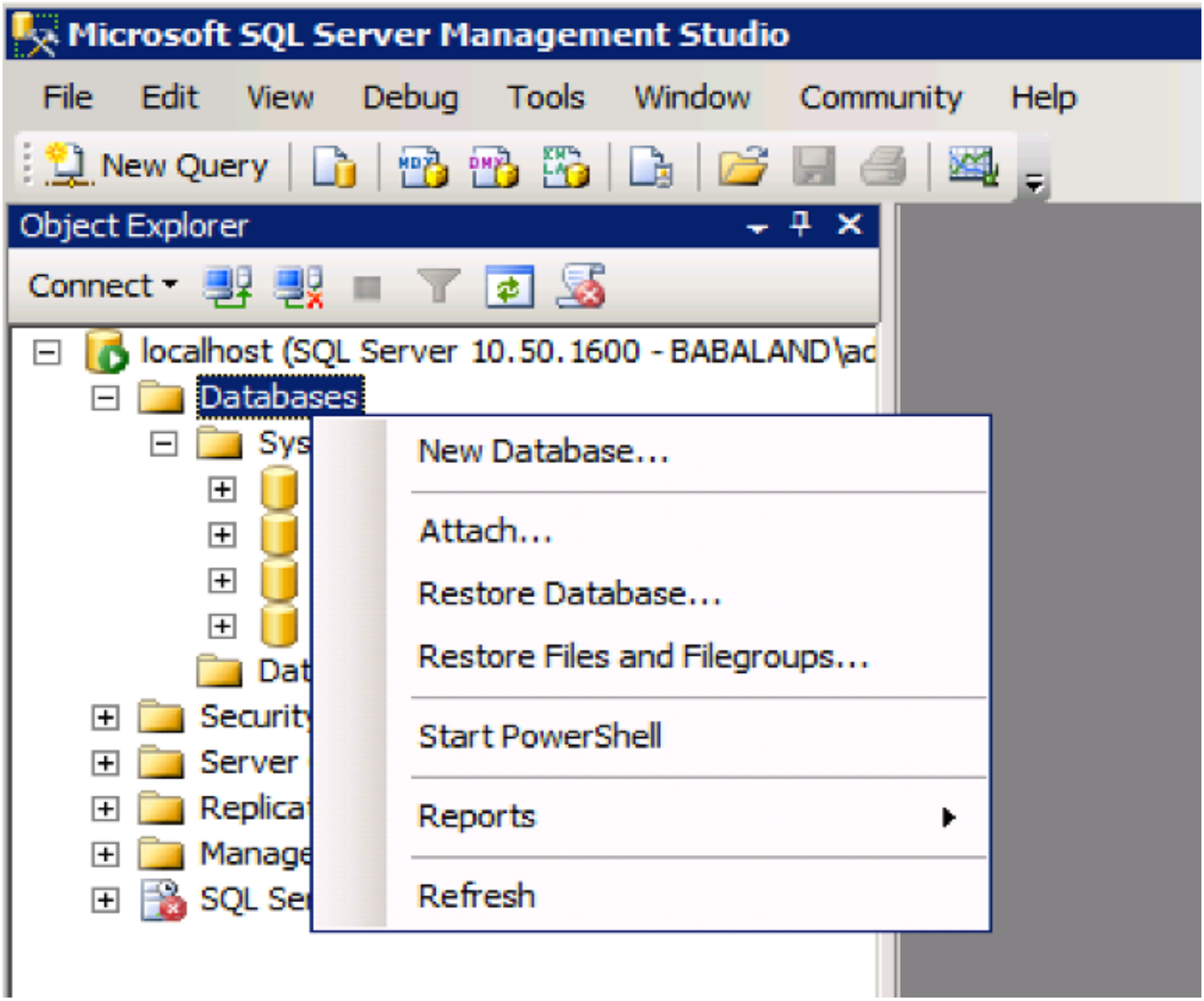
Fonte de identidade externa	SO/Versão
Diretório ativo	
Microsoft Windows Ative Diretory 2003	—
Microsoft Windows Ative Diretory 2003 R2	—
Microsoft Windows Ative Diretory 2008	—
Microsoft Windows Ative Diretory 2008 R2	—
Microsoft Windows Ative Diretory 2012	—
Microsoft Windows Ative Diretory 2012 R2	—
Microsoft Windows Ative Diretory 2016	—

Servidores LDAP	
Servidor de Diretório LDAP da SunONE	Versão 5.2
Servidor de diretório OpenLDAP	Versão 2.4.23
Qualquer servidor compatível com LDAP v3	—
Servidores de tokens	
RSA ACE/Servidor	Série 6.x
RSA Authentication Manager	Séries 7.x e 8.x
Qualquer servidor de token compatível com RADIUS RFC 2865	—
Logon Único (SSO) SAML (Security Assertion Markup Language)	
Microsoft Azure	—
Oracle Access Manager (OAM)	Versão 11.1.2.2.0
Oracle Identity Federation (OIF)	Versão 11.1.1.2.0
Servidor PingFederate	Versão 6.10.0.4
Nuvem PingOne	—
Autenticação segura	8.1.1
Qualquer Provedor de Identidade compatível com SAMLv2	—
Fonte de Identidade do Open Database Connectivity (ODBC)	
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition Versão 12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Login social (para contas de usuário convidado)	
Facebook	—

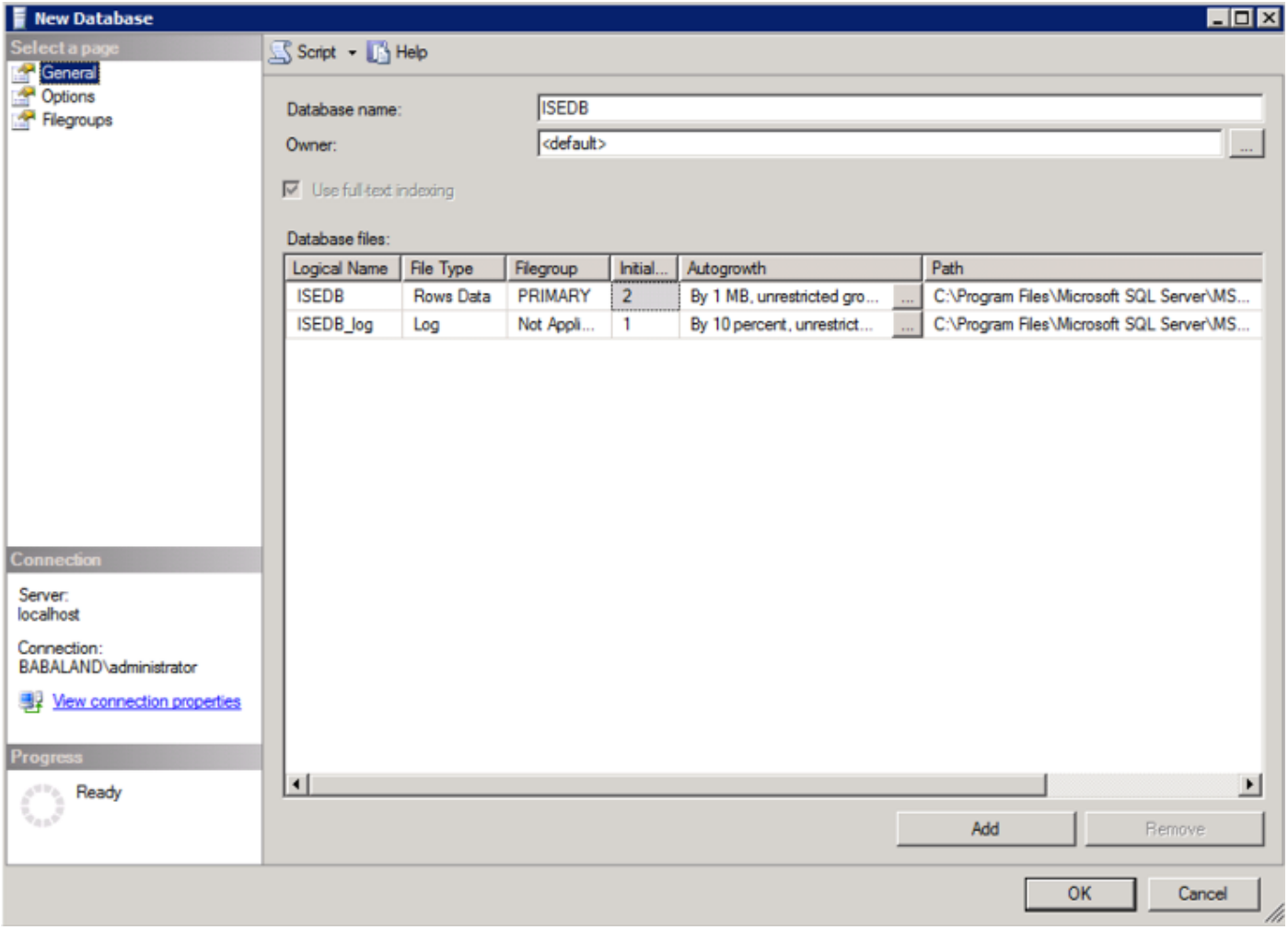
Configurações de exemplo de ODBC

Esta configuração é feita no Microsoft SQL para criar a solução:

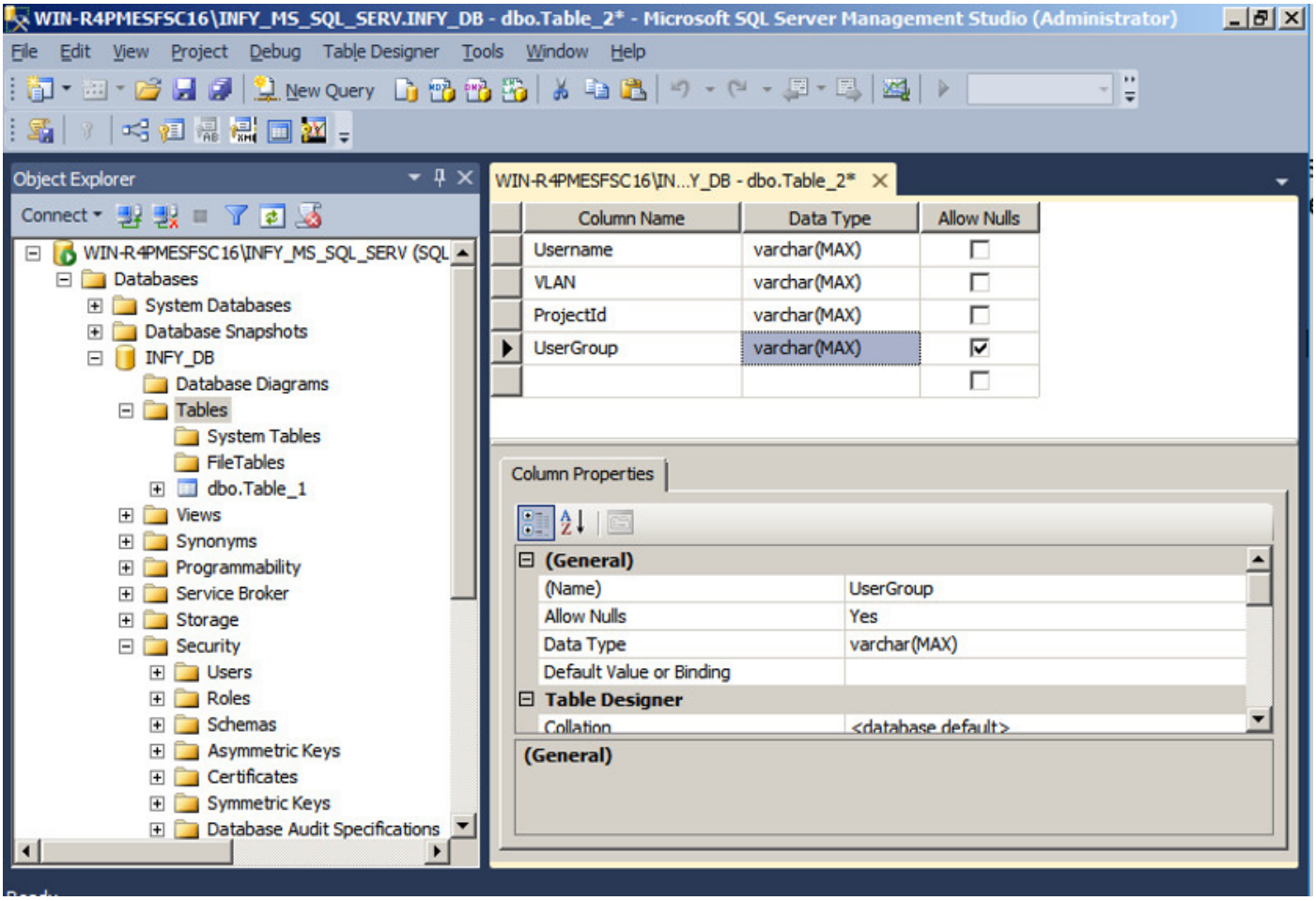
Etapa 1. Abra o SQL Server Management Studio (**menu Iniciar > Microsoft SQL Server**) para criar um banco de dados:



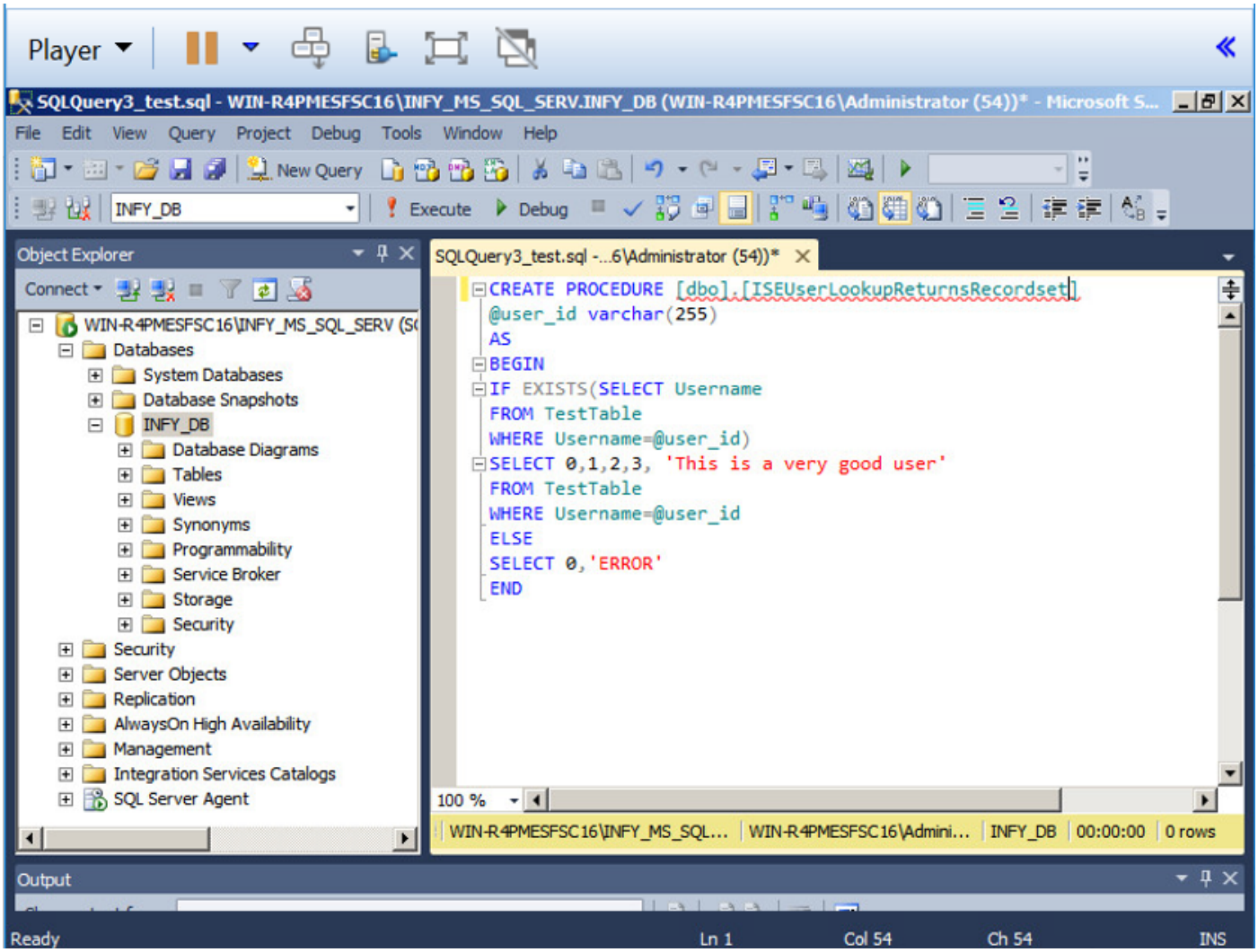
Etapa 2. Forneça um nome e crie o banco de dados.



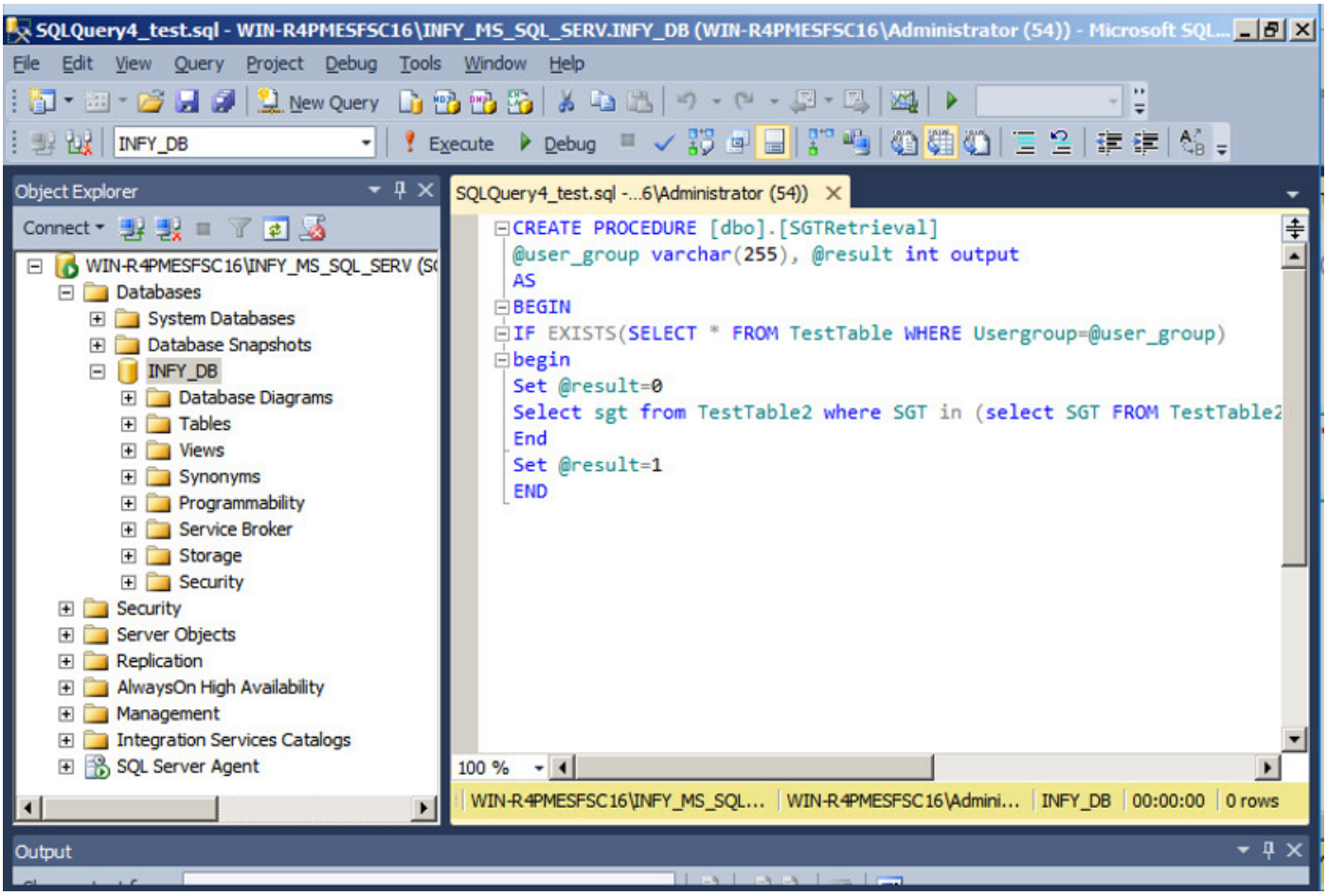
Etapa 3. Crie uma nova tabela com as colunas necessárias como parâmetros para os pontos finais serem autorizados.



Etapa 4. Crie um **procedimento** para verificar se o nome de usuário existe.



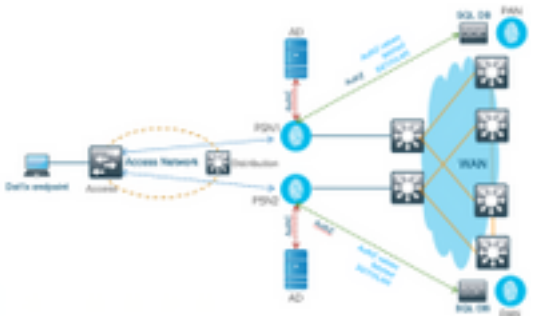
Etapa 5. Crie um procedimento para buscar atributos (SGT) da tabela.

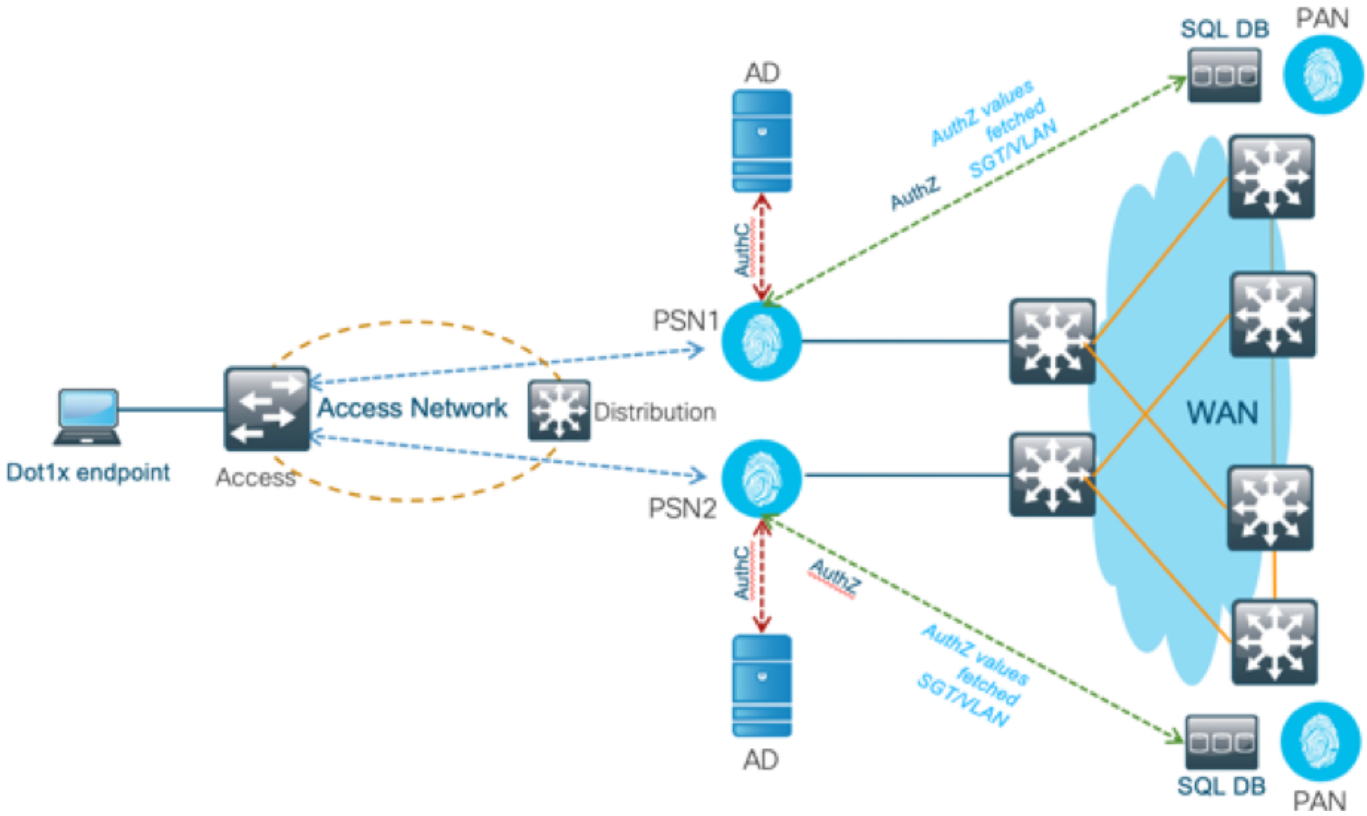


Neste documento, o Cisco ISE é integrado à solução Microsoft SQL para atender aos requisitos de escala de autorização em redes de grandes empresas.

Fluxo de trabalho da solução (ISE 2.7 e anterior)

Nessa solução, o Cisco ISE é integrado a um Ative Diretory (AD) e Microsoft SQL. O AD é usado como um repositório de ID de autenticação e MS SQL para autorização. Durante o processo de autenticação, o Network Access Device (NAD) encaminha as credenciais do usuário para a PSN - o servidor AAA na solução IBN. A PSN valida as credenciais do ponto de extremidade com o repositório de ID do Ative Diretory e autentica o usuário. A política de autorização se refere ao banco de dados MS SQL para buscar os resultados autorizados como SGT / VLAN para os quais **user-id** é usado como referência.





Vantagens

Essa solução tem as seguintes vantagens, o que a torna flexível:

- O Cisco ISE pode aproveitar todos os recursos adicionais possíveis que o BD externo oferece.
- Essa solução não depende de nenhum limite de escala do Cisco ISE.

Desvantagens

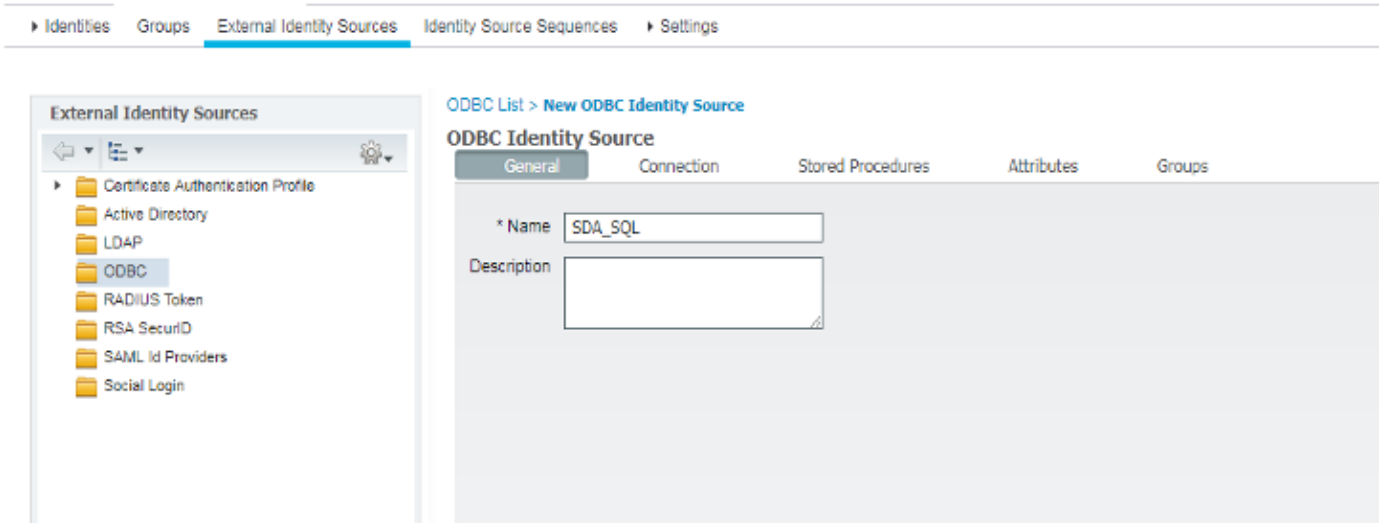
Essa solução tem as seguintes desvantagens:

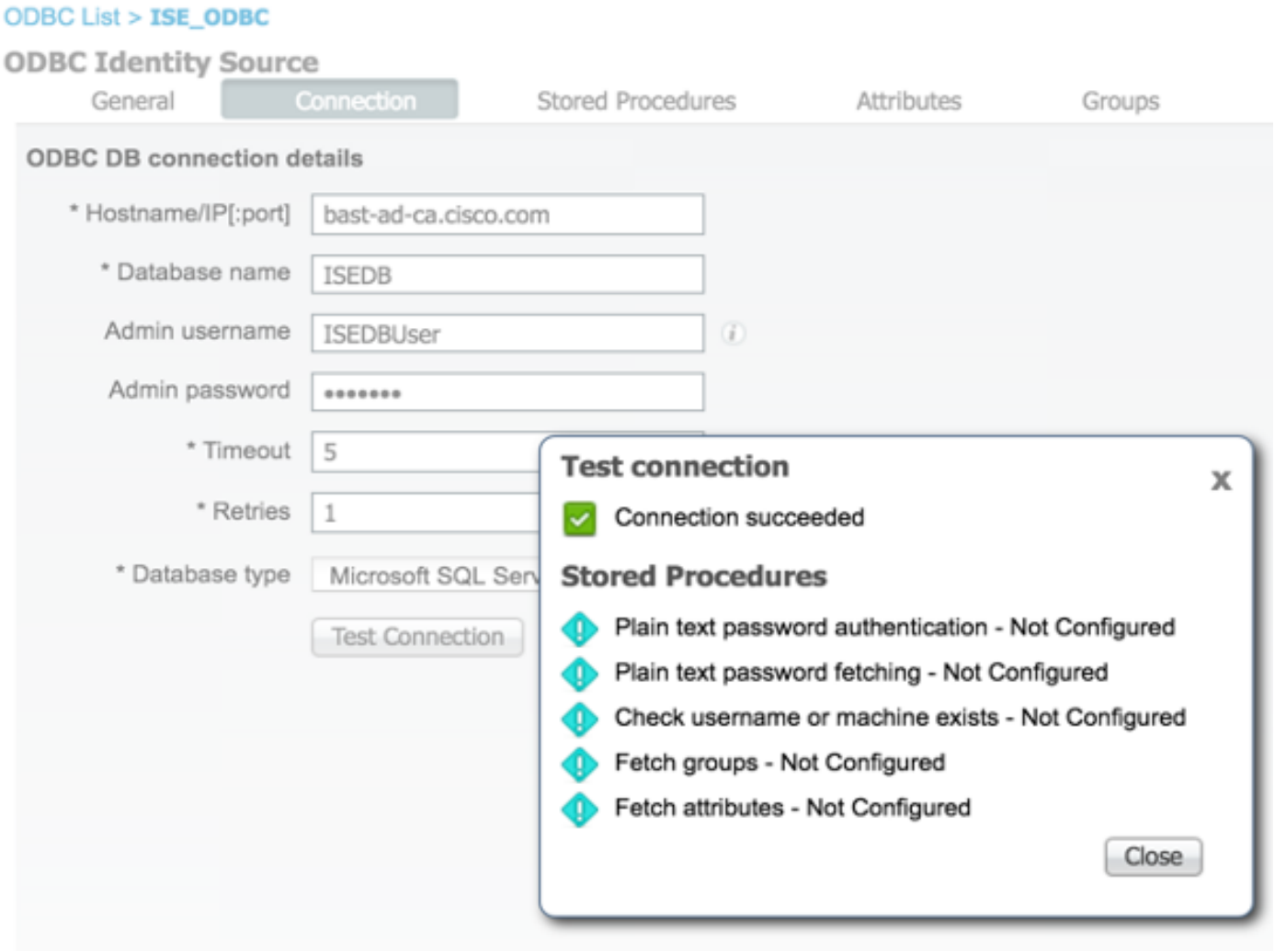
- Requer programação adicional para preencher o BD externo com credenciais de ponto de extremidade.
- Se o DB externo não estiver localmente presente como PSNs, essa solução depende da WAN, o que o torna o 3° ponto de falha no fluxo de dados AAA do endpoint.
- Requer conhecimento adicional para manter processos e procedimentos externos do BD.
- Os erros causados pela configuração manual da id de usuário para o BD devem ser considerados.

Configurações de Exemplo de BD Externo

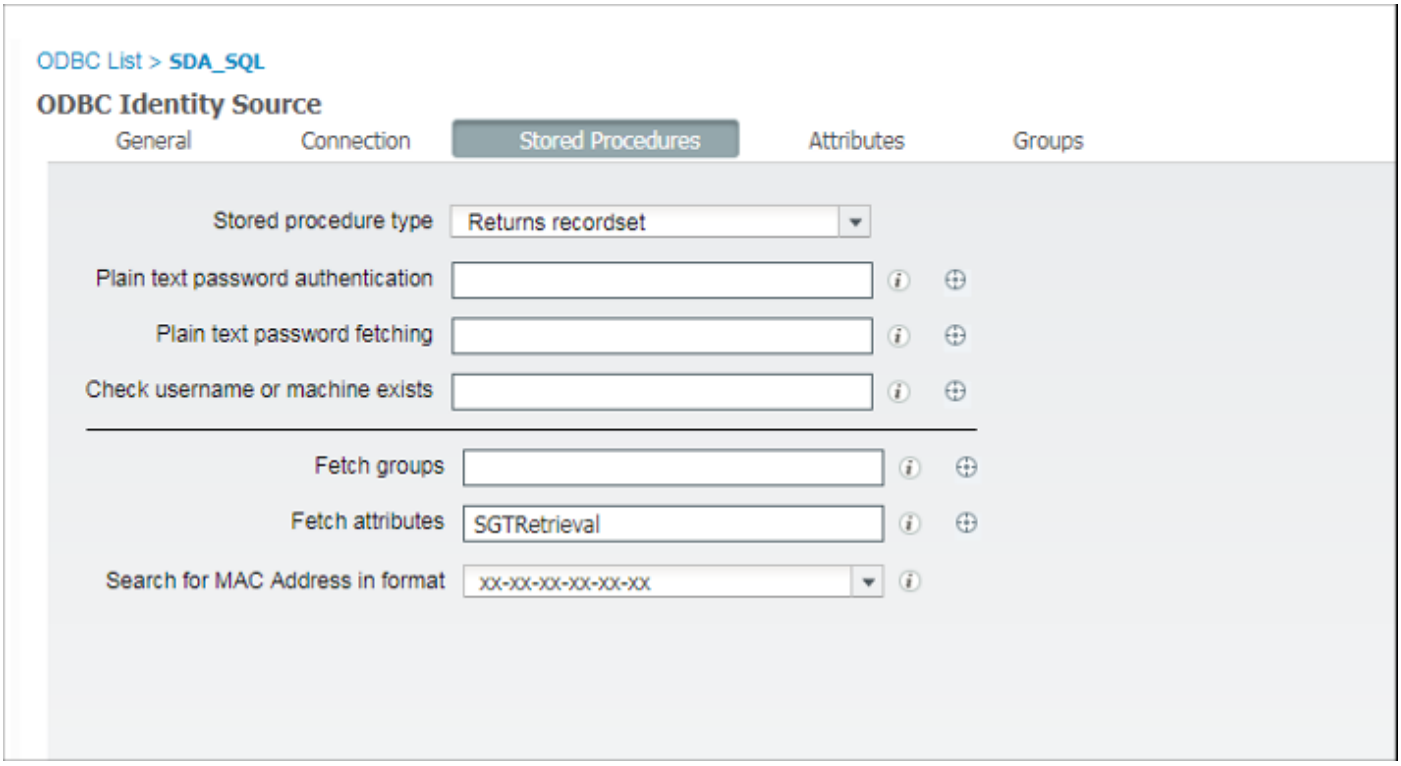
Neste documento, o Microsoft SQL é mostrado como o banco de dados externo usado como um ponto de autorização.

Etapa 1. Crie o ODBC Identity store no Cisco ISE no menu **Administration > External Identity Source > ODBC** e teste as conexões.

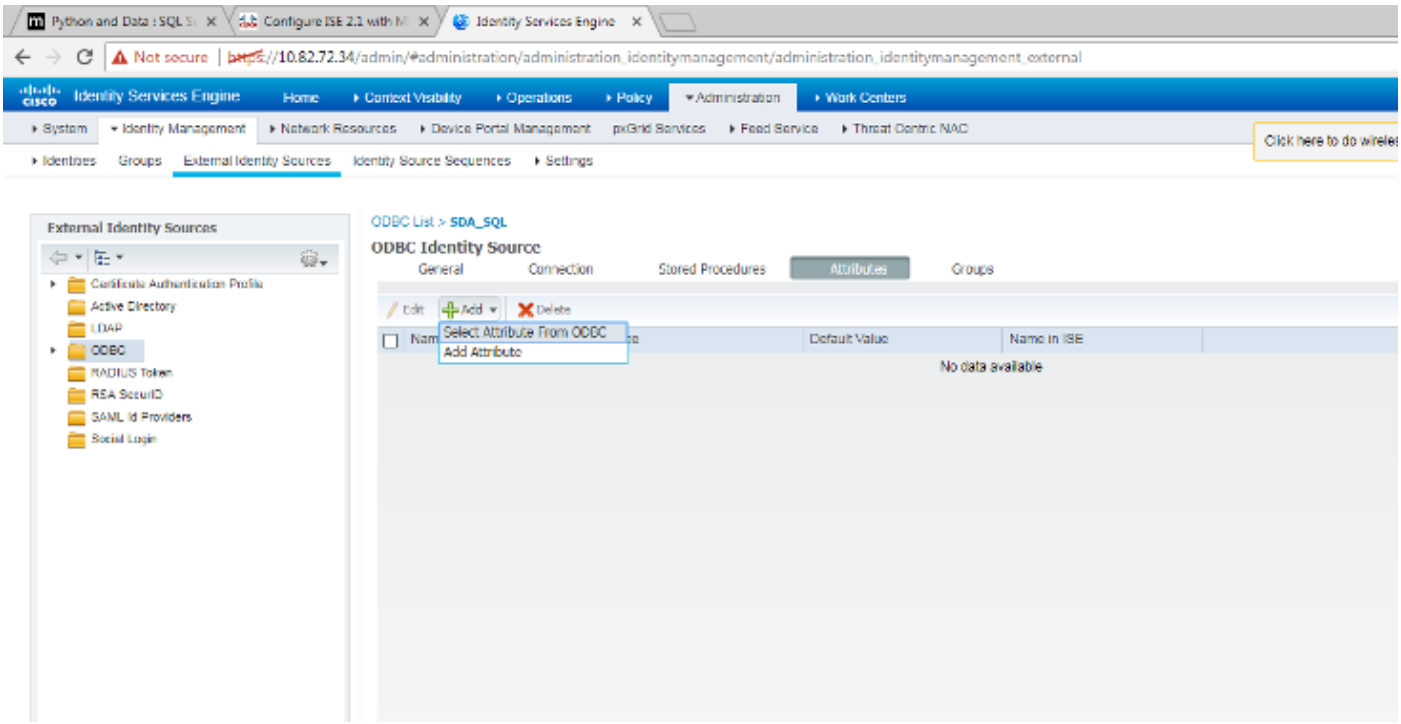


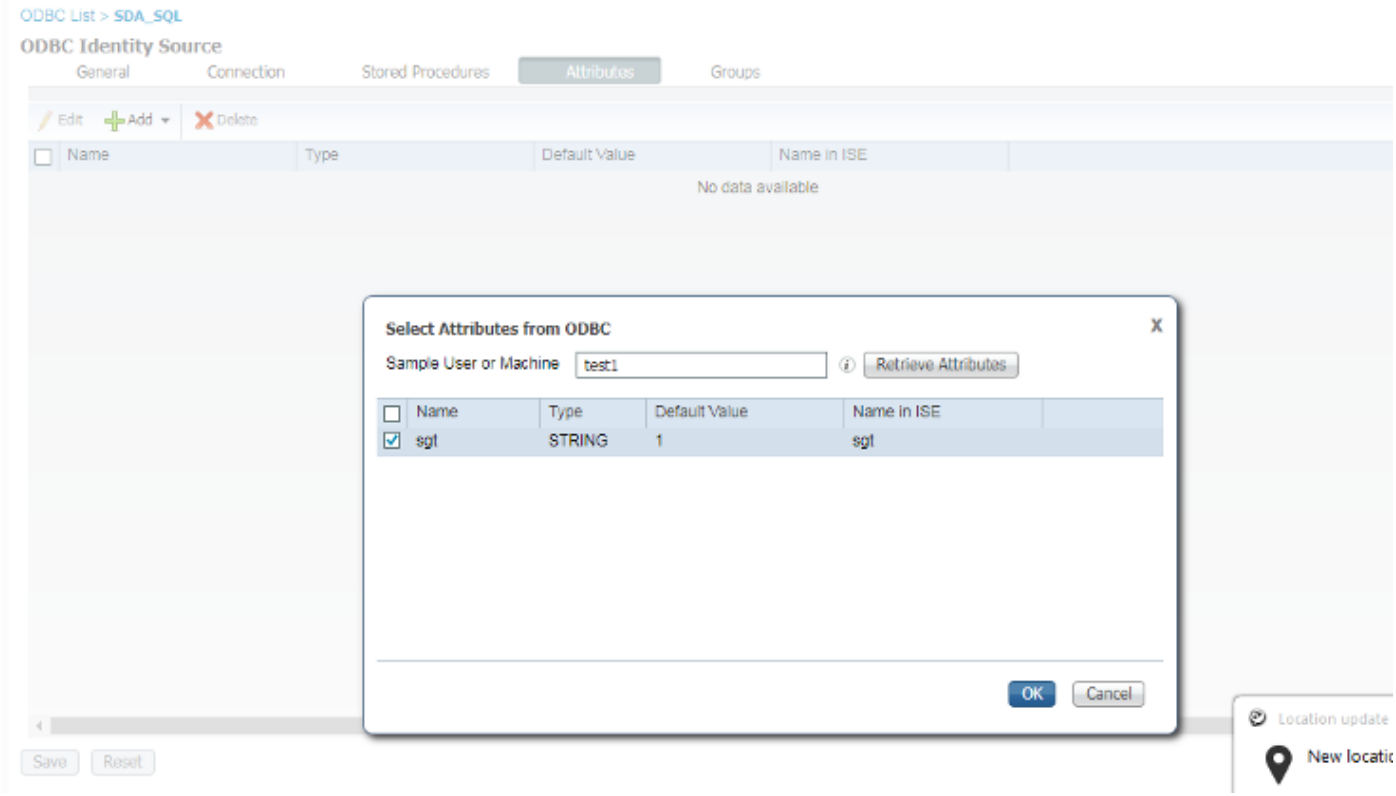


Etapa 2. Navegue até a guia Procedimentos armazenados na página ODBC para configurar os procedimentos criados no Cisco ISE.

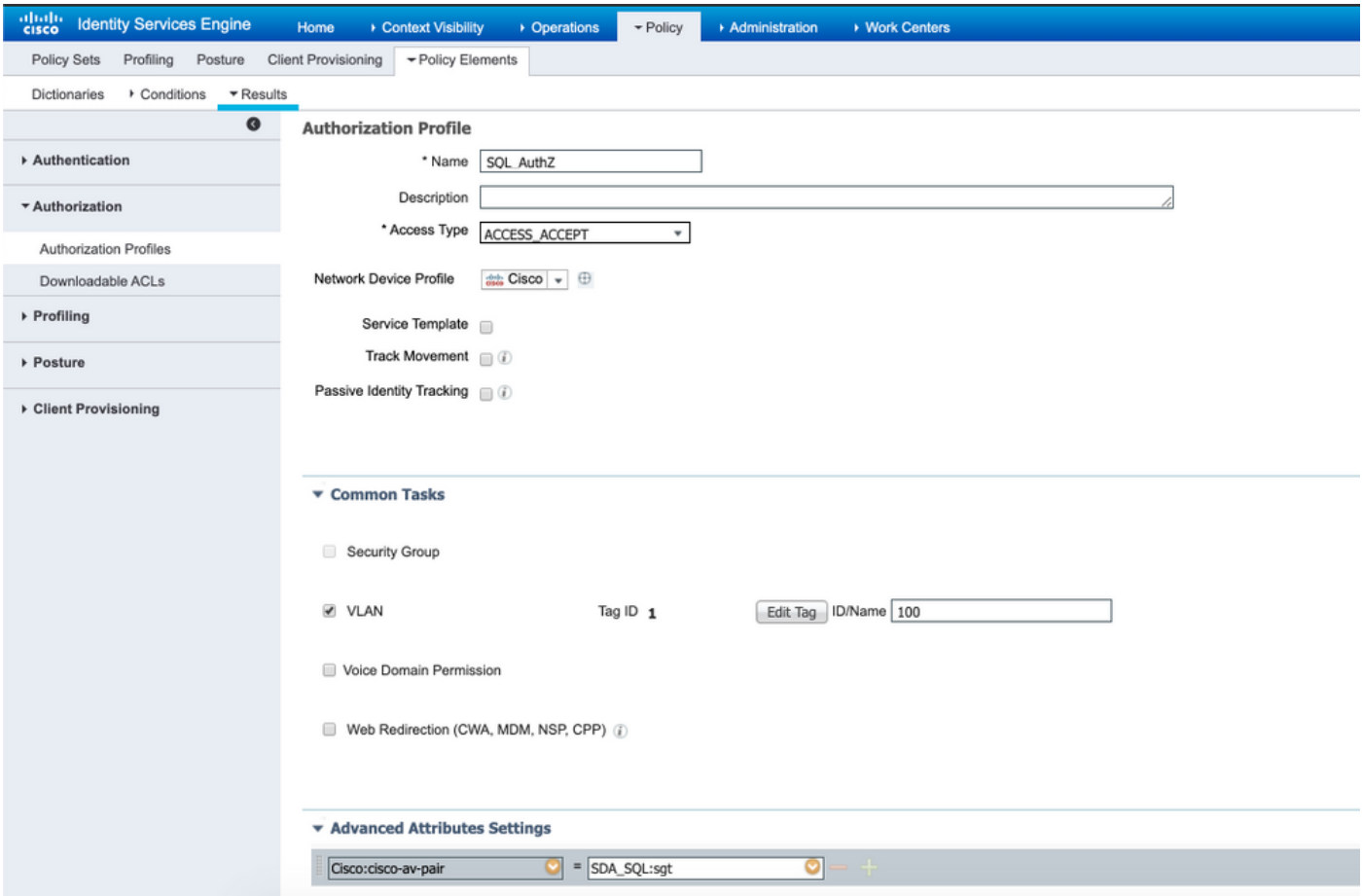


Etapa 3. Busque os atributos do ID de usuário na origem do ID ODBC para verificação.

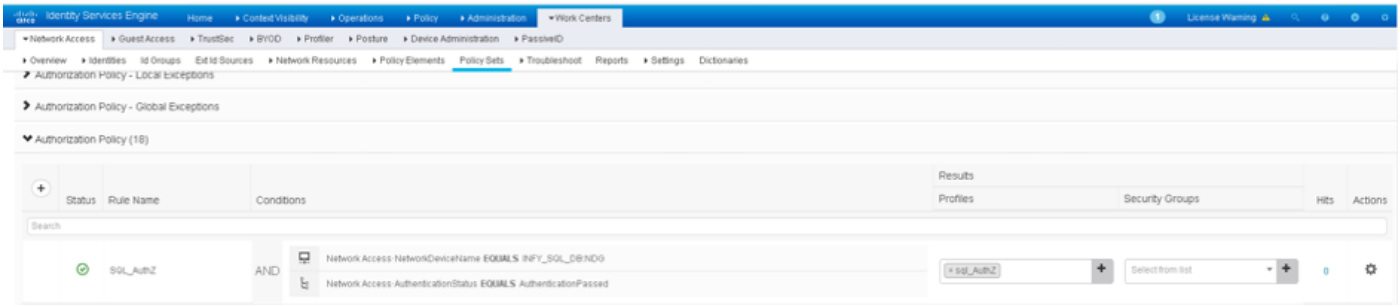




Etapa 4. Crie um **perfil de autorização** e configure-o. No Cisco ISE, vá para **Policy > Results > Authorization profile > Advance Attributes Settings** e selecione o atributo como **Cisco:cisco-av-pair.** Selecione os valores como <name of ODBC database>:sgt e salve-o.



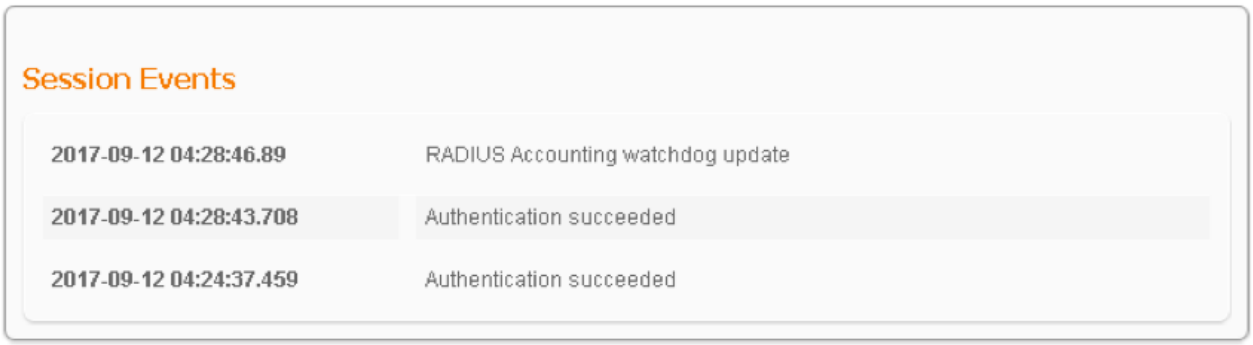
Etapa 5. Crie uma **política de autorização** e configure-a. No Cisco ISE, navegue para **Policy > Policy sets > Authorization Policy > Add.** Coloque a condição como Identity Source is the SQL server. Selecione o perfil Resultado como o perfil de Autorização criado anteriormente.



Passo 6. Uma vez autenticado e autorizado o utilizador, os registros devem conter o sgt atribuído ao utilizador, para verificação.

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

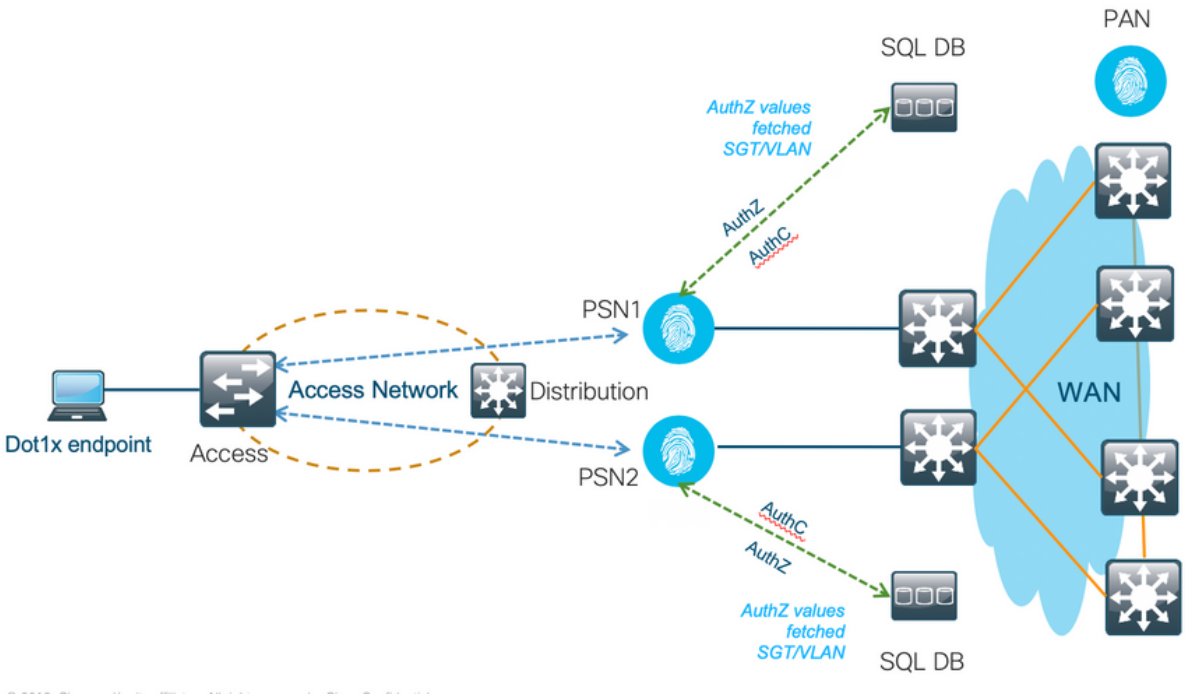
2017-09-12 04:28:46.89	RADIUS Accounting watchdog update
2017-09-12 04:28:43.708	Authentication succeeded
2017-09-12 04:24:37.459	Authentication succeeded

Fluxo de trabalho da solução (pós-ISE 2.7)

Após o ISE 2.7, os atributos de autorização podem ser buscados no ODBC, como Vlan, SGT, ACL, e esses atributos podem ser consumidos em Políticas.

Nessa solução, o Cisco ISE é integrado ao Microsoft SQL. O MS SQL é usado como um armazenamento de ID para autenticação e autorização. Quando as credenciais dos pontos de extremidade são fornecidas ao PSN, ele valida as credenciais em relação ao banco de dados MS

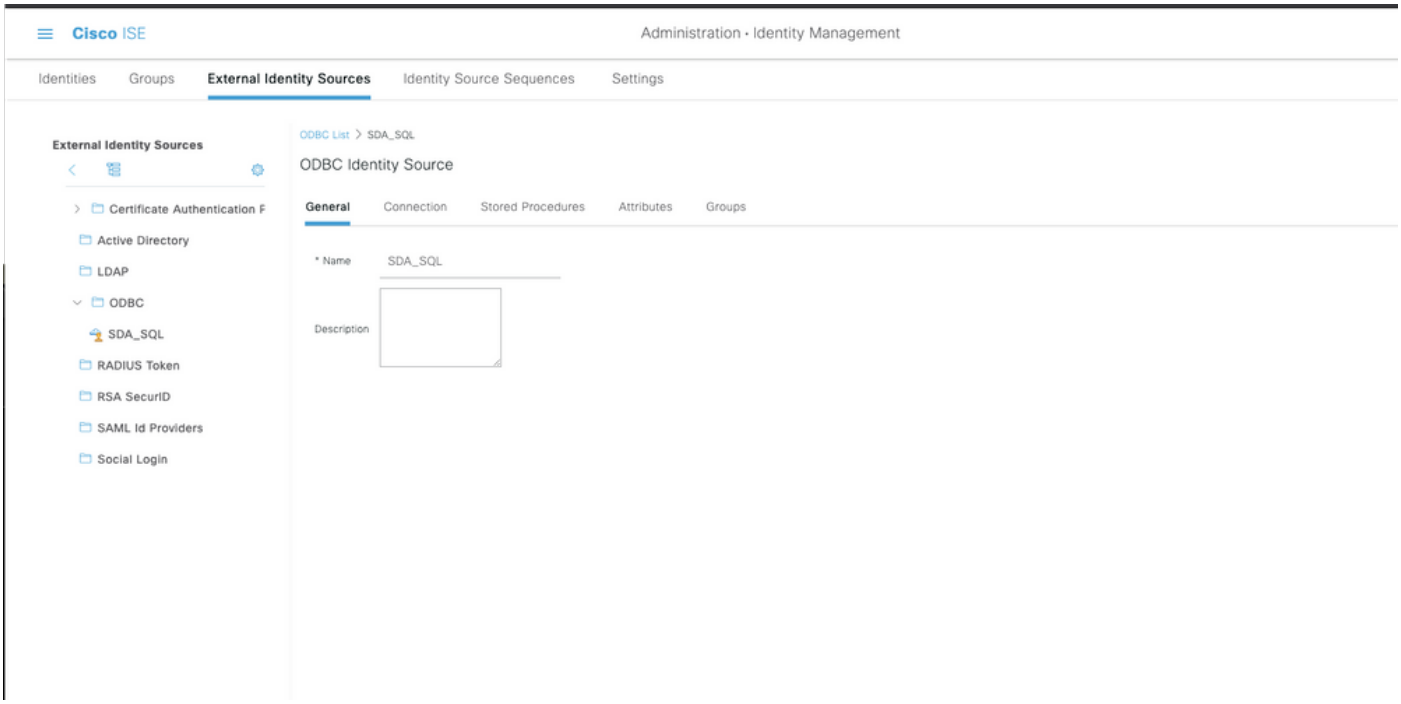
SQL. A política de autorização se refere ao banco de dados MS SQL para buscar os resultados autorizados, como SGT / VLAN, para os quais **user-id** é usado como referência.



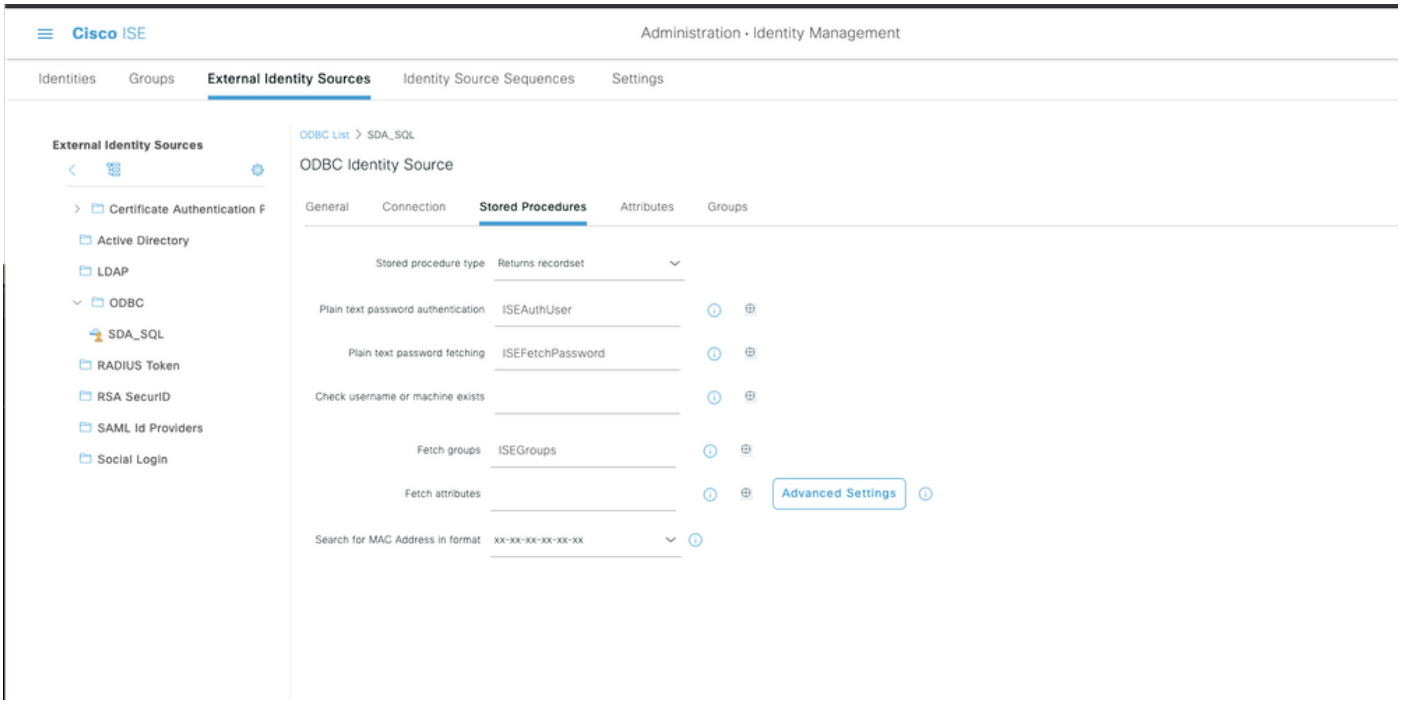
Configurações de Exemplo de BD Externo

Siga o procedimento fornecido anteriormente neste documento para criar o banco de dados MS SQL junto com o nome de usuário, a senha, a ID da VLAN e o SGT.

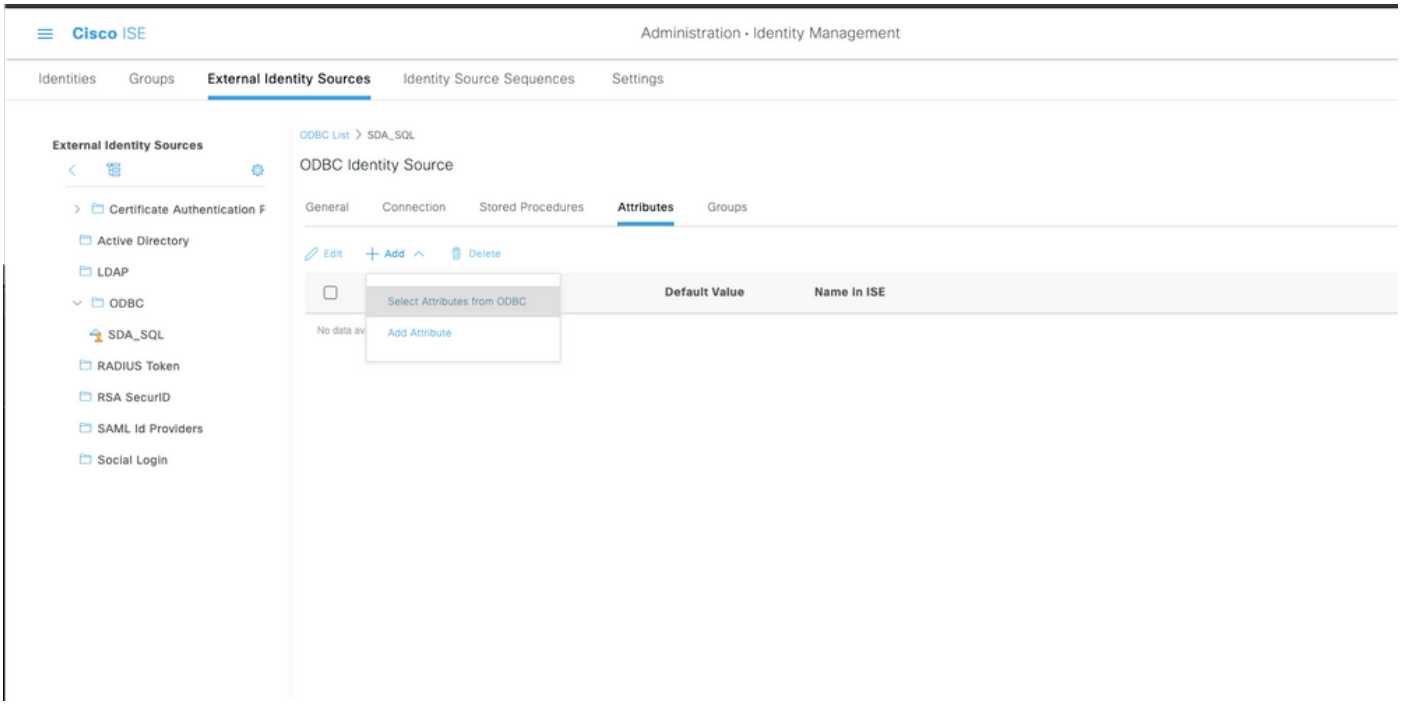
Etapa 1. Crie um armazenamento de Identidade ODBC no Cisco ISE a partir do menu **Administration > External Identity Source > ODBC** e teste as conexões.

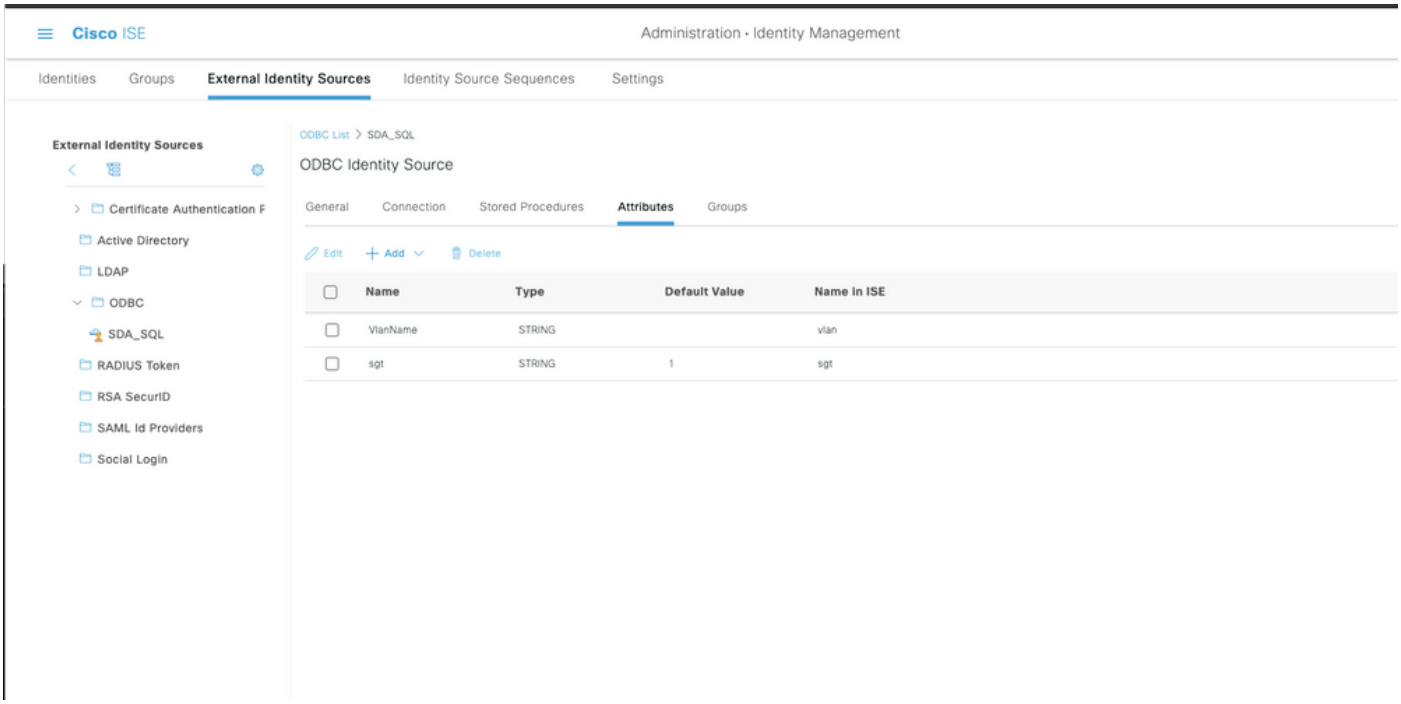


Etapa 2. Navegue até a guia Procedimentos armazenados na página ODBC para configurar os procedimentos criados no Cisco ISE.

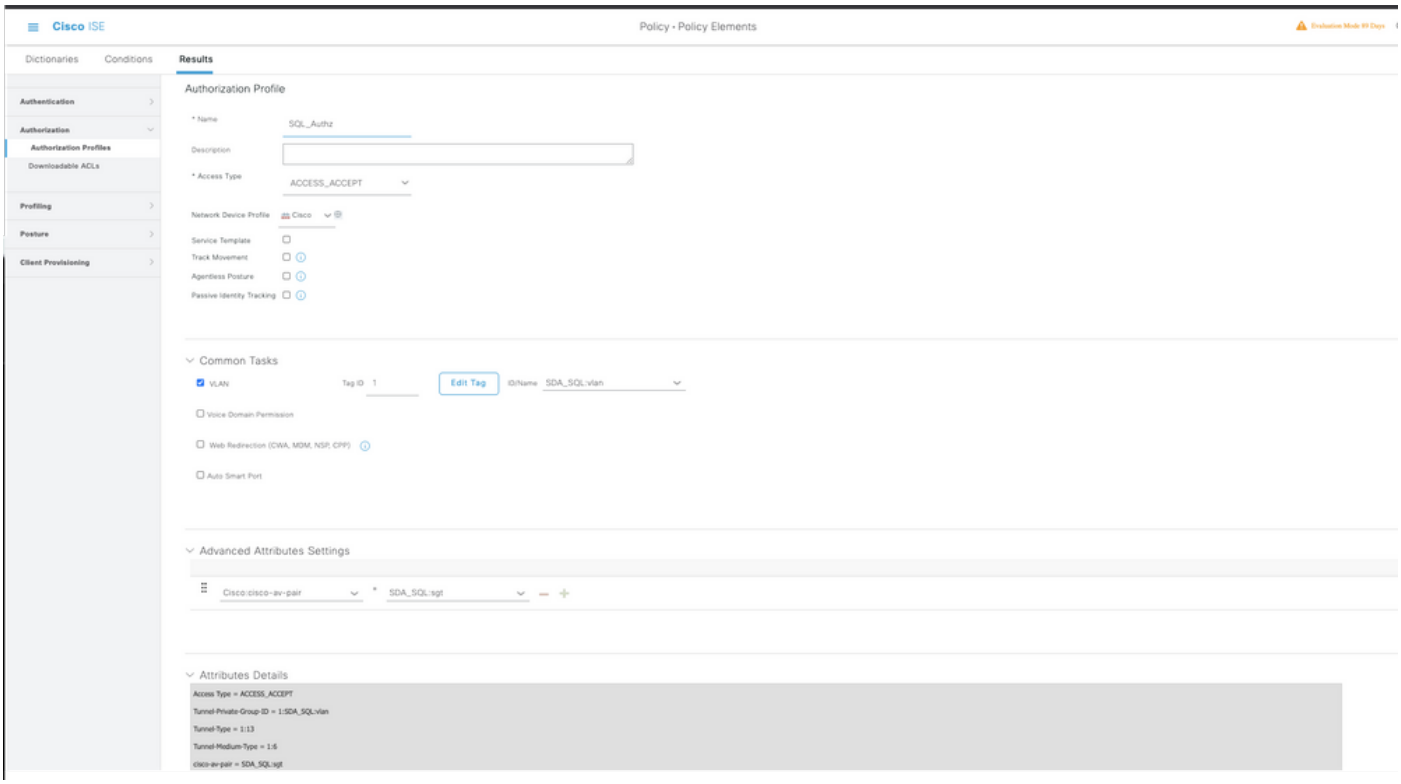


Etapa 3. Busque os atributos do ID de usuário na origem do ID ODBC para verificação.

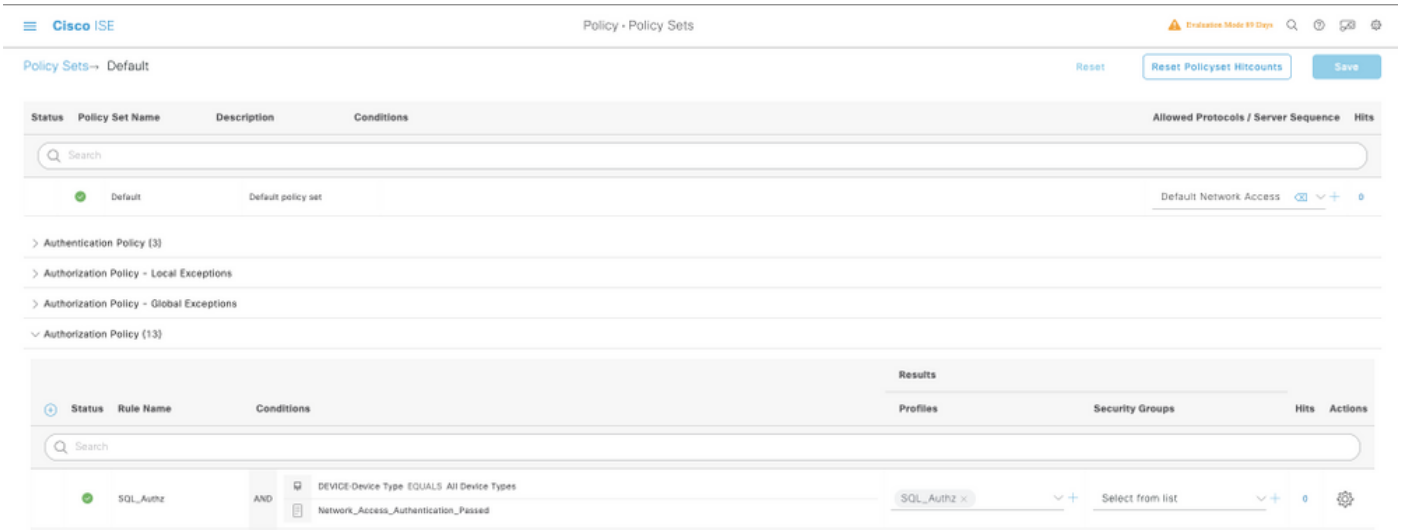




Etapa 4. Crie um **perfil de autorização** e configure-o. No Cisco ISE, vá para **Policy > Results > Authorization profile > Advance Attributes Settings** e selecione o atributo como **Cisco:cisco-av-pair.** Selecione os valores como <name of ODBC database>:sgt. Em Common Tasks, selecione **VLAN** com ID/Name como <name of ODBC database>:vlan e salve-o



Etapa 5. Crie uma **política de autorização** e configure-a. No Cisco ISE, navegue para **Policy > Policy sets > Authorization Policy > Add.** Coloque a condição como Identity Source is the SQL server. Selecione o perfil Resultado como o perfil de Autorização criado anteriormente.

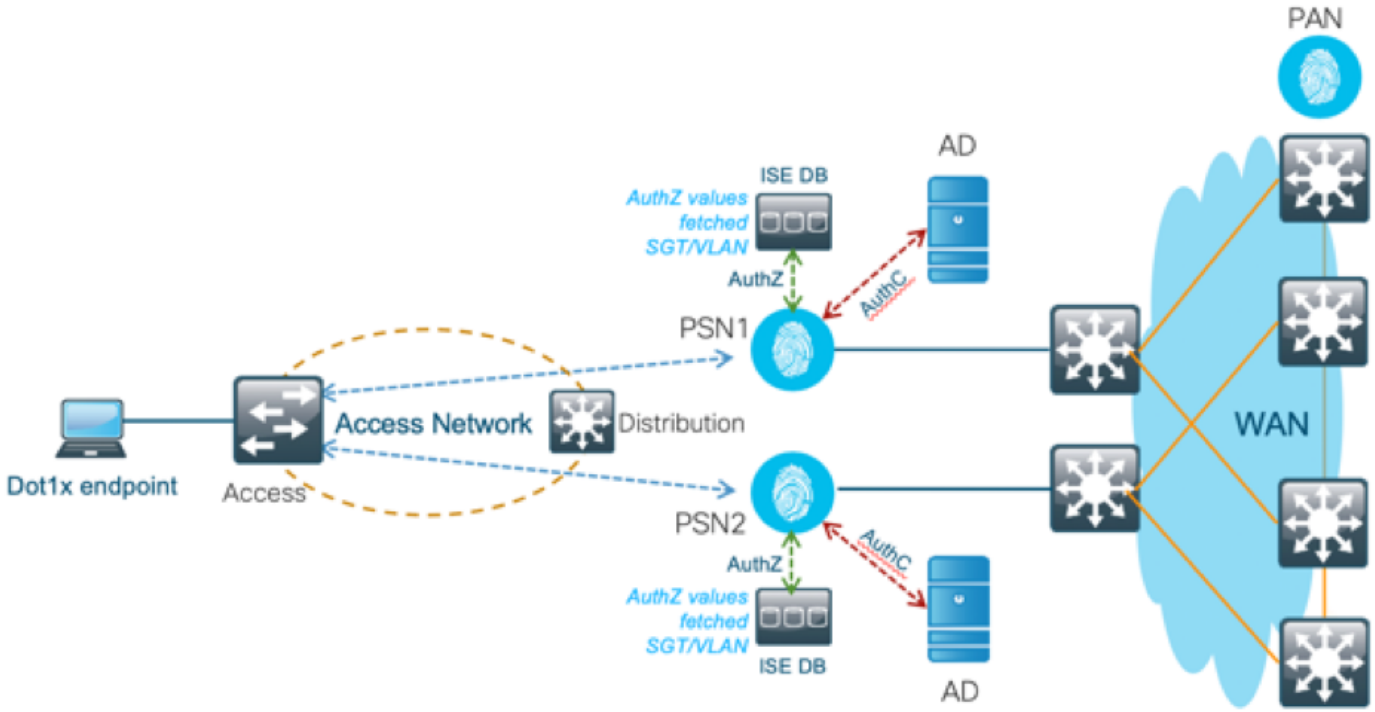


Usar BD Interno

O próprio Cisco ISE tem um BD integrado que pode ser utilizado para ter IDs de usuário para autorização.

Fluxo de trabalho da solução

Nessa solução, o BD interno do Cisco ISE é usado como um ponto de autorização, enquanto o Ative Diretory (AD) continua a ser a origem da autenticação. A ID de usuário de endpoints está incluída no Cisco ISE DB junto com **atributos personalizados** que retornam os resultados autorizados, como SGT ou VLAN. Quando as credenciais dos pontos de extremidade são fornecidas ao PSN, ele verifica a validade das credenciais dos pontos de extremidade com o armazenamento de ID do Ative Diretory e autentica o ponto de extremidade. A política de autorização se refere ao BD do ISE para buscar os resultados autorizados, como SGT/VLAN, para os quais a ID de usuário é usada como referência.



Vantagens

Essa solução tem as seguintes vantagens, o que a torna uma solução flexível:

- O Cisco ISE DB é uma solução integrada e, portanto, não tem o terceiro ponto de falha, ao contrário da solução de BD externa.
- Como o cluster do Cisco ISE garante sincronização em tempo real entre todas as personas, não há dependência de WAN, pois a PSN tem todas as IDs de usuário e atributos personalizados enviados da PAN em tempo real.
- O Cisco ISE pode aproveitar todos os recursos adicionais possíveis que o BD externo oferece.
- Essa solução não depende de nenhum limite de escala do Cisco ISE.

Desvantagens

Essa solução tem as seguintes desvantagens:

- O número máximo de IDs de usuário que o Cisco ISE DB pode reter é 300.000.
- Os erros causados pela configuração manual da id de usuário para o BD devem ser considerados.

Configurações de Exemplo de BD Interno

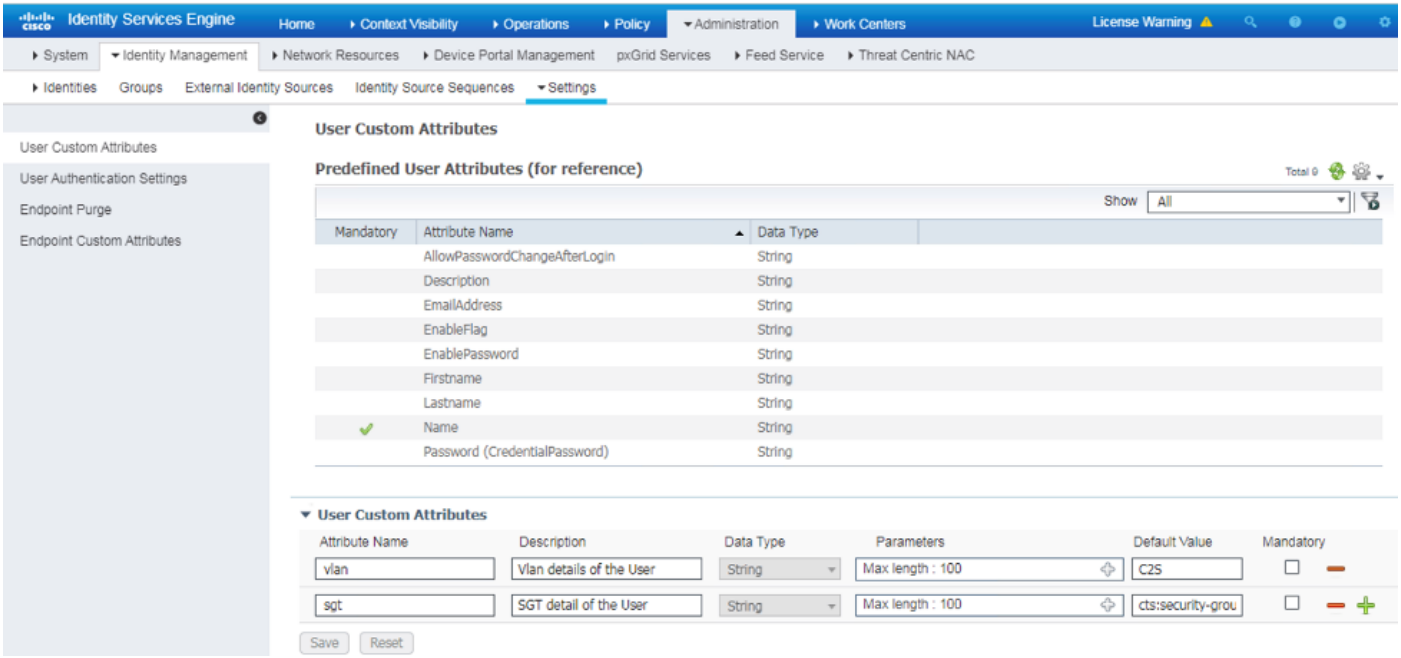
VLAN e SGT por usuário podem ser configurados para qualquer usuário no armazenamento de ID interno com um atributo de usuário personalizado.

Etapa 1. Crie novos atributos personalizados do usuário para representar o valor de VLAN e SGT dos respectivos usuários. Navegue até **Administração > Gerenciamento de Identidades > Configurações > Atributos Personalizados do Usuário.** Crie novos atributos personalizados do Usuário conforme mostrado nesta tabela.

Aqui, a tabela ISE DB é mostrada com atributos personalizados.

Nome do atributo	Tipo de dados	Parâmetros(Comprimento)	Valor padrão
vlan	Série	100	C2S (Nome De Vlan Padrão)
sgt	Série	100	cts:security-group-tag=0003-0 (valor SGT padrão)

- Neste cenário, o valor da VLAN representa o nome da vlan e o valor sgt representa o atributo cisco-av-pair de SGT em hexadecimal.

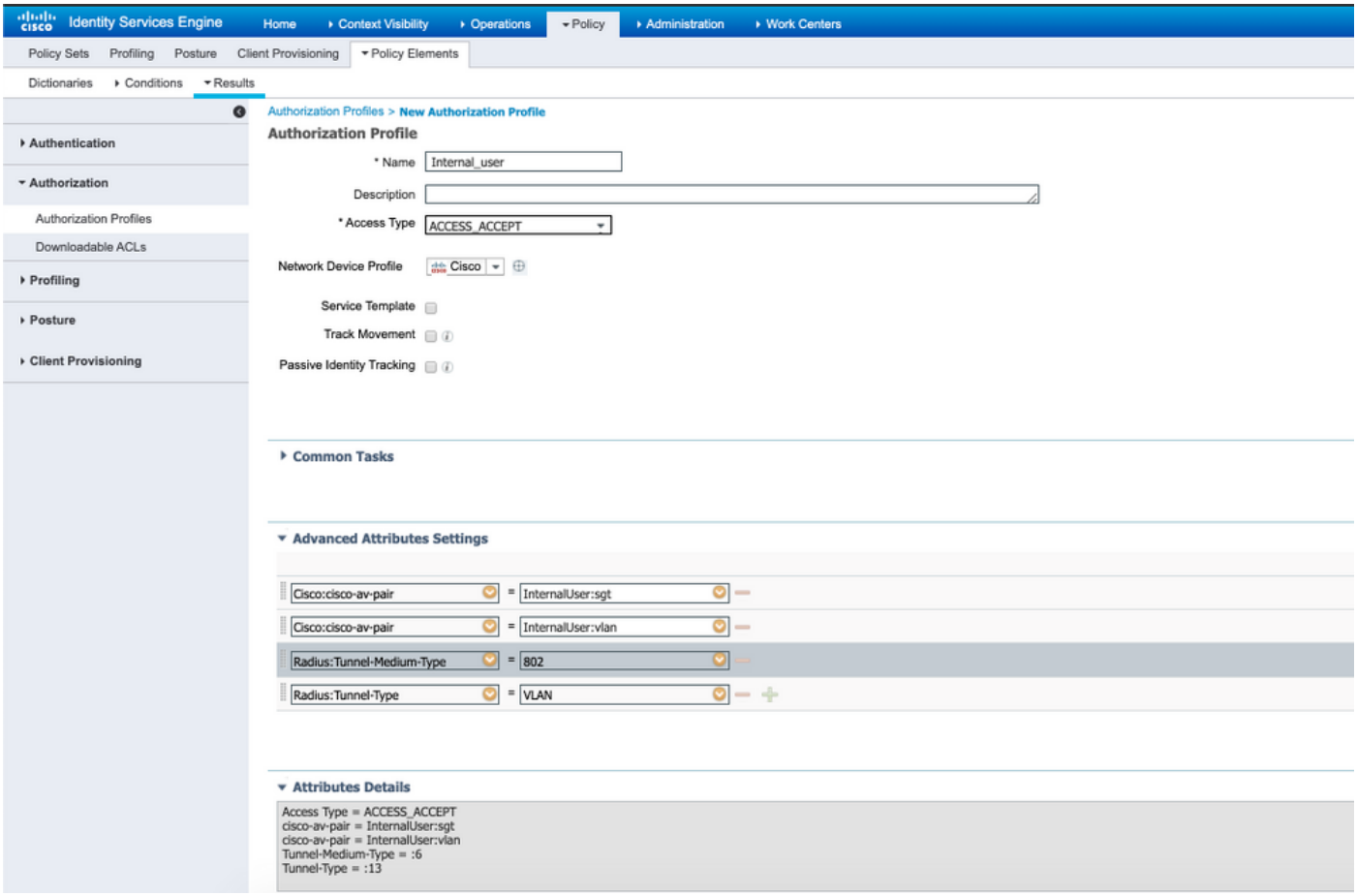


Etapa 2. Crie um Perfil de autorização com atributos personalizados do usuário para implicar os valores vlan e sgt dos respectivos usuários. Navegue até **Política > Elementos de política > Resultados > Autorização > Perfis de autorização > Adicionar.** Adicione os atributos mencionados abaixo em Configurações avançadas de atributos.

Esta tabela mostra o Perfil AuthZ para Usuário Interno.

Atributo	Valor
Cisco:cisco-av-pair	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	InternalUser:vlan
Raio:Tipo De Meio De Túnel	802
Raio:Tipo De Túnel	VLAN

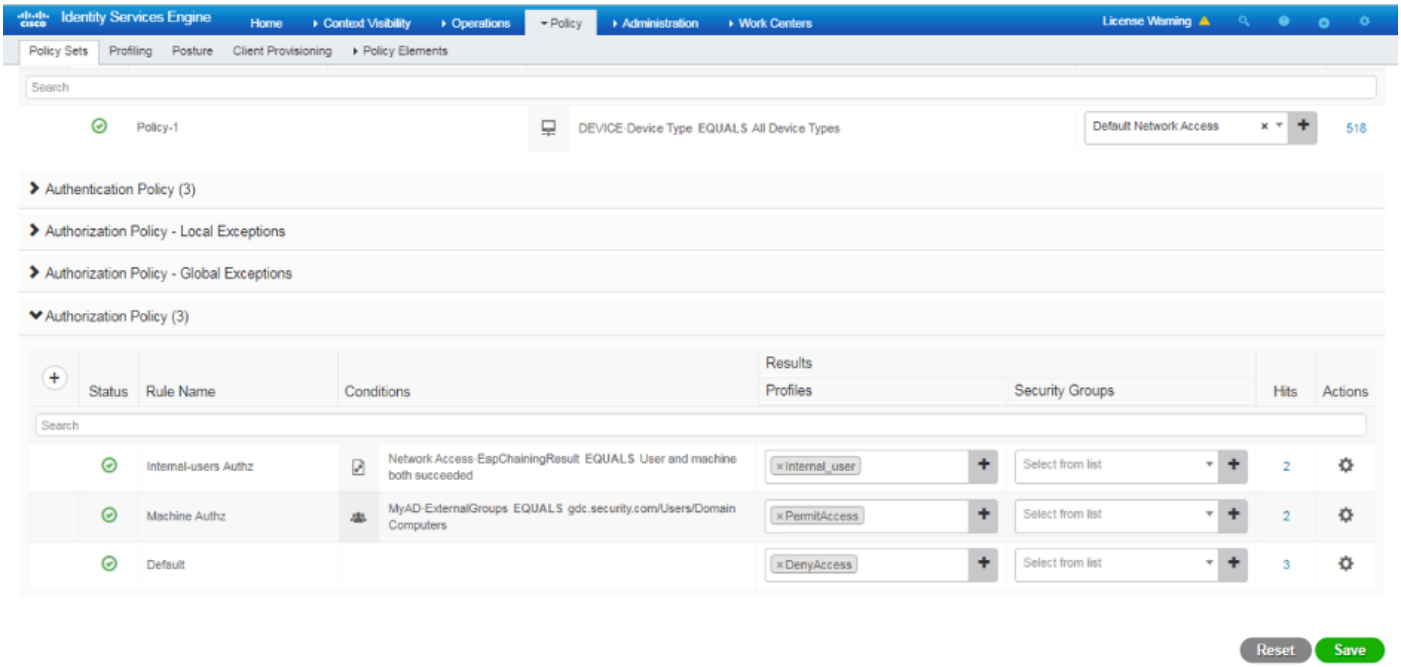
Como mostrado na imagem, para os usuários internos, o perfil **Internal_user** é configurado com o SGT e a Vlan configurados como **InternalUser:sgt** e **InternalUser:vlan**, respectivamente.



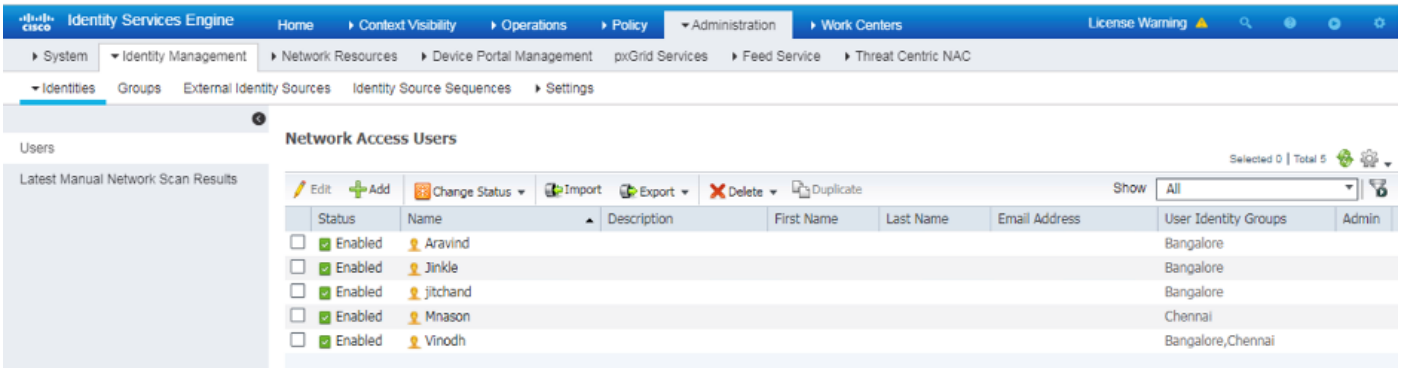
Etapa 3. Crie a política de autorização, Navegue até **Policy > Policy Sets > Policy-1 > Authorization.** Crie políticas de autorização com as condições mencionadas abaixo e mapeie-as para os respectivos perfis de autorização.

Esta tabela mostra a Diretiva AuthZ para Usuário Interno.

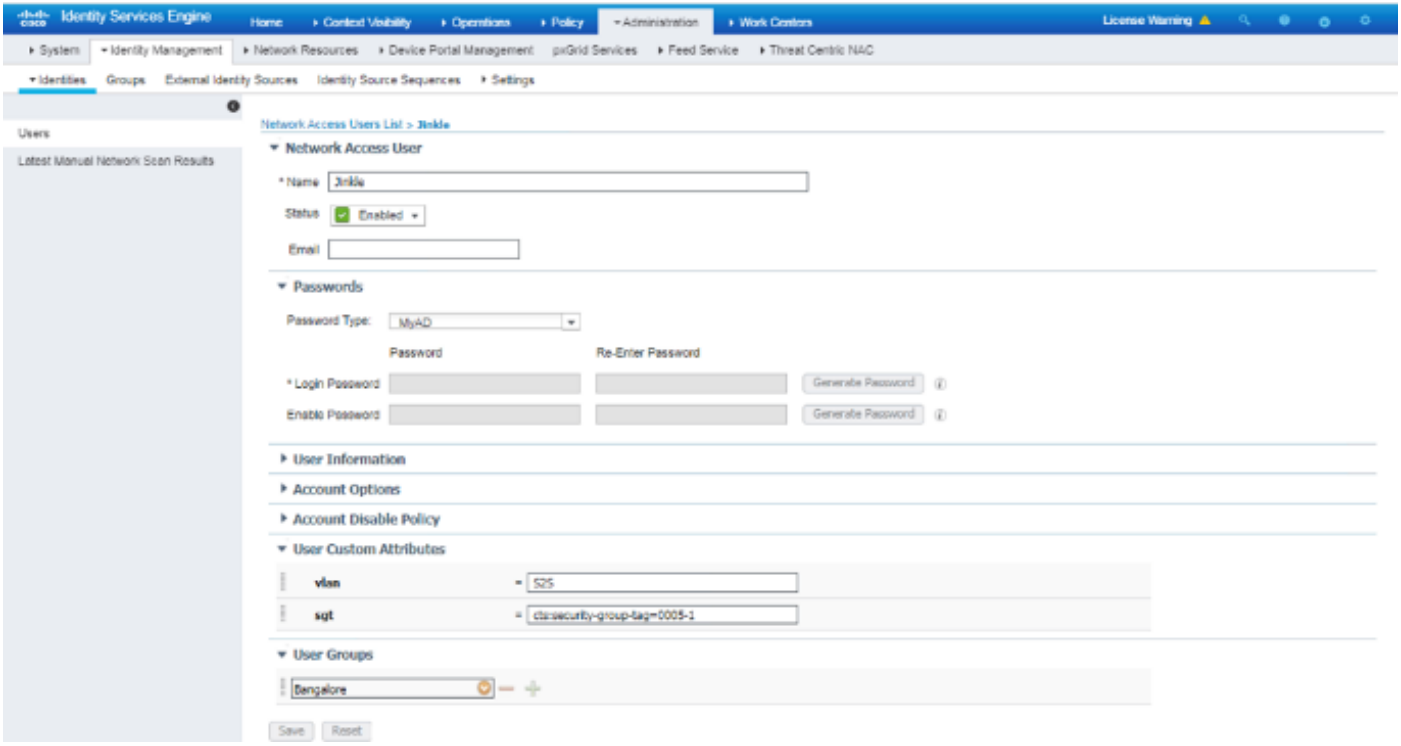
Nome da regra	Condição	Perfil de Autorização de Resultado
Autorização_Usuário_Interno	Se Network Access.EapChainingResults for IGUAL a usuário e máquina tiveram êxito	Internal_user
Autorização_Somente_Máquina	Se MyAD.ExternalGroups for IGUAL a gdc.security.com/Users/Domain Computadores	PermitirAcesso



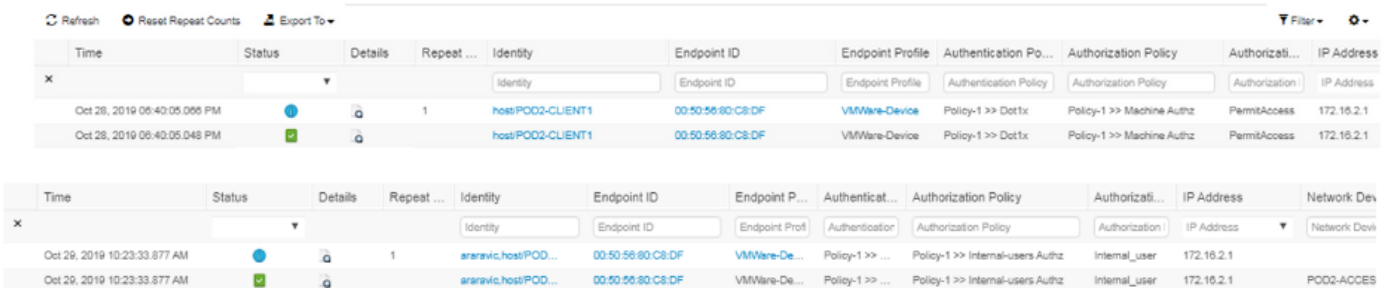
Etapa 4. Crie identidades de usuário em massa com atributos personalizados com detalhes do usuário e seus respectivos atributos personalizados no modelo csv. Importe o csv por Navegue até **Administração > Gerenciamento de identidades > Identidades > Usuários > Importar > Escolha o arquivo > Importar.**



Esta imagem mostra um usuário de exemplo com detalhes de atributos personalizados. Selecione o usuário e clique em editar para exibir os detalhes do atributo personalizado mapeados para o respectivo usuário.



Passo 5: Verifique os logs dinâmicos:



Verifique a seção **Resultado** para verificar se o atributo **Vlan** & **SGT** é enviado como parte de Access-Accept.

Conclusão

Essa solução permite que alguns dos clientes de grandes empresas dimensionem conforme suas necessidades. É necessário ter cuidado ao adicionar/excluir IDs de usuário. Os erros, se acionados, podem levar a acesso não autorizado para usuários genuínos ou vice-versa.

Informações Relacionadas

Configurar o Cisco ISE com 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

Glossário

AAA	Autenticação Autorização Contabilidade
ANÚNCIO	Diretório ativo
AuthC	Autenticação
AuthZ	Autorização
DB	Base de dados
DOT1X	802.1X
IBN	Rede baseada em identidade
ID	Banco de dados de identidade
ISE	Identity Services Engine
MnT	Monitoramento e solução de problemas
MsSQL	SQL da Microsoft

ODBC	Conectividade aberta do banco de dados
PAN	Nó do Administrador de Política
PSN	Nó de serviços de política
SGT	Tag de grupo segura
SQL	Linguagem de Consulta Estruturada
VLAN	LAN Virtual
WAN	Rede de longa distância

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.