Politique d'accès simplifiée avec ODBC et base de données ISE (attribut personnalisé) pour les réseaux de campus à grande échelle

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales **Tendances technologiques** Problème Solution proposée Configuration avec une base de données externe Exemples de configuration ODBC Workflow de la solution (ISE 2.7 et versions antérieures) **Avantages Inconvénients** Exemples de configurations de base de données externe Workflow de la solution (après ISE 2.7) Exemples de configurations de base de données externe Utiliser la base de données interne Workflow de solution **Avantages** Inconvénients Exemples de configurations de base de données interne Conclusion Informations connexes Glossaire

Introduction

Ce document décrit le déploiement de campus à grande échelle sans compromettre ses fonctionnalités et l'application de la sécurité. La solution de sécurité des terminaux de Cisco, Identity Services Engine (ISE), répond à cette exigence en intégrant une source d'identité externe.

Pour les réseaux à grande échelle comportant plus de 50 géolocalisations, plus de 4 000 profils d'utilisateurs différents et 600 000 terminaux ou plus, les solutions IBN traditionnelles doivent être considérées sous un angle différent : plus que de simples fonctionnalités, qu'elles s'adaptent à toutes les fonctionnalités. La solution IBN (Intent-Based Network) dans les réseaux traditionnels à grande échelle d'aujourd'hui nécessite de se concentrer davantage sur l'évolutivité et la facilité de gestion, et pas seulement sur ses fonctionnalités.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine (ISE) version 2.6, correctif 2 et version 3.0
- Windows Active Directory (AD) Server 2008 version 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. Si le réseau est actif, assurez-vous de comprendre l'impact potentiel de toute configuration.

Informations générales

Dans une solution de réseau basé sur l'identité (IBN), les éléments de base sont le demandeur, l'authentificateur et le serveur d'authentification (AAA). Le demandeur est un agent sur le terminal qui fournit les informations d'identification lorsqu'il est sollicité pour l'accès au réseau. Authenticator ou NAS (Network Access Server) est la couche d'accès, qui comprend les commutateurs réseau et les WLC qui transportent les informations d'identification vers le serveur AAA. Le serveur d'authentification valide la demande d'authentification utilisateur par rapport à un magasin d'ID et l'autorise avec un access-accept ou un access-reject. Le magasin d'ID peut se trouver sur le serveur AAA ou sur un serveur dédié externe.

Cette image présente les éléments IBN de base.



RADIUS est un protocole basé sur le protocole UDP (User Datagram Protocol) avec authentification et autorisation couplées. Dans la solution IBN de Cisco pour campus d'entreprise, le personnage PSN (Policy Service Node) d'ISE agit en tant que serveur AAA qui authentifie les terminaux par rapport à l'ID Store d'entreprise et autorise en fonction d'une condition.

Dans Cisco ISE, les stratégies d'authentification et d'autorisation sont configurées pour répondre à ces exigences. Les stratégies d'authentification comprennent le type de support, filaire ou sans fil, et les protocoles EAP pour la validation utilisateur. Les politiques d'autorisation sont constituées de conditions qui définissent les critères de correspondance des différents terminaux et les résultats d'accès au réseau, qui peuvent être un VLAN, une liste de contrôle d'accès téléchargeable ou une balise de groupe sécurisé (SGT). Il s'agit des valeurs d'échelle maximales pour les politiques avec lesquelles ISE peut être configuré.

Ce tableau présente l'échelle des politiques Cisco ISE.

Attribut	Numéro d'échelle
Nombre maximal de règles	1000 (mode Jeu de
d'authentification	strategies)
Nombre maximal de règles d'autorisation	3 000 (mode Jeu de stratégies) avec 3 200 profils Authz

Tendances technologiques

La segmentation est devenue l'un des principaux éléments de sécurité pour les réseaux d'entreprise actuels, sans qu'il soit nécessaire de mettre en place un véritable réseau de périphérie. Les terminaux sont autorisés à circuler entre les réseaux internes et externes. La segmentation permet de contenir toute attaque de sécurité sur un segment particulier afin de l'étendre au réseau. La solution Software-Defined Access (SDA) d'aujourd'hui, avec l'aide de TrustSec de Cisco ISE, permet de segmenter en fonction du modèle commercial du client afin d'éviter les dépendances sur des éléments de réseau tels que les VLAN ou les sous-réseaux IP.

Problème

Configuration des politiques ISE pour les réseaux d'entreprise à grande échelle avec plus de 500 profils de terminaux différents, le nombre de politiques d'autorisation peut augmenter jusqu'à un point ingérable. Même si Cisco ISE prend en charge des conditions d'autorisation dédiées pour répondre à un tel volume de profils utilisateur, la gestion de ce grand nombre de politiques par les administrateurs pose un défi.

En outre, les clients peuvent avoir besoin de politiques d'autorisation communes plutôt que de politiques dédiées pour éviter les frais de gestion et disposer d'un accès réseau différencié pour les terminaux en fonction de leurs critères.

Par exemple, considérez un réseau d'entreprise avec Active Directory (AD) comme **source de vérité** et le différenciateur unique du terminal est l'un des attributs dans AD. Dans ce cas, la méthode traditionnelle de configuration des stratégies comporte davantage de stratégies d'autorisation pour chaque profil de point de terminaison unique.

Dans cette méthode, chaque profil de point de terminaison est distingué avec un attribut AD sous domain.com. Par conséquent, une stratégie d'autorisation dédiée doit être configurée.

Ce tableau présente les stratégies AuthZ traditionnelles.

	Si AnyConnect est égal à User-AND-Machine-Both-Passed
Delitique	ET
Politique	Si Groupe AD EST ÉGAL À domain.com/groups/ABC
ADC	ALORS
	SGT:C2S-ABC ET VLAN:1021
politique	Si AnyConnect est égal à User-AND-Machine-Both-Passed
d'aide aux	ET
pays en	Si Groupe AD EST ÉGAL À domain.com/groups/DEF
développe	ALORS
ment	SGT:C2S-DEF ET VLAN:1022
	Si AnyConnect est égal à User-AND-Machine-Both-Passed
Politique	ET
CHI	Si Groupe AD EST ÉGAL À domain.com/groups/GHI
UIII	ALORS
	SGT:C2S-GHI ET VLAN:1023
	Si AnyConnect est égal à User-AND-Machine-Both-Passed
Politique	ET
XV7	Si Groupe AD EST ÉGAL À domain.com/groups/XYZ
X12	ALORS
	SGT:C2S-XYZ ET VLAN:1024

Solution proposée

Pour contourner la violation du nombre maximal évolutif de politiques d'autorisation prises en charge sur Cisco ISE, la solution proposée consiste à utiliser une base de données externe qui autorise chaque terminal avec le résultat d'autorisation extrait de ses attributs. Par exemple, si AD est utilisé en tant que base de données externe pour l'autorisation, tous les attributs utilisateur inutilisés (comme le service ou le code PIN) peuvent être référencés pour fournir des résultats autorisés mappés avec SGT ou VLAN.

Cela est possible grâce à l'intégration de Cisco ISE avec une base de données externe ou dans la base de données interne d'ISE configurée avec des attributs personnalisés. Cette section explique le déploiement de ces 2 scénarios :

Note: Dans les deux options, la base de données contient l'ID utilisateur mais pas le mot de passe des points d'extrémité DOT1X. La base de données est utilisée comme point d'autorisation uniquement. L'authentification peut toujours être le magasin d'ID du client qui, dans la plupart des cas, réside sur le serveur Active Directory (AD).

Configuration avec la base de données externe

Cisco ISE est intégré à une base de données externe pour la validation des identifiants de terminal :

Ce tableau présente les sources d'identité externe validées.

Source d'identité externe	OS/Version
Active Directory	
Microsoft Windows Active Directory 2003	—
Microsoft Windows Active Directory 2003 R2	—
Microsoft Windows Active Directory 2008	—

Microsoft Windows Active Directory 2012 — Microsoft Windows Active Directory 2012 R2 — Microsoft Windows Active Directory 2016 — Serveurs LDAP Serveur d'annuaire LDAP SunONE Version 5.2 Serveur d'annuaire OpenLDAP Version 2.4.23 Tout serveur compatible LDAP v3 — Serveurs de jetons RSA ACE/Server Série 6.x RSA Authentication Manager Séries 7.x et 8.x Tout serveur de jeton compatible RADIUS RFC 2865 Authentification unique (SSO) SAML (Security Assertion Markup Language) Microsoft Azure — Oracle Access Manager (OAM) Version 11.1.2.2.0 Oracle Identity Federation (OIF) Version 11.1.1.2.0 Serveur PingFederate Version 6.10.0.4 Cloud PingOne — Authentification sécurisée 8.1.1 Tout fournisseur d'identité conforme à
Microsoft Windows Active Directory 2012 R2 — Microsoft Windows Active Directory 2016 — Serveurs LDAP Serveur d'annuaire LDAP SunONE Version 5.2 Serveur d'annuaire OpenLDAP Version 2.4.23 Tout serveur compatible LDAP v3 — Serveurs de jetons RSA ACE/Server Série 6.x RSA Authentication Manager Séries 7.x et 8.x Tout serveur de jeton compatible RADIUS RFC 2865 Authentification unique (SSO) SAML (Security Assertion Markup Language) Microsoft Azure — Oracle Access Manager (OAM) Version 11.1.2.2.0 Oracle Identity Federation (OIF) Version 11.1.1.2.0 Serveur PingFederate Version 6.10.0.4 Cloud PingOne — Authentification sécurisée 8.1.1 Tout fournisseur d'identité conforme à
Microsoft Windows Active Directory 2016—Serveurs LDAPVersion 5.2Serveur d'annuaire LDAP SunONEVersion 2.4.23Serveur d'annuaire OpenLDAPVersion 2.4.23Tout serveur compatible LDAP v3—Serveurs de jetons—RSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS—RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Serveurs LDAPServeur d'annuaire LDAP SunONEVersion 5.2Serveur d'annuaire OpenLDAPVersion 2.4.23Tout serveur compatible LDAP v3—Serveurs de jetons—RSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS—RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Serveur d'annuaire LDAP SunONEVersion 5.2Serveur d'annuaire OpenLDAPVersion 2.4.23Tout serveur compatible LDAP v3—Serveurs de jetons—RSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS—RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Serveur d'annuaire OpenLDAPVersion 2.4.23Tout serveur compatible LDAP v3—Serveurs de jetons—RSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Tout serveur compatible LDAP v3—Serveurs de jetonsSérie 6.xRSA ACE/ServerSéries 7.x et 8.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Serveurs de jetonsRSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS—RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
RSA ACE/ServerSérie 6.xRSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS RFC 2865Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft AzureOracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOneAuthentification sécurisée8.1.1Tout fournisseur d'identité conforme à
RSA Authentication ManagerSéries 7.x et 8.xTout serveur de jeton compatible RADIUS RFC 2865Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft AzureOracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOneAuthentification sécurisée8.1.1Tout fournisseur d'identité conforme à
Tout serveur de jeton compatible RADIUS RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
RFC 2865—Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Authentification unique (SSO) SAML (Security Assertion Markup Language)Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Microsoft Azure—Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Oracle Access Manager (OAM)Version 11.1.2.2.0Oracle Identity Federation (OIF)Version 11.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Oracle Identity Federation (OIF)Version 11.1.1.2.0Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à—
Serveur PingFederateVersion 6.10.0.4Cloud PingOne—Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à
Cloud PingOne — Authentification sécurisée 8.1.1 Tout fournisseur d'identité conforme à
Authentification sécurisée8.1.1Tout fournisseur d'identité conforme à
Tout fournisseur d'identité conforme à
SAMLv2
Source d'identité ODBC (Open Database Connectivity)
Microsoft SQL Server (MS SQL) Microsoft SQL Server 2012
Oracle Enterprise Edition version
12.1.0.2.0
PostgreSQL 9
Sybase 16
MySQL 6.3
MySQL 6.3 Connexion sociale (pour les comptes d'utilisateurs invités)

Exemples de configuration ODBC

Cette configuration est effectuée sur Microsoft SQL pour créer la solution :

Étape 1. Ouvrez SQL Server Management Studio (**menu Démarrer > Microsoft SQL Server**) pour créer une base de données :



Étape 2. Entrez un nom et créez la base de données.

New Database							_ 🗆 ×
Select a page	🖳 Script 👻 📑 Help						
General							
Coptions	Database name:		ISEDB				
in the groups	Owner:		<default></default>				
	Use full-text index	ang					
	Database files:						
	Logical Name File	Tune	ilearoun	lotial	Autogrowth	Path	
	ISEDB Bo	ws Data P	PRIMARY	2	By 1 MB unrestricted aro	C:\Program Files\Microsoft SQL Serve	ar\MS
	ISEDB log Lo	a N	Not Apoli	1	By 10 percent, unrestrict	C:\Program Files\Microsoft SQL Serve	ar\MS
Connection							
Server:							
localhost							
Connection: BABALAND\administrator							
Wew connection properties							
Progress							
Ready	•						•
Wear and a second secon						Add Bemoy	e
							1 1000

Étape 3 : création d'une table avec les colonnes requises comme paramètres pour les points de terminaison autorisés

🔆 WIN-R4PMESFSC16\INFY_MS_SQL_SERV.INFY_DB - dbo.Table_2* - Microsoft SQL Server Management Studio (Administrator)							_ 8 ×
Eile Edit View Project Debug Table Designer Tool	ls	Window Help					
: 🛅 🕶 📨 📂 🚚 🥥 🗳 New Ouery 🛛 📭 🐴 🐴	572	X = = - 0				- <u>-</u>	
			~				
Object Explorer 🛛 🝷 부 🗙	WI	N-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	AX)			
🖃 🚞 Databases		VLAN	varchar(MA	AX)			
🛨 🚞 System Databases		ProjectId	varchar(MA	AX)			
Database Snapshots	Þ	UserGroup	varchar(MA	(X)	V		
E INFY_DB	÷						
Tables							
System Tables							
FileTables	-						
🗊 dbo.Table 1	C	olumn Properties					
+ 🔁 Views	1						
🕀 🚞 Synonyms							
🛨 🪞 Programmability	E	🗄 (General)					-
🕀 🧰 Service Broker		(Name)		UserGrou	dr.		
🛨 🧰 Storage		Allow Nulls		Yes			
Security		Data Type		varchar(MAX)		
🕀 🚞 Users		Default Value or Binding					
	E	3 Table Designer					
🕀 🚞 Schemas		Collation		<databa< td=""><td>se default></td><td></td><td></td></databa<>	se default>		
🕀 🚞 Asymmetric Keys	(General)						
E Certificates							
🕀 🚞 Symmetric Keys							
🕀 📄 Database Audit Specifications 🗾	L						

Étape 4. Créez une **procédure** pour vérifier si le nom d'utilisateur existe.



Étape 5. Créez une procédure pour extraire des attributs (SGT) de la table.



Dans ce document, Cisco ISE est intégré à la solution Microsoft SQL pour répondre aux exigences d'évolutivité des autorisations sur les réseaux de grandes entreprises.

Workflow de la solution (ISE 2.7 et versions antérieures)

Dans cette solution, Cisco ISE est intégré à Active Directory (AD) et Microsoft SQL. AD est utilisé comme magasin d'ID d'authentification et MS SQL pour l'autorisation. Au cours du processus d'authentification, le périphérique d'accès réseau (NAD) transmet les informations d'identification de l'utilisateur au PSN, le serveur AAA de la solution IBN. PSN valide les informations d'identification d'identification du point de terminaison avec le magasin d'ID Active Directory et authentifie l'utilisateur. La politique d'autorisation se réfère à la base de données MS SQL pour récupérer les résultats autorisés comme SGT / VLAN pour lequel **user-id** est utilisé comme référence.





Avantages

Cette solution présente les avantages suivants, ce qui la rend flexible :

- Cisco ISE peut tirer parti de toutes les fonctionnalités supplémentaires que la base de données externe peut offrir.
- Cette solution ne dépend d'aucune limite d'évolutivité Cisco ISE.

Inconvénients

Cette solution présente les inconvénients suivants :

- Nécessite une programmation supplémentaire pour remplir la base de données externe avec des informations d'identification de point de terminaison.
- Si la base de données externe n'est pas présente localement comme les PSN, cette solution dépend du WAN, ce qui en fait le 3^e point de défaillance dans le flux de données AAA du point d'extrémité.
- Nécessite des connaissances supplémentaires pour gérer les processus et procédures de base de données externes.
- Les erreurs provoquées par la configuration manuelle de l'ID d'utilisateur dans la base de données doivent être prises en compte.

Exemples de configurations de base de données externe

Dans ce document, Microsoft SQL apparaît comme la base de données externe utilisée comme point d'autorisation.

Étape 1 : création du magasin d'identités ODBC dans Cisco ISE à partir du menu Administration >

External Identity Source > ODBC et test des connexions

External Identity Sources	a ⁿ a	ODBC List > New ODBC Identit	v ODBC Ider v Source	tity Source			
Certificate Authentication Profile Active Directory LDAP ODBC RADIUS Token RSA SecurID SAML Id Providers Social Login	<u>89</u> ≁	General * Name Description	Co	nnection	Stored Procedures	Attributes	Groups
DBC List > ISE_ODBC							
General General	a Connectio	n	Stored	Procedures	s At	tributes	Groups
ODBC DB connection de	etails						
* Hostname/IP[:port]	bast-ad	l-ca.cisco.co	m				
* Database name	ISEDB						
Admin username	ISEDBU	Jser			Ð		
Admin password	******	•					
* Timeout	5		Tes	t connec	tion		
* Retries	1			Connection	n succeeded		х
* Database type	Micros	oft SQL Ser	Sto	red Proc	edures	antiantian N	at Confirmed
	Test C	onnection		Plain text p Plain text p Check use Fetch grou Fetch attrit	bassword auth bassword fetch rname or mac ps - Not Confi butes - Not Co	entication - N iing - Not Cor hine exists - I gured nfigured	ot Configured Ifigured Not Configured

Étape 2. Accédez à l'onglet Procédures stockées de la page ODBC pour configurer les procédures créées dans Cisco ISE.

ODBC List > SDA_S ODBC Identity S General	QL Gource Connection	Stored Procedures	Attributes	Groups
Sto Plain text pass	word authentication	Returns recordset	•	
Plain tex Check usernam	e or machine exists		0 ⊕ 0 ⊕	
Search for MA	Fetch attributes	SGTRetrieval XX-XX-XX-XX-XX	(+	

Étape 3. Récupérez les attributs de l'ID utilisateur à partir de la source d'ID ODBC pour vérification.

Python and Data : SQL SI: X V & Configure ISE 2.1 with MI: X V & Identity Services Engine X	
← → C 🗛 Not secure bttps://10.82.72.34/admin/#administration/administration_identitymanagement/administration_identitymanagement_external	
alphalts Identity 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 Click here to do	wireles
Identities Groups External Identity Sources Identity Source Sequences Settings	
External Identity Sources Image: Source Conception of the Conceptice of the Conception of the Conceptice of t	

General	Connection	Sto	ored Procedures	Attributes	Groups				
Name	Desae	Туре		Default Value	No data av	Name in ISE allable			
			Select Attribute: Sample User or M	s from ODBC		 Retrieve / 	Attributes	x	
			□ Name ☑ sgt	Type STRING	Default Value	Sgt			
		-					ОК	Cancel	🕑 Location
Reset									Q Ner

Étape 4 : création d'un **profil d'autorisation** et configuration Dans Cisco ISE, accédez à **Policy > Results > Authorization profile > Advance Attributes Settings** et sélectionnez l'attribut en tant que **Cisco : cisco-av-pair.** Sélectionnez les valeurs en tant que <nom de la base de données ODBC> : sgt, puis enregistrez-le.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers									
Policy Sets Profiling Posture Cl	ient Provisioning -Policy Elements									
Dictionaries + Conditions - Result	S									
G	Authorization Profile									
Authentication	* Name SQL_AuthZ									
- Authorization	Description //									
Authorization Profiles	*Access Type ACCESS_ACCEPT *									
Downloadable ACLs	Network Device Profile 📾 Cisco 👻 🕀									
▶ Profiling	Convice Template									
	Service template									
▶ Posture										
Client Provisioning	Passive identity fracking									
	* Common Tasks									
	Security Group									
	VLAN Tag ID 1 Edit Tag ID/Name 100									
	Voice Domain Permission									
	Web Redirection (CWA, MDM, NSP, CPP) ()									
	Advanced Attributes Settings									
	Cisco:cisco-av-pair 🖸 = SDA_SQL:sgt 📀 — +									

Étape 5 : création d'une **stratégie d'autorisation** et configuration de celle-ci Dans Cisco ISE, accédez à **Policy > Policy sets > Authorization Policy > Add.** Placez la condition comme Identity

Source est le serveur SQL. Sélectionnez le profil Résultat comme profil d'autorisation créé précédemment.

-duals identity Services Engine Home + Cor	ted Visibility + Operations + Policy + Administration +Work Centers		Ucense Warning A 9.	•	• •
Network Access + Guest Access + TrustSec + I	BYOD + Profiler + Posture + Device Administration + PassiveID				
Oveniew Identities Id Oroups Et Id Sources Authonization Policy - Local Exceptions	Network Resources Policy Elements Policy Sets Proubleshoot Reports Settings Dictionaries				
Authorization Policy - Global Exceptions					
✓ Authorization Policy (18)					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search					
⊘ sol_kunz ,	AND L Network Access NetworkDeviceName EXXLS INFY_SOL_DBNDG	(×sqLAuftZ)	Select from list • •	0	¢

Étape 6. Une fois que l'utilisateur est authentifié et autorisé, les journaux contiennent la sgt attribuée à l'utilisateur, pour vérification.

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

Workflow de la solution (après ISE 2.7)

Après ISE 2.7, les attributs d'autorisation peuvent être récupérés à partir d'ODBC tels que Vlan, SGT, ACL et ces attributs peuvent être utilisés dans les stratégies.

Dans cette solution, Cisco ISE est intégré à Microsoft SQL. MS SQL est utilisé comme magasin d'ID pour l'authentification ainsi que pour l'autorisation. Lorsque les informations d'identification des points d'extrémité sont fournies à PSN, elles sont validées par rapport à la base de données MS SQL. La stratégie d'autorisation fait référence à la base de données MS SQL pour récupérer les résultats autorisés tels que SGT / VLAN pour lequel **user-id** est utilisé comme référence.



Exemples de configurations de base de données externe

Suivez la procédure fournie précédemment dans ce document pour créer MS SQL DB avec Username, Password, VLAN id et SGT.

Étape 1. Créez un magasin d'identités ODBC dans Cisco ISE à partir du menu Administration > External Identity Source > ODBC et testez les connexions.

E Cisco ISE	Administration - Identity Management
Identities Groups External Iden	ntity Sources Identity Source Sequences Settings
External Identity Sources	ODBC List > SDA_SQL ODBC Identity Source
> 🛅 Certificate Authentication F	General Connection Stored Procedures Attributes Groups
Active Directory LDAP	* Name SDA_SQL
	Description
RSA SecuriD	
SAML Id Providers	
🗀 Social Login	

Étape 2. Accédez à l'onglet Procédures stockées de la page ODBC pour configurer les procédures créées dans Cisco ISE.

E Cisco ISE Administration - Identity Management				
Identities Groups External Ide	tity Sources Identity Source Sequences Settings			
External Identity Sources < Image: Sources > Image: Sources > Image: Sources	ODBC List > SDA_SQL ODBC Identity Source General Connection Stored Procedures Attributes Groups			
 Active Directory LDAP 	Stared procedure type Returns recordset V			
V 🗂 ODBC	Plain text password authentication ISEAuthUser ()			
👻 SDA_SQL	Plain text password fetching ISEFetchPassword ()			
C RSA SecurID	Check username or machine exists			
🖻 SAML Id Providers	Fetch groups ISEGroups 🕕 🕀			
	Fetch attributes O D Advanced Settings			
	Search for MAC Address in format xx-xx-xx-xx-xx V			

Étape 3. Récupérez les attributs de l'ID utilisateur à partir de la source d'ID ODBC pour vérification.

E Cisco ISE	Administration - Identity Management
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings
External Identity Sources < Image: Control of the second sec	ODBC List > SDA_SQL ODBC Identity Source General Connection Stored Procedures Attributes Groups
Active Directory LDAP	Edit + Add ^ Delete Default Value Name In ISE
 SODBC SDA_SQL RADIUS Token RSA SecuriD SAML Id Providers Social Login 	Select Attributes from ODBC No data av Add Attribute

E Cisco ISE Administration - Identity Management					
Identities Groups External Ide	entity Sources Identity So	urce Sequences S	Settings		
External Identity Sources < Image: Control of the second sec	ODBC List > SDA_SQL ODBC Identity Source General Connection	Stored Procedures	Attributes Groups		
C LDAP	Name Name	Туре	Default Value	Name in ISE	
👻 SDA_SQL	VianName	STRING		vlan	
RADIUS Token	Sgt Sgt	STRING	1	sgt	
C RSA SecuriD					
SAML Id Providers					
🗀 Social Login					
I					

Étape 4 : création d'un **profil d'autorisation** et configuration Dans Cisco ISE, accédez à **Policy > Results > Authorization profile > Advance Attributes Settings** et sélectionnez l'attribut **Cisco : cisco-av-pair.** Sélectionnez les valeurs comme <nom de la base de données ODBC>:sgt. Sous Common Tasks, sélectionnez VLAN with ID/Name as <nom de la base de données ODBC>:vlan et enregistrez-le

E Cisco ISE	Policy - Policy Elements
Dictionaries Conditions	Results
Authentication >	Authorization Profile
Authorization \sim	*Name SQL_Autra
Authorization Profiles	Desription
Downloadable ADLs	*Access Type ACCESS_ACCEPT V
Profiling	National Device Profile (EDC) V 🔍
Posture >	Service temptas
Client Provisioning	Track Movement 🛛 🕕
	Agenties Pesture 🔲 🕐
	Passion learning hacking 🛛 🕐
	Common Tasks
	C VLAN Tag D 1 Edit Tag DA, SQL:Van V
	O vise Aumain Permaion
	Web Redressin (CMA, MOR, NSE, CPF)
	U Als Sext Pit
	✓ Advanced Attributes Settings
	■ <u>Oscolsco-w-part</u> v * <u>S0A_S0Lipt</u> v = +
	Attributes Details
	Access Type = ACCISS, ACCIF1
	Tamé Muste Group 20 = 1.526, SQL-Min
	Terrel Age + 1:13
	TamoHodum-type = 1.6
	000 w ptr = 300, 520, bpt

Étape 5 : création d'une **stratégie d'autorisation** et configuration de celle-ci Dans Cisco ISE, accédez à **Policy > Policy sets > Authorization Policy > Add.** Placez la condition comme Identity Source est le serveur SQL. Sélectionnez le profil Résultat comme profil d'autorisation créé précédemment.

≡ Cisco ISE	Policy · Policy Sets		Evaluation Mode 39 Days	୦ ଡ	58 ¢
Policy Sets→ Default		Re	Reset Policyset Hitcounts		Save
Status Policy Set Name Description Conditions			Allowed Protocols / Server	Seque	nce 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	Security Groups	Hits	Actions
Q Search					
SQL_Astric AND AND DEVICE-Device Type EQUALS All Device Types Network_Access_Authentication_Passed		$({\rm SQL}_{\rm a}{\rm Authz}\times)$	Select from list \sim +	0	ŵ

Utiliser la base de données interne

Cisco ISE possède lui-même une base de données intégrée qui peut être utilisée pour avoir des ID utilisateur pour l'autorisation.

Workflow de solution

Dans cette solution, la base de données interne de Cisco ISE est utilisée comme point d'autorisation tandis qu'Active Directory (AD) continue d'être la source d'authentification. L'ID utilisateur des terminaux est inclus dans la base de données Cisco ISE avec des **attributs personnalisés** qui renvoient les résultats autorisés tels que SGT ou VLAN. Lorsque les informations d'identification des terminaux avec le magasin d'ID Active Directory et authentifie le terminal. La stratégie d'autorisation fait référence à la base de données ISE pour extraire les résultats autorisés tels que SGT / VLAN pour lesquels l'ID d'utilisateur est utilisé comme référence.



Avantages

Cette solution présente les avantages suivants, ce qui en fait une solution flexible :

- La base de données Cisco ISE est une solution intégrée et n'a donc pas de 3^e point de défaillance, contrairement à la solution de base de données externe.
- Comme le cluster Cisco ISE assure la synchronisation en temps réel entre toutes les personnes, il n'y a pas de dépendance WAN, car le PSN dispose de tous les ID utilisateur et attributs personnalisés transmis par le PAN en temps réel.
- Cisco ISE peut tirer parti de toutes les fonctionnalités supplémentaires que la base de données externe peut offrir.
- Cette solution ne dépend d'aucune limite d'évolutivité Cisco ISE.

Inconvénients

Cette solution présente les inconvénients suivants :

- Le nombre maximal d'ID utilisateur que Cisco ISE DB peut refuser est de 300 000.
- Les erreurs provoquées par la configuration manuelle de l'ID d'utilisateur dans la base de données doivent être prises en compte.

Exemples de configurations de base de données interne

Les VLAN et SGT par utilisateur peuvent être configurés pour n'importe quel utilisateur dans le magasin d'ID interne avec un attribut utilisateur personnalisé.

Étape 1. Créez de nouveaux attributs personnalisés utilisateur pour représenter la valeur VLAN et SGT des utilisateurs respectifs. Accédez à **Administration > Identity Management > Settings > User Custom Attributes.** Créez de nouveaux attributs personnalisés utilisateur comme indiqué dans ce tableau.

Ici, la table de base de données ISE est affichée avec des attributs personnalisés.

Nom d'attribut	Type de données	Paramètres (longueur)	Valeur par défaut
vlan	Chaîne (string)	100	C2S (Nom De Vlan Par Défaut)
sgt	Chaîne (string)	100	cts : security-group- tag=0003-0 (valeur SGT par défaut)

• Dans ce scénario, la valeur VLAN représente le nom du VLAN et la valeur sgt représente l'attribut cisco-av-pair de SGT au format hexadécimal.

-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				

Étape 2 : création d'un profil d'autorisation avec des attributs utilisateur personnalisés pour impliquer les valeurs vlan et sgt des utilisateurs respectifs. Accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation > Ajouter.** Ajoutez les attributs mentionnés ci-dessous sous Paramètres d'attributs avancés.

Ce tableau présente le profil AuthZ pour l'utilisateur interne.

Attribut	Valeur
Cisco:paire-av-cisco	InternalUser:sgt
Radius:Tunnel-Private-Group-ID	InternalUser:vlan
Rayon:Tunnel-Medium-Type	802
Rayon:Type De Tunnel	VLAN

Comme l'illustre l'image, pour les utilisateurs internes, le profil **Internal_user** est configuré avec le SGT et le Vlan configurés en tant que **InternalUser:sgt** et **InternalUser:vlan** respectivement.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Elements
Dictionaries + Conditions - Resul	15
0	Authorization Profiles > New Authorization Profile
Authentication	Authorization Profile
- Authoritan	*Name Internal_user
* Authorization	Description
Authorization Profiles	* Access Type ACCESS_ACCEPT *
Downloadable ACLs	Natural Davisa Brafia da Cisca - 0
Profiling	
Posture	Service Template
	Track Movement 📋 🕧
Client Provisioning	Passive Identity Tracking 📋 🕧
	Common Tasks
	Advanced Attributes Settings
	Cisco:cisco-av-pair O = InternalUser:sgt O -
	Cisco:cisco-av-pair 💟 = InternalUser:vlan 💟
	Radius:Tunnel-Medium-Type 💟 = 802 💟
	reading: full the type
	Access Time = ACCESS ACCEPT
	recess rype = Access_recer r cisco-av-pair = InternalUser:sgt
	Tunnel-Medium-Type = :6
	turner-type = .10

Étape 3. Créez une stratégie d'autorisation, accédez à **Stratégie > Jeux de stratégies > Stratégie-1 > Autorisation.** Créez des stratégies d'autorisation avec les conditions mentionnées ci-dessous et mappez-les aux profils d'autorisation respectifs.

Ce tableau présente la stratégie AuthZ pour l'utilisateur interne.

Nom de règle	Condition	Résultat Authz Profile
Authentification_Utilis ateur_Interne	Si Network Access.EapChainingResults EST ÉGAL à Utilisateur et machine ont réussi	Utilisateur_interne
Machine_Only_Authz	Si MyAD.ExternalGroups EST ÉGAL À gdc.security.com/Users/Domain Ordinateurs	AutoriserAccès

; Ide	entity Serv	vices Engine	Home	 Context Vis 	ibility 🕨	Operations	→ Policy	+ Administral	tion	Work Centers			License Warning	A				
licy Se	ts Profil	ling Posture	Client Provisi	ioning 🕨 Poli	cy Elements													
arch																		
	0	Policy-1					₽	DEVICE Device Ty	pe EQU/	ALS All Device Types			Default Network A	ccess	3	x * +		1
Authe	entication	Policy (3)																
Autho	orization F	Policy - Local E	xceptions															
Autho	prization F	Policy - Global	Exceptions															
Autho	prization F	Policy (3)																
										Results								
+	Status	Rule Name		Condit	onditions					Profiles		Security G	Groups			Hits	Ac	ti
Search																		
	Ø	internal-users	Authz		Network Acc both succee	ess-EapChair ded	ningResult	EQUALS User an	nd machin	e vinternal_user	+	Select from	n list	*	÷	2		4
	Ø	Machine Authz		-18-	MyAD-ExternalGroups EQUALS gdc.security.co Computers			lc.security.com/Use	ers/Domai	n ×PermitAccess	+	Select from	n list	٣	+	2		¢
	Ø	Default								× DenyAccess	+	Select from	n list		+	3	1	¢
																Dogot		

Étape 4. Créez des identités d'utilisateur en masse avec des attributs personnalisés avec les détails de l'utilisateur et leurs attributs personnalisés respectifs dans le modèle CSV. Importez le fichier CSV en accédant à Administration > Identity Management > Identities > Users > Import > Choisissez le fichier > Import.

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 Net	twork Scan Results	1	Edit 🕂 🕂 Add	Change Status 👻	Import	t 🕞 Export 👻	X Delete				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		

Cette image présente un exemple d'utilisateur avec des détails d'attribut personnalisés. Sélectionnez l'utilisateur et cliquez sur Modifier pour afficher les détails d'attribut personnalisés mappés à l'utilisateur respectif.

-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					
Status 📴 Enabled +					
Email					
* Passwords					
Pessword Type: MyAD *					
Password Re-Enter Password					
*Lonin Pressword @					
Eastha Danaward					
User Information					
Account Options					
Account Disable Policy					
 User Custom Attributes 					
vlan - 525					
sgt = [cta:security-group-tag=0005-1					
Emplore					
Save Reset					

Étape 5 : Vérifiez les journaux actifs :

C	Refresh O Reset Repeat	Counts 🕹 Expor	t To 👻										₹ Fit	er- 0-
	Time	Status	Detai	is Repeat	t Identity		Endpoint	ID	Endpoint Pr	ofile Authentication Po	Authorization Polic	y Aut	horizati	IP Addres
×			*		Identity		Endpoint	ID	Endpoint Pro	file Authentication Policy	Authorization Policy	Aut	horization	IP Address
	Oct 28, 2019 06:40:05.066	РМ 🕕	0	1	host/POD2-CLIEN	T1	00:50:56:8	0:C8:DF	VMWare-Dev	e Policy-1 >> Dot1x	Policy-1 >> Machine A	kuthz Perr	nitAccess	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	ice Policy-1 >> Dot1x	Policy-1 >> Machine A	luthz Perr	nitAccess	172.16.2.1
Tim	e	Status	Details	Repeat	Identity	Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address		Network Dev
		٠			Identity	Endpoint ID		Endpoint Profi	Authentication	Authorization Policy	Authorization	IP Address	٠	Network Devi
Oct	29, 2019 10:23:33.877 AM		0	1	araravic,host/POD	00:50:56:80.Cl	8:DF	VMWare-De	Policy-1 >>	Policy-1 >> Internal-users Auth	z Internal_user	172.16.2.1		
Oct	29, 2019 10:23:33.877 AM	.	Q		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

Consultez la section **Result** pour vérifier si l'attribut **Vlan & SGT** est envoyé en tant que partie 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	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Conclusion

Cette solution permet à certains des clients des grandes entreprises de s'adapter à leurs besoins. L'ajout/la suppression d'ID utilisateur doit être effectué avec prudence. Les erreurs, si elles sont déclenchées, peuvent entraîner un accès non autorisé pour les utilisateurs authentiques ou vice versa.

Informations connexes

Configuration de Cisco ISE avec 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

Glossaire

Authentication Authorization Accounting
Active Directory
Authentification
Autorisation
Base de données
802.1X
Réseau basé sur l'identité
Base De Données D'Identité
Plateforme de services d'identité

MnT Surveillance et dépannage Microsoft SQL MsSQL Connectivité Open DataBase ODBC Noeud Administration de stratégie POÊLE PSN Noeud Services de stratégie SGT Balise Groupe sécurisé langage d'interrogation structuré SQL VLAN Réseau local virtuel Réseau réseau étendu WAN

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.