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

Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Tendências em tecnologia Problema Solução proposta Configuração com BD externo Configurações de exemplo de ODBC Fluxo de trabalho da solução (ISE 2.7 e anterior) Vantagens **Desvantagens** Configurações de Exemplo de BD Externo Fluxo de trabalho da solução (pós-ISE 2.7) Configurações de Exemplo de BD Externo Usar BD Interno Fluxo de trabalho da solução Vantagens **Desvantagens** Configurações de Exemplo de BD Interno Conclusão Informações Relacionadas Glossário

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 accessaccept 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 máximo de regras de autenticação

Número máximo de regras de autorização

Número da escala 1000 (modo de definição de política) 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 Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed ABC E

	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
DEF- Policy	Se AD-Group FOR IGUAL A domain.com/groups/DEF EM SEGUIDA
	SGT:C2S-DEF E VLAN:1022
	Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed
Dolítico	E
GHI	Se AD-Group FOR IGUAL A domain.com/groups/GHI EM SEGUIDA
	SGT:C2S-GHI E VLAN:1023
	Se o AnyConnect EQUALIZAR User-AND-Machine-Both-Passed E
Politica XYZ	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 REC 2865	_
Logon Único (SSO) SAML (Security Assertion	n 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 Conr	nectivity (ODBC)
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracla	Enterprise Edition Versão
Oldcle	12.1.0.2.0
PostgreSQL	9
Sybase	16
MySQL	6.3
Login social (para contas de usuário convidad	do)
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.

🚪 New Database							. 🗆 ×
Select a page	🔄 Script 👻 📑 H	lelp					
General							
Flegroups	Database name:		ISEDB				
	Owner:		<default></default>				
	Use full-text in	ndexing					
	Database files:	CL T	0	1.2.1	A	[
	Logical Name	He lype	Hiegroup	Intial	Autogrowth	Path	
	ISEDB log	Rows Data	Not Apoli	1	By 1 MB, unrestricted gro	C:\Program Files\Microsoft SQL Server\	MS
	ISEDB_log	Log	Not Appl		by to percent, unrestrict	C. Grogram Hies Wicrosoft Solt Solt Server of	n.ə
Connection Server: localhost Connection: BABALAND\administrator							
Progress							
Ready	•					Add Remove	
						OK Cano	el /

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

🔆 WIN-R4PMESFSC16\INFY_MS_SQL_SERV.INFY_DB - dbo.Table_2* - Microsoft SQL Server Management Studio (Administrator) 📃							
Ele Edit View Project Debug Table Designer Tools	s	<u>W</u> indow <u>H</u> elp					
i 🛅 = 🗁 = 😂 🛃 🥔 🔔 New Query 📑 📸 📸 🍇 💺 🎕 隆 🔊 = 🗠 = 💷 = 🖳 🚳 🕨 = 🙄							
i 🕰 🕴 🛹 🐖 🐘 📰 🗱 📮							
Object Explorer 👻 무 🗙	WIN	I-R4PMESFSC16\INY_DB	- dbo.Table_2	2* ×			-
Connect 🕶 🛃 🗒 🔳 🍸 🧟		Column Name	Data T	ype	Allow Nulls		
🖃 🐻 WIN-R4PMESFSC16\INFY_MS_SQL_SERV (SQL 🔺		Username	varchar(MA	XX)			
🖃 🚞 Databases		VLAN	varchar(MA	X)			
🛨 🚞 System Databases		ProjectId	varchar(MA	X)			
🛨 🧰 Database Snapshots		UserGroup	varchar(M/	N)			
	-	oscroroup	Val Char (Ph	~,			
Database Diagrams							
- Indies							
System Tables	-						
The rapies	C	olumn Properties					
T i Views	ALL INT						
🕀 🧰 Synonyms	Z +						
🕀 🚞 Programmability	🗆 (General)					- -	
🕀 🧰 Service Broker	(Name) UserGroup						
🕂 🧰 Storage		Allow Nulls		Yes			
Security		Data Type		varchar(MAX)		
🕀 🧰 Users		Default Value or Binding					
	E	Table Designer					
🕀 🦲 Schemas		Collation		<databa< td=""><td>se default></td><td></td><td></td></databa<>	se default>		
Asymmetric Keys		(General)					
Certificates							
Symmetric Keys							
Database Audit Specifications							

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.

Identities Groups External Identit	y Sources Identity Source Seque	nces + Settings			
External Identity Sources	ODBC List > New ODBC Identity General * Name S Description	ODBC Identity Source Connection	Stored Procedures	Attributes	Groups
ODBC List > ISE_ODBC					
ODBC Identity Source	e Connection	Stored Procedure	s At	tributes	Groups
ODBC DB connection de	etails				
* Hostname/IP[:port]	bast-ad-ca.cisco.con	n			
* Database name	ISEDB				
Admin username	ISEDBUser		Ð		
Admin password					
* Timeout	5				
* Retries	1	Connectio	n succeeded		×
* Database type	Microsoft SQL Serv	Stored Proc	edures		
	Test Connection	 Plain text Plain text Plain text Check use Fetch grou Fetch attri 	password auth password fetcl ername or mac ups - Not Conf butes - Not Co	nentication - No hing - Not Con chine exists - N igured onfigured	ot Configured figured lot Configured Close

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

ODE OD	BC List > SDA_SQ BC Identity S General	eL ource Connection	Stored Procedures	Attributes		Groups	
	Stor Plain text passw Plain text Check username	vord authentication password fetching e or machine exists	Returns recordset	•	⊕ ⊕		
	Fetch groups Fetch attributes Search for MAC Address in format		SGTRetrieval xx-xx-xx-xx-xx	(((•		

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

m Python and Data : SQL S : X 32 Configure ISE 2.1 with M : X 2 Configure ISE 2.1 with M : X					
← → C 🗛 Not secure 🖛 🛠 //10.82.72.34/admin/#administration/administration_identitymanagement/administration_identitymanagement_external					
off-off- dentity Services Engine Home + Context Visibility + Operations + Policy Administration + Work Centers					
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC Clock In	re to do wireles				
Identities Groups External Identity Sources Identity Source Sequences + Settings					
External Identity Sources Image: Second Logic Contracts Additionations Purpling <					

eta _L_add _	¥ Delete									
Name	A DONNO	Туре		Default Valu	e	Name in ISE				
					No data a	vailable				
		ſ	Select Attribute	s from ODBC					x	
			Sample User or M	achine test1		(i) F	tetrieve Attributes	1		
			Nama	Tune	Default Value	Nor	io io ISE	,	_	
			sgt	STRING	1	sgt	e in ise			
									- 1	
									- 1	
									- 1	
									- 1	
		-								
								ОК	ncel	
									_ 1	O Los

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-avpair.** Selecione os valores como <name of ODBC database>:sgt e salve-o.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ient Provisioning - Policy Elements
Dictionaries + Conditions - Result	\$
0	Authorization Profile
▶ Authentication	* Name SQL_AuthZ
- Authorization	Description
Authorization Profiles	*Access Type ACCESS_ACCEPT *
Downloadable ACLs	Network Device Profile dith Cisco v 🕀
▶ Profiling	
	Service template
▶ Posture	
Client Provisioning	Passive identity frackling
	* Common Taske
	Security Group
	VLAN Tag ID 1 Edit Tag ID/Name 100
	- Vicina Descrite Descriterion
	Web Redirection (CWA, MDM, NSP, CPP) ()
	Advanced Attributes Settings
	Cisco:cisco-av-pair 💟 = SDA_SQL:sgt 💟 = +
	 Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) () Advanced Attributes Settings Cisco:cisco-av-pair () = SDA_SQL:sgt () + +

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.

office entre	Identity	y Serv	vices Engine Home +	Context VI	Operations Policy Administration Work Centers			🕕 🛛 License Warning 🔺 🕬	. o	• •
*No	Notwork Access Outst Access Outst Access Notwork Outst Access Outst Access Notwork Outst Access Outst Acc									
• Or	Overview Identifies Id Oncups Ed Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports Settings Dictionaries Authomation Princy - Local Exceptions									
> ^	uthoriza	tion P	Policy - Global Exceptions							
*^	uthoriza	tion P	Policy (18)							
6							Results			
G	Sti	atus	Rule Name	Cond			Profiles	Security Groups	Hits	Actions
De	Seath									
	⊘ sol_Aumz		0/1 4-87	Network Access NetworkDeviceName EQUALS INFY_SQL_DB/ND0			(voi 4.07) 4	Calad Bran Sel		~
			Carl Conner	AND	Network Access AuthenticationStatus EOUALS AuthenticationPassed	indicationPassed			0	**

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:f7:31:5 b: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.

E Cisco ISE	Administration - Identity Management
Identities Groups External Identities	entity Sources Identity Source Sequences Settings
External Identity Sources <	ODBC List > SDA_SQL ODBC Identity Source General Connection Stored Procedures Attributes Groups
 Active Directory LDAP ODBC SDA_SQL RADIUS Token RSA SecurID SAML Id Providers Social Login 	* Name SDA_SQL Description

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

E Cisco ISE	Administration - Identity Management
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings
External Identity Sources	ODBC List > SDA_SQL ODBC Identity Source General Connection Stored Procedures Attributes Groups
Active Directory	
LDAP	Stored procedure type Returns recordset V
V 🗁 ODBC	Plain text password authentication ISEAuthUser 🕕 🕀
👻 SDA_SQL	Ptain text password fetching ISEFetchPassword ()
🖹 RSA SecuriD	Check username or machine exists
 SAML Id Providers Social Login 	Fetch groups () ()
	Fetch attributes O O Advanced Settings O
	Search for MAC Address in formatxx-xx-xx-xx

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

■ Cisco ISE	Administration - Identity Management
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings
External Identity Sources < Image: Certificate Authentication F	COBC List > SDA_SQL ODBC Identity Source General Connection Stored Procedures Attributes Groups
Active Directory	🖉 Edit 🕂 Add 🔿 🎯 Delete
	Select Attributes from ODBC Default Value Name in ISE
🔁 SDA_SQL	No data av Add Attribute
RADIUS Token	
C RSA SecurID	
SAML Id Providers	
🗀 Social Login	

E Cisco ISE			Administration • Ider	ntity Management	
Identities Groups External Ide	entity Sources Identity S	ource Sequences	Settings		
External Identity Sources < Image: Source and S	ODBC List > SDA_SQL ODBC Identity Source General Connection	Stored Procedures	Attributes Groups		
	Edit + Add V	Type	Default Value	Name in ISE	
SDA_SQL	VianName	STRING		vlan	
C RADIUS Token	sgt	STRING	1	sgt	
 RSA SecuriD SAML Id Providers Social Login 					

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-avpair.** 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

E Cisco ISE	Policy - Policy Elements
Dictionaries Conditions	Results
Authentication	Authorization Profile
Authorization \sim	* Sane SQL_Autra
Authorization Profiles	Desirgion
Downloadable ACLs	*Access Type ACCESS_ACCEPT V
Profiling	Network Davice Ruffles 🚊 Class 🗸 👳
Posture	Sanice Template
Client Provisioning	Track Movement 🛛 🖸
	Passive species 0 V.Common Tasks V.LNN
	✓ Advanced Attributes Settings E Ciscolston-av-pair ✓ * SDA_SOC.spt ✓ = +
	✓ Attributes Details Access Type + ACX85, ACX07T Turnet-InvestGrape 0 = 1:50A 50.v/en
	fund bye 113
	Turnet Hadus-Type - 1.6
	coore-angel = SQA SQL-spt

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.

≡ Cisco ISE	Policy - Policy Sets		🛕 Evaluation Mode 19 Days 🤇	2 0	58 ¢
Policy Sets→ Default		Reset	Reset Policyset Hitcounts		Save
Status Policy Set Name Description Conditions			Allowed Protocols / Server	Sequen	ce Hits
Q Search					
Default Default policy set			Default Network Access	∞ ~	+ 0
> Authentication Policy (3)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
\sim Authorization Policy (13)					
		Results			
Status Rule Name Conditions		Profiles Secur	ity Groups	Hits	Actions
Q Search					
SQL_Authz Authz SQL_Authz Authz Aut		SQL_Authz × + Sele	ct from list \sim +	0	\$

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.



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(Cor ento)	^{nprim} 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.

-the Identity Services Engine Home + Context	Visibility	ministration	License Warning 🔺 🤇	l 🛛 🔿 🌣
System Identity Management Network Resources	Device Portal Management pxGrid Services	Feed Service Threat Centric NAC		
Identities Groups External Identity Sources Identity S	ource Sequences - Settings			
User Custon	Attributes			
User Custom Attributes	Attibutes			
User Authentication Settings Predefined	User Attributes (for reference)			Total 9 🥵 🎡 🖕
Endpoint Purce			Show All	- 5
Endepint Custom Attributes Mandatory	Attribute Name	▲ Data Type		
Endpoint Castom Attributes	AllowPasswordChangeAfterLogin	String		
	Description	String		
	EmailAddress	String		
	EnableFlag	String		
	EnablePassword	String		
	Firstname	String		
	Lastname	String		
	Name	String		
	Password (CredentialPassword)	String		
▼ User Custom	Attributes			
Attribute Name	Description	Data Type Parameters	Default Value	Mandatory
vlan	Vlan details of the User	String v Max length : 100	4 C2S	□ —
sgt	SGT detail of the User	String + Max length : 100	Cts:security-grou	+
Save Reset				

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.

AtributoValorCisco:cisco-av-pairInternalUser:sgtRadius:Tunnel-Private-Group-IDInternalUser:vlanRaio:Tipo De Meio De Túnel802Raio:Tipo De TúnelVLAN

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.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ient Provisioning Policy Elements
Dictionaries + Conditions - Result	8
0	Authorization Profiles > New Authorization Profile
Authentication	Authorization Profile
- Authorization	*Name Internal_user
	Description
Authorization Profiles	*Access Type ACCESS_ACCEPT *
Downloadable ACLs	Network Device Profile 🛛 🎰 Cisco 💌 🕀
	Service Template
Posture	Track Movement 🗐 🕧
Client Provisioning	Passive Identity Tracking 📋 🕧

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

sco Ide	entity Serv	vices Engine	Home	Context Visib	ility • Operations	- Policy	 Administration 	 Work Centers 			License Warning					
Policy Se	ts Profil	ing Posture	Client Provisio	ning + Policy	/ Elements											
earch																
	0	Policy-1				₽ (DEVICE-Device Type EC	UALS All Device Types			Default Network Acr	699	×	• +		51
Auth	entication	Policy (3)														
Auth	orization F	Policy - Local Ex	ceptions													
Auth	orization F	Policy - Global E	xceptions													
Autho	orization F	Policy (3)														
								Results								
Ŧ	Status	Rule Name		Conditio	ons			Profiles	Profiles Security (Hits	Acti	or
Search	1															
	Ø	internal-users Ar	uthz		Network Access-EapChe both succeeded	ainingResult	EQUALS User and man	hineuser	+	Select from	ı list	-	F	2	*	¥
	ø	Machine Authz		-ata - 2	MyAD-ExternalGroups I Computers	EQUALS gd	c.security.com/Users/Do	main PermitAccess	•	Select from) list	× •	F	2	*	¥
	Ø	Default						× DenyAccess	+	Select from	i list	-	F	3	4	ž
													D.	osot		

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.

dentity s	Services Engine	Home	e Contex	t Visibility → Opera	ations	Policy A	dministration	• Work Cer	nters		License Wa	iming 🔺			•	
► System -	Identity Management	▶ Netv	vork Resources	 Device Portal Ma 	nagement	pxGrid Service	es 🕨 Feed	Service + Thr	eat Centric NAC							
+ Identities G	Broups External Iden	tity Sour	rces Identity	Source Sequences	 Settings 											
0																
Users		Ne	twork Acces	s Users									Selected	I O Total !	s 🛞 i	ê.
Latest Manual Ne	twork Scan Results	1	Edit 🕂 🕂 Add	Change Status 👻	Import	t 🕞 Export 👻	X Delete	Duplicate			Show	All			•	8
			Status	Name	-	Description		First Name	Last Name	Email Address		User Iden	tity Grou	ips	Adn	nin
			Enabled	2 Aravind								Bangalore				
			Enabled	🧕 Jinkle								Bangalore				
			Enabled	🧕 jitchand								Bangalore				
			Enabled	9 Mnason								Chennai				
			Enabled	9 Vinodh								Bangalore	,Chenna	i		

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.

-shaft- case Identity Services Engine Home + Context Visibility + Operations + Policy *Administration + Work Contexs License Warnin	a 🔺	$\mathbf{Q}_{\mathbf{k}}$	•	•	•		
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC							
tidentities Groups External identity Sources Identity Source Sequences + Settings							
0							
Uters Vietwork Access List > Justee							
Latest Manual Network Scan Results							
"Name Jinke	*Name 2nkie						
Status 📴 Enabled +	Status 🥑 Enabled *						
Email							
* Passwords							
Pessword Type: MyAD *							
Password Re-Enter Password							
*Lonin Pressword @							
Eastha Danaward							
User Information	➤ User Information						
Account Options							
Account Disable Policy							
 User Custom Attributes 							
vlan - 525							
sgt = [cta:security-group-tag=0005-1							
	✓ User Groups						
Emplore	Elengatore						
Save Reset							

Passo 5: Verifique os logs dinâmicos:

C R	Refresh O Reset Repest	Counts 🚨 Export	To 🕶									7	Filter • •
	Time	Status	Detail	s Repeat	Identity		Endpoint	ID	Endpoint Pr	ofile Authentication Po	Authorization Polic	y Authorizat	IP Address
×					Identity		Endpoint	D	Endpoint Pro	fie Authentication Policy	Authorization Policy	Authorizati	IP Address
	Oct 28, 2019 06:40:05.068	РМ 🕕	0	1	host/POD2-CLIEN	T1	00:50:56:8	0:C8:DF	VMWare-Devi	Policy-1 >> Dot1x	Policy-1 >> Machine A	uthz PermitAcce	172.16.2.1
	Oct 28, 2019 06:40:05.048	PM 🗹	0		host/POD2-CLIEN	T1	00:50:56:8	0:C8:DF	VMWare-Devi	ce Policy-1 >> Dot1x	Policy-1 >> Machine A	uthz PermitAcce	is 172.16.2.1
Time	ê	Status	Details	Repeat	dentity	Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network Dev
		٣			Identity	Endpoint ID		Endpoint Profi	Authentication	Authorization Policy	Authorization	IP Address	Network Devi
Oct 2	29, 2019 10:23:33.877 AM	٠	a	1 1	araravic,host/POD	00:50:56:80.C	8:DF	VMWare-De	Policy-1 >>	Policy-1 >> Internal-users Auth	z Internal_user	172.16.2.1	
Oct 2	29, 2019 10:23:33.877 AM	.	ò		araravic,host/POD	00:50:56:80.C	8:DF	VMWare-De	Policy-1 >>	Policy-1 >> Internal-users Auth	z Internal_user	172.16.2.1	POD2-ACCES

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

Result	
User-Name	araravic
Class	CACS:AC1002320000E5E815DA26BA:pod2ise6/361122903/4422
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:d 8: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	848A
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

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

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

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.