Vereinfachte Zugriffsrichtlinie mit ODBC und ISE DB (benutzerdefiniertes Attribut) für großes Campus-Netzwerk

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen **Technologietrends** Problem Vorgeschlagene Lösung Konfiguration mit externer DB **ODBC-Beispielkonfigurationen** Lösungs-Workflow (ISE 2.7 und früher) Vorteile Nachteile Externe DB - Beispielkonfigurationen Lösungs-Workflow (nach ISE 2.7) Externe DB - Beispielkonfigurationen Interne Datenbank verwenden Lösungs-Workflow Vorteile Nachteile Interne DB-Beispielkonfigurationen Schlussfolgerung Zugehörige Informationen Glossar

Einleitung

In diesem Dokument wird eine umfangreiche Campus-Bereitstellung ohne Kompromisse bei den Funktionen und der Durchsetzung von Sicherheitsrichtlinien beschrieben. Die Identity Services Engine (ISE), die Sicherheitslösung von Cisco für Endgeräte, erfüllt diese Anforderung durch die Integration in eine externe Identitätsquelle.

Bei großen Netzwerken mit mehr als 50 geografischen Standorten, mehr als 4.000 unterschiedlichen Benutzerprofilen und mehr als 600.000 Endpunkten müssen herkömmliche IBN-Lösungen aus einem anderen Blickwinkel betrachtet werden - mehr als nur Funktionen, unabhängig davon, ob sie mit allen Funktionen skalierbar sind. Die IBN-Lösung (Intent-Based Network) in herkömmlichen großen Netzwerken erfordert neben den Funktionen einen zusätzlichen Fokus auf Skalierbarkeit und einfaches Management.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 802.1x/MAB-Authentifizierung
- Cisco Identity Service Engine (Cisco ISE)
- Cisco TrustSec (CTS)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine (ISE) Version 2.6 Patch 2 und Version 3.0
- Windows Active Directory (AD) Server 2008 Version 2
- Microsoft SQL Server 2012

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn das Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen jeder Konfiguration kennen.

Hintergrundinformationen

Die grundlegenden Elemente einer Identity Based Network (IBN)-Lösung sind Supplicant, Authenticator und Authentication (AAA) Server. Der Supplicant ist ein Agent auf dem Endpunkt, der die Anmeldeinformationen bereitstellt, wenn der Netzwerkzugriff angefordert wird. Authenticator oder NAS (Network Access Server) ist die Zugriffsebene, die Netzwerk-Switches und WLCs umfasst, die die Anmeldeinformationen für den AAA-Server übertragen. Der Authentifizierungsserver validiert die Benutzerauthentifizierungsanforderung anhand eines ID-Speichers und autorisiert sie entweder durch Akzeptieren oder Ablehnen des Zugriffs. Der ID-Speicher kann sich im AAA-Server oder auf einem externen dedizierten Server befinden.

Dieses Bild zeigt die grundlegenden IBN-Elemente.



RADIUS ist ein UDP-basiertes Protokoll (User Datagram Protocol), bei dem Authentifizierung und Autorisierung miteinander verbunden sind. In der Cisco IBN-Lösung für Campus-Unternehmen

fungiert der Policy Service Node (PSN) der ISE als AAA-Server, der die Endpunkte anhand des Unternehmens-ID-Speichers authentifiziert und unter bestimmten Bedingungen autorisiert.

In der Cisco ISE werden Authentifizierungs- und Autorisierungsrichtlinien konfiguriert, um diese Anforderungen zu erfüllen. Die Authentifizierungsrichtlinien umfassen den Medientyp (kabelgebunden oder drahtlos) sowie die EAP-Protokolle für die Benutzervalidierung. Autorisierungsrichtlinien bestehen aus Bedingungen, die die Kriterien für die Übereinstimmung der verschiedenen Endpunkte und das Netzwerkzugriffsergebnis definieren. Dabei kann es sich um ein VLAN, eine herunterladbare ACL oder ein Secure Group Tag (SGT) handeln. Dies sind die maximalen Skalierungszahlen für Richtlinien, mit denen die ISE konfiguriert werden kann.

Diese Tabelle zeigt die Skalierung der Cisco ISE-Richtlinien.

Attribut	Skalierungszahl
Maximale Anzahl von Authentifizierungsregeln	1000 (Policy Set Mode)
Maximale Anzahl von Autorisierungsregeln	3.000 (Richtliniensatzmodus) mit 3200 Autz-Profilen

Technologietrends

Die Segmentierung hat sich zu einem der wichtigsten Sicherheitselemente für moderne Unternehmensnetzwerke entwickelt, ohne dass ein tatsächliches Edge-Netzwerk erforderlich ist. Die Endpunkte können zwischen internen und externen Netzwerken wechseln. Die Segmentierung hilft, alle Sicherheitsangriffe auf ein bestimmtes Segment einzudämmen, um das Netzwerk zu durchdringen. Die SDA-Lösung (Software-Defined Access) von heute bietet mithilfe von Cisco ISE TrustSec eine Möglichkeit zur Segmentierung auf Grundlage des Geschäftsmodells des Kunden, um Abhängigkeiten von Netzwerkelementen wie VLANs oder IP-Subnetzen zu vermeiden.

Problem

ISE-Richtlinienkonfiguration für große Unternehmensnetzwerke mit mehr als 500 unterschiedlichen Endgeräteprofilen - die Anzahl der Autorisierungsrichtlinien kann bis zu einem nicht zu verwaltenden Punkt ansteigen. Selbst wenn die Cisco ISE dedizierte Autorisierungsbedingungen unterstützt, um so viele Benutzerprofile zu verwalten, besteht die Herausforderung darin, diese Vielzahl an Richtlinien durch Administratoren zu verwalten.

Darüber hinaus benötigen Kunden ggf. gemeinsame Autorisierungsrichtlinien anstelle dedizierter Richtlinien, um Managementkosten zu vermeiden, und verfügen auf der Grundlage ihrer Kriterien über differenzierten Netzwerkzugriff für Endgeräte.

Betrachten Sie beispielsweise ein Unternehmensnetzwerk mit Active Directory (AD) als **Quelle der Wahrheit,** und das einzigartige Differenzierungsmerkmal des Endpunkts ist eines der Attribute in AD. In diesem Fall umfasst die herkömmliche Richtlinienkonfiguration mehr Autorisierungsrichtlinien für jedes einzelne Endgeräteprofil.

Bei dieser Methode wird jedes Endpunktprofil mit einem AD-Attribut unter domain.com unterschieden. Daher muss eine dedizierte Autorisierungsrichtlinie konfiguriert werden.

Diese Tabelle zeigt die traditionellen AuthZ-Richtlinien.

	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND
Richtlinie	Wenn AD-Gruppe GLEICH domain.com/groups/ABC DANN
	SGT:C2S-ABC UND VLAN:1021
	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND
Richtlinie	Wenn AD-Gruppe GLEICH domain.com/groups/DEF DANN
	SGT:C2S-DEF UND VLAN:1022
	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich UND
Richtlinie	Wenn AD-Gruppe GLEICH domain.com/groups/GHI DANN
	SGT:C2S-GHI UND VLAN:1023
	Wenn AnyConnect gleich Benutzer-UND-Maschine-beide-erfolgreich
XV 7	UND
Richtlinie	Wenn AD-Gruppe GLEICH domain.com/groups/XYZ DANN
	SGT:C2S-XYZ UND VLAN:1024

Vorgeschlagene Lösung

Um die Verletzung der maximal skalierbaren Anzahl unterstützter Autorisierungsrichtlinien auf der Cisco ISE zu umgehen, wird eine externe Datenbank vorgeschlagen, die die Autorisierung jedes Endpunkts mit dem aus den Attributen abgerufenen Autorisierungsergebnis vornimmt. Wenn AD beispielsweise als externe Datenbank für die Autorisierung verwendet wird, können alle nicht verwendeten Benutzerattribute (wie Abteilungs- oder Pin-Code) referenziert werden, um autorisierte Ergebnisse bereitzustellen, die mit SGT oder VLAN verknüpft sind.

Dies wird durch die Integration der Cisco ISE in eine externe Datenbank oder in die interne ISE-Datenbank erreicht, die mit benutzerdefinierten Attributen konfiguriert ist. In diesem Abschnitt wird die Bereitstellung dieser beiden Szenarien erläutert:

Anmerkung: In beiden Optionen enthält die DB die Benutzer-ID, aber nicht das Kennwort der DOT1X-Endpunkte. Die DB dient nur als Autorisierungspunkt. Die Authentifizierung kann weiterhin der ID-Speicher des Kunden sein, der sich in den meisten Fällen auf dem Active Directory (AD)-Server befindet.

Konfiguration mit externer DB

Die Cisco ISE ist zur Validierung der Endgeräteanmeldeinformationen in eine externe Datenbank integriert:

Diese Tabelle zeigt die validierten externen Identitätsquellen.

Externe IdentitätsquelleBetriebssystem/VersionActive DirectoryHicrosoft Windows Active Directory 2003—

Microsoft Windows Active Directory 2003 R2 Microsoft Windows Active Directory 2008 Microsoft Windows Active Directory 2008 R2 Microsoft Windows Active Directory 2012 Microsoft Windows Active Directory 2012 R2 Microsoft Windows Active Directory 2016 LDAP-Server	
SunONE LDAP-Verzeichnisserver	Version 5.2
OpenLDAP-Verzeichnisserver	Version 2.4.23
Jeder LDAP v3-kompatible Server	—
Token-Server	
RSA ACE/Server	Serie 6.x
RSA-Authentifizierungs-Manager	Serien 7.x und 8.x
Jeder RADIUS RFC 2865-kompatible	
Tokenserver	
Security Assertion Markup Language (SAML)	Single Sign-On (SSO)
Microsoft Azure	—
Oracle Access Manager (OAM)	Version 11.1.2.2.0
Oracle Identity Federation (OIF)	Version 11.1.1.2.0
PingFederate-Server	Version 6.10.0.4
PingOne Cloud	
Sichere Authentifizierung	8.1.1
Jeder SAMLv2-konforme Identitätsanbieter	
Open Database Connectivity (ODBC) Identity	Source
Microsoft SQL Server (MS SQL)	Microsoft SQL Server 2012
Oracle	Enterprise Edition Version
PostareSQL	9
Svbase	16
MySQI	6.3
Social Login (für Gastbenutzerkonten)	
Facebook	_

ODBC-Beispielkonfigurationen

Diese Konfiguration wird in Microsoft SQL durchgeführt, um die Lösung zu erstellen:

Schritt 1: Öffnen Sie SQL Server Management Studio (**Startmenü > Microsoft SQL Server**), um eine Datenbank zu erstellen:



Schritt 2: Geben Sie einen Namen an, und erstellen Sie die Datenbank.

🚪 New Database							- 🗆 ×
Select a page	🔄 Script 🝷 📑 H	Help					
General							
Flegroups	Database name:		ISEDB				
	Owner:		<default></default>	,			
	🔽 Use full-text in	ndexing					_
	Database files:						
	Logical Name	File Type	Filegroup	Initial	Autogrowth	Path	
	ISEDB	Rows Data	PRIMARY	2	By 1 MB, unrestricted gro	C:\Program Files\Microsoft SQL Server\	MS
	ISEDB_log	Log	Not Appli	1	By 10 percent, unrestrict	C:\Program Files\Microsoft SQL Server\	MS
Connection Server: localhost Connection: BABALAND\administrator Wew connection properties Progress Ready Ready						Add Remove	
						OK Cano	a/

Schritt 3: Erstellen Sie eine neue Tabelle mit den erforderlichen Spalten als Parameter für Endpunkte, um autorisiert zu werden.

😾 WIN-R4PMESFSC16\INFY_MS_SQL_SERV.INFY_DB - dbo.Table_2* - Microsoft SQL Server Management Studio (Administrator) 📃 🗗						_ 8 ×	
File Edit View Project Debug Table Designer Tools Window Help							
: 🏂 / 🗝 📁 📾 🐜 🛄 🎬 🖕							
Object Explorer	WIN	N-R4PMESFSC16\INY_DB	dbo.Table_2	2* ×			<u> </u>
Connect 🕶 🛃 💷 🍸 🧟 🍒		Column Name	Data T	ype	Allow Nulls		
🖃 🐻 WIN-R4PMESFSC16\INFY_MS_SQL_SERV (SQL 🔺		Username	varchar(MA	AX)			
🖃 🚞 Databases		VLAN	varchar(MA	X)			
🛨 🚞 System Databases		ProjectId	varchar(MA	X)	Г		
Database Snapshots	Þ	UserGroup	varchar(MA	(X)	V		
	÷						
					L		
System Tables							
FileTables	-	and the second					
	C	olumn Properties					
+ 🧰 Views	ſ						
🛨 🚞 Synonyms							
🕀 🚞 Programmability	Ŀ	(General)					11
🕀 🚞 Service Broker		(Name)		UserGrou	q		
🛨 🧰 Storage		Allow Nulls		Yes			
Security		Data Type		varchar(MAX)		
Users		Default Value or Binding					
🗄 🦲 Roles	E	Table Designer					_
🛨 🦲 Schemas	Collation <database default=""></database>						<u> </u>
Asymmetric Keys		(General)					
Ceruncates							
E Database Audit Specifications							
	_						
	-						

Schritt 4: Erstellen Sie eine Prozedur, um zu überprüfen, ob der Benutzername vorhanden ist.



Schritt 5: Erstellen Sie eine Prozedur, um Attribute (SGT) aus der Tabelle abzurufen.



In diesem Dokument wird die Cisco ISE in die Microsoft SQL-Lösung integriert, um die Anforderungen für die Autorisierungsskalierung in großen Unternehmensnetzwerken zu erfüllen.

Lösungs-Workflow (ISE 2.7 und früher)

Bei dieser Lösung ist die Cisco ISE in ein Active Directory (AD) und Microsoft SQL integriert. AD wird als Authentifizierungs-ID-Speicher und MS SQL für die Autorisierung verwendet. Während des Authentifizierungsprozesses leitet das Netzwerkzugriffsgerät (Network Access Device, NAD) die Benutzeranmeldeinformationen an das PSN weiter - den AAA-Server in der IBN-Lösung. PSN überprüft die Anmeldeinformationen des Endpunkts im Active Directory-ID-Speicher und authentifiziert den Benutzer. Die Autorisierungsrichtlinie bezieht sich auf die MS SQL-Datenbank, um autorisierte Ergebnisse wie SGT/VLAN abzurufen, für die die **Benutzer-ID** als Referenz verwendet wird.





Vorteile

Diese Lösung bietet die folgenden Vorteile, die sie flexibel macht:

- Die Cisco ISE kann alle möglichen zusätzlichen Funktionen nutzen, die die externe DB bietet.
- Für diese Lösung gelten keine Größenbeschränkungen der Cisco ISE.

Nachteile

Diese Lösung hat folgende Nachteile:

- Zusätzliche Programmierung erforderlich, um die Anmeldeinformationen für den Endpunkt in die externe DB einzutragen.
- Wenn die externe DB nicht lokal wie PSNs vorhanden ist, ist diese Lösung vom WAN abhängig, das sie zum ^{dritten} Fehlerpunkt im AAA-Datenfluss des Endpunkts macht.
- Erfordert zusätzliches Wissen zur Verwaltung externer DB-Prozesse und -Verfahren.
- Fehler, die durch die manuelle Konfiguration der Benutzer-ID für DB verursacht wurden, müssen berücksichtigt werden.

Externe DB - Beispielkonfigurationen

In diesem Dokument wird Microsoft SQL als externe Datenbank dargestellt, die als Autorisierungspunkt verwendet wird.

Schritt 1: Erstellen Sie den ODBC Identity Store in Cisco ISE aus dem Menü Administration > External Identity Source > ODBC und testen Sie die Verbindungen.

Identities Groups External Identit	y Sources Identity Source Seque	ences + Settings			
External Identity Sources	ODBC List > New ODBC List > New ODBC List > New ODBC Identity General * Name Si Description	ODBC Identity Source Connection S DA_SQL	Stored Procedures	Attributes	Groups
ODBC List > ISE_ODBC					
ODBC Identity Source	e Connection	Stored Procedures	Attri	butes	Groups
ODBC DB connection de	etails				
* Hostname/IP[:port]	bast-ad-ca.cisco.con	n			
* Database name	ISEDB				
Admin username	ISEDBUser	()			
Admin password	*****				
* Timeout	5	—	•		
* Retries	1		ION succeeded		x
* Database type	Microsoft SQL Sep	Stored Proce	duree		
Database type	Tact Connection	Plain text pa	assword auther	tication - No	t Configured
	rest connection	Plain text pa	assword fetchin	g - Not Conf	igured
		Check userr	name or machin	ne exists - N	ot Configured
		Fetch group	s - Not Configu	ired	I
		Tetch attribu	nes - Not Cont	gurea	Close

Schritt 2: Navigieren Sie auf der Seite ODBC zur Registerkarte Gespeicherte Prozeduren, um die in Cisco ISE erstellten Prozeduren zu konfigurieren.

General	Connection	Stored Procedures	Attributes	Groups
Sto	ored procedure type	Returns recordset	v	
Plain text pass	word authentication		۲	\oplus
Plain tex	t password fetching		(i)	\oplus
heck usernam	e or machine exists		1	\oplus
	Fetch groups		(1)	
	Fetch attributes	SGTRetrieval		Ð
Search for MA	AC Address in format	XX-XX-XX-XX-XX	• ()	

Schritt 3: Holen Sie die Attribute für die Benutzer-ID aus der ODBC-ID-Quelle zur Überprüfung.

Python and Data : SQL SI X 44 Configure ISE 2.1 with MIX 44 Generative Services Engine X				
← → C 🗛 Not secure bmps//10.82.72.34/admin/#administration/administration_identitymanagement/administration_identitymanagement_external				
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC Click here Identities Groups External Identity Sources Identity Sources Settings	o do wirele:			
External Identity Sources Construct Authoniculan Purplia Active Directory LUAP COBEC RSA Social Directory Social Login				

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

Schritt 4: Erstellen Sie ein Autorisierungsprofil und konfigurieren Sie es. Gehen Sie in Cisco ISE zu Richtlinie > Ergebnisse > Autorisierungsprofil > Erweiterte Attributeinstellungen, und wählen Sie das Attribut als Cisco:cisco-av-pair. Wählen Sie die Werte als <Name der ODBC-Datenbank>:sgt aus, und speichern Sie sie.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture C	Client Provisioning - Policy Elements
Dictionaries + Conditions - Result	Is
0	Authorization Profile
► Authentication	* Name SQL_AuthZ
▼ Authorization	Description //
Authorization Drafilon	*Access Type ACCESS_ACCEPT *
Downloadable ACLs	Network Device Profile det Cisco *
Profiling	
Froming	Service Template
▶ Posture	Track Movement
Client Provisioning	Passive Identity Tracking
	▼ 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
	Courter and South Sector Court Sector

Schritt 5: Erstellen Sie eine Autorisierungsrichtlinie, und konfigurieren Sie sie. Navigieren Sie in der Cisco ISE zu Policy > Policy Sets > Authorization Policy > Add. Setzen Sie die Bedingung als

Identity Source auf den SQL-Server. Wählen Sie das Ergebnisprofil als Autorisierungsprofil aus, das zuvor erstellt wurde.

divelocities Identity Serv	vices Engine Home 🔸 (ontext Visibility + Operations + Policy + Administration +Work Centers	🕕 License Warning 🔺 🔍		o o
▼Network Access	GuestAccess TrustSec	PYOD + Profiler + Posture + Device Administration + PassiveID			
Oveniew Ide Authorization I	entities lid Groups Ext lid Source Policy - Local Exceptions	Network Resources PolicyElements Polic			
> Authorization I	Policy - Global Exceptions				
♥ Authorization I	Policy (18)				
		Results			
+ Status	Rule Name	Conditions Profiles S	Security Groups	Hits	Actions
Search					
0	SOL_AutriZ	AND L Network Access NetworkDeviceName EQBALS REY_SQL_DENDO EsgL_Auth2	Select from list • •	0	٥

Schritt 6: Sobald der Benutzer authentifiziert und autorisiert ist, müssen die Protokolle die dem Benutzer zugewiesene sgt zur Überprüfung enthalten.

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

Lösungs-Workflow (nach ISE 2.7)

Nach ISE 2.7 können Autorisierungsattribute von ODBC abgerufen werden, z. B. Vlan, SGT, ACL, und diese Attribute können in Richtlinien verwendet werden.

Bei dieser Lösung ist die Cisco ISE in Microsoft SQL integriert. MS SQL wird als ID-Speicher sowohl für die Authentifizierung als auch für die Autorisierung verwendet. Wenn die Anmeldeinformationen von den Endpunkten für PSN bereitgestellt werden, werden die Anmeldeinformationen mit der MS SQL-Datenbank abgeglichen. Die Autorisierungsrichtlinie bezieht sich auf die MS SQL-Datenbank zum Abrufen der autorisierten Ergebnisse wie SGT/VLAN, für die die **Benutzer-ID** als Referenz verwendet wird.

Externe DB - Beispielkonfigurationen

Befolgen Sie die zuvor in diesem Dokument beschriebene Prozedur, um MS SQL DB zusammen mit Username, Password, VLAN ID und SGT zu erstellen.

Schritt 1: Erstellen Sie einen ODBC Identity Store in Cisco ISE aus dem Menü Administration > External Identity Source > ODBC und testen Sie die Verbindungen.

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
 Certificate Authentication F Active Directory LDAP ODBC SDA_SQL RADIUS Token RSA SecuriD SAML Id Providers Social Login 	General Connection Stored Procedures Attributes Groups * Name SDA_SQL

Schritt 2: Navigieren Sie auf der Seite ODBC zur Registerkarte Gespeicherte Prozeduren, um die in Cisco ISE erstellten Prozeduren zu konfigurieren.

E Cisco ISE			Adminis	tratio	n • Idr	- Identity Management
Identities Groups External Ide	ntity Sources Identity Source	e Sequences Set	tings			
External Identity Sources < Image: Confident Authoritation 5	ODBC List > SDA_SQL ODBC Identity Source	tored Procedures Att	tributes	Grou	05	15
Active Directory						
	Stored procedure type	Returns recordset	~			
✓ □ ODBC	Plain text password authentication	ISEAuthUser		0	Ð	0
SDA_SQL	Plain text password fetching	ISEFetchPassword		()	•	0
RADIOS TOKEN	Check username or machine exists			()	۲	0
 SAML Id Providers Social Login 	Fetch groups	ISEGroups		0	0	Θ
	Fetch attributes			0	\oplus	Advanced Settings ①
	Search for MAC Address in format	XX-30X-30X-XX-XX-30X	~ (D		

Schritt 3: Holen Sie die Attribute für die Benutzer-ID aus der ODBC-ID-Quelle zur Überprüfung.

E Cisco ISE	Administration - Identity Management
Identities Groups External Ide	entity 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
C Active Directory	🖉 Edit + Add 🔿 🍵 Delete
	Select Attributes from ODBC Default Value Name in ISE
2 SDA_SQL	No data av Add Attribute
C RADIUS Token	
RSA SecuriD	
🗀 Social Login	

E Cisco ISE			Administration • Ider	ntity Management	
Identities Groups External Ide	entity Sources Identity So	ource Sequences	Settings		
External Identity Sources	ODBC List > SDA_SQL ODBC Identity Source General Connection	Stored Procedures	Attributes Groups		
C Active Directory	2 Edit + Add \sim	Delete			
V DDBC	Name	Туре	Default Value	Name in ISE	
ng SDA_SQL	VianName	STRING		vlan	
C RADIUS Token	sgt sgt	STRING	1	sgt	
 RSA SecurID SAML Id Providers Social Login 					

Schritt 4: Erstellen Sie ein Autorisierungsprofil und konfigurieren Sie es. Gehen Sie in Cisco ISE zu Richtlinie > Ergebnisse > Autorisierungsprofil > Erweiterte Attributeinstellungen, und wählen Sie das Attribut als Cisco:cisco-av-pair. Wählen Sie die Werte als <Name der ODBC-Datenbank>:sgt. Wählen Sie unter Allgemeine Aufgaben VLAN mit ID/Name als <Name der ODBC-Datenbank>:vlan aus, und speichern Sie es.

E Cisco ISE	Policy - Policy Elements
Dictionaries Conditions	Results
Authentication	Authorization Profile
Authorization 🗸	* Name SQL_Authz
Authorization Profiles	Description
Downloadable ACLs	*Access Type ACCESS_ACCEPT V
Profiling >	Network Davies Profile 🚊 Claco 🗸 🛞
Posture	Senice Temptee
Client Provisioning	Track Movement 💿
	Apertess Yourse U U
	✓ Common Tasks
	🛙 VLAN Tag 10 1 Edit Tag Olitume SDA, SOL vian 🗸
	O Vice Consin Permission
	U Web Redrection (CNA, MDM, NDP, CPP)
	C Auto Smart Fort
	 Aqvancea Attributes Settings
	E Clisco clisco-av-pair v * SDA_SQL sigt v = +
	V Attributes Details
	Acom Type + ACDIS, ACDPT
	Turnet Physic Grap D = 1:05, 52, Usin Turnet Physic Grap D = 1:05, 52, Usin
	Tarea Marken Sura 1.6

Schritt 5: Erstellen Sie eine Autorisierungsrichtlinie, und konfigurieren Sie sie. Navigieren Sie in der Cisco ISE zu Policy > Policy Sets > Authorization Policy > Add. Setzen Sie die Bedingung als Identity Source auf den SQL-Server. Wählen Sie das Ergebnisprofil als Autorisierungsprofil aus, das zuvor erstellt wurde.

E Cisco ISE		Policy · Policy Sets		A Distantion Mode 19 Days	ର୍ ଡ	58 ¢
Policy Sets→ Default			R	Reset Policyset Hitcounts		Save
Status Policy Set Name Der	cription 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 Exception						
\sim Authorization Policy (13)						
			Results			
Status Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Q Search						
SQL_Authz	AND		(SQL_Authz ×) +	Select from list \sim +	0	¢۵

Interne Datenbank verwenden

Die Cisco ISE selbst verfügt über eine integrierte Datenbank, die über Benutzer-IDs zur Autorisierung verfügt.

Lösungs-Workflow

Bei dieser Lösung wird die interne Datenbank der Cisco ISE als Autorisierungspunkt verwendet, während Active Directory (AD) weiterhin die Authentifizierungsquelle ist. Die Benutzer-ID von Endpunkten ist in der Cisco ISE DB enthalten, zusammen mit **benutzerdefinierten Attributen**, die die autorisierten Ergebnisse zurückgeben, wie z. B. SGT oder VLAN. Wenn die

Anmeldeinformationen von den Endpunkten an PSN übermittelt werden, wird die Gültigkeit der Anmeldeinformationen der Endpunkte mit dem Active Directory-ID-Speicher überprüft und der Endpunkt authentifiziert. Die Autorisierungsrichtlinie bezieht sich auf die ISE-DB zum Abrufen der autorisierten Ergebnisse wie SGT/VLAN, für die die Benutzer-ID als Referenz verwendet wird.

Vorteile

Diese Lösung bietet die folgenden Vorteile, die sie zu einer flexiblen Lösung machen:

- Die Cisco ISE DB ist eine integrierte Lösung und bietet daher im Gegensatz zur externen DB-Lösung keinen ^{dritten} Fehlerpunkt.
- Da der Cisco ISE-Cluster die Echtzeit-Synchronisierung zwischen allen Personen gewährleistet, besteht keine WAN-Abhängigkeit, da beim PSN alle Benutzer-IDs und benutzerdefinierten Attribute in Echtzeit vom PAN übernommen werden.
- Die Cisco ISE kann alle möglichen zusätzlichen Funktionen nutzen, die die externe DB bietet.
- Für diese Lösung gelten keine Größenbeschränkungen der Cisco ISE.

Nachteile

Diese Lösung hat folgende Nachteile:

- Die maximale Anzahl von Benutzer-IDs, die die Cisco ISE DB zurückhalten kann, beträgt 300.000.
- Fehler, die durch die manuelle Konfiguration der Benutzer-ID für DB verursacht wurden, müssen berücksichtigt werden.

Interne DB-Beispielkonfigurationen

Das benutzerspezifische VLAN und SGT können für jeden Benutzer im internen ID-Speicher mit einem benutzerdefinierten Benutzerattribut konfiguriert werden.

Schritt 1. Erstellen Sie neue benutzerdefinierte Benutzerattribute, um den VLAN- und SGT-Wert der entsprechenden Benutzer darzustellen. Navigieren Sie zu Administration > Identity Management > Settings > User Custom Attributes. Erstellen Sie neue benutzerdefinierte Benutzerattribute, wie in dieser Tabelle dargestellt.

Hier wird die ISE-DB-Tabelle mit benutzerdefinierten Attributen angezeigt.

Attributname	Datentyp	Parameter (Länge)	Standardwert
VLAN	String	100	C2S (Standard- VLAN-Name)
Zielgruppe	String	100	cts:security-group- tag=0003-0 (Standard-SGT- Wert)

• In diesem Szenario stellt der VLAN-Wert den VLAN-Namen dar, und der SGT-Wert stellt das cisco-av-pair-Attribut des SGT in Hex dar.

dentity Services Engine	Home Context	Visibility	Policy ▼/	Administration	Work Centers	License Warning 🔺		
System - Identity Management	Network Resources	Device Portal Managemen	nt pxGrid Service	es Feed Service	e Threat Centric NAC			
Identities Groups External Identit	y Sources Identity S	Source Sequences - Setting	s					
0	User Custon	a Attributor						
User Custom Attributes	User Custon	II Attributes						
User Authentication Settings	Predefined	User Attributes (for refe	erence)				Tota	40 🛞 🎡 🖕
Endpoint Purge						Show All		- 8
Endpoint Custom Attributes	Mandatory	Attribute Name		 Data Type 				
Endpoint Gustom Attributes		AllowPasswordChangeAfterL	ogin	String				
		Description		String				
		EmailAddress		String				
		EnableFlag		String				
		EnablePassword		String				
		Firstname		String				
		Lastname		String				
	v	Name		String				
		Password (CredentialPasswo	ord)	String				
	▼ User Custom	Attributes						
	Attribute Name	Description		Data Type	Parameters	Default Value	Manda	tory
	vlan	Vlan details	of the User	String	 Max length : 100 	C2S		-
	sgt	SGT detail o	f the User	String	 Max length : 100 	Cts:security-group	ou 🗆	- +
	Enun Passa						_	-
	Dave							

Schritt 2. Erstellen Sie ein Autorisierungsprofil mit benutzerdefinierten Benutzerattributen, um die VLAN- und SGT-Werte der jeweiligen Benutzer zu implizieren. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > Hinzufügen.** Fügen Sie die unten genannten Attribute unter Erweiterte Attributeinstellungen hinzu.

Diese Tabelle zeigt das AuthZ-Profil für interne Benutzer.

Attribut	Wert
Cisco:cisco-av-pair	Interner Benutzer:sgt
Radius:Tunnel-Private-Group-ID	Interner Benutzer:vlan
Radius:Tunnel-Medium-Type	802
Radius:Tunneltyp	VLAN

Wie im Bild gezeigt, ist das Profil **Internal_user** für die internen Benutzer so konfiguriert, dass SGT und Vlan jeweils als **InternalUser:sgt** und **InternalUser:vlan** konfiguriert sind.

Policy Sets Profiling Posture Clie Dictionaries Conditions Results Authentication Authorization Profiles Downloadable ACLs Profiling Posture	Authorization Profiles > New Authorization Profile Authorization Profile * Name Internal_user Description * Access Type ACCESS_ACCEPT * Network Device Profile @Cisco @ D Service Template Track Movement @ Passive Identity Tracking @
Dictionaries Conditions • Results • Authentication • Authorization • Authorization Profiles • Downloadable ACLs • Profiling • Posture	Authorization Profiles > New Authorization Profile Authorization Profile * Name Internal_user Description * Access Type ACCESS_ACCEPT Network Device Profile Service Template Track Movement Image: Construction of the service Itemplate Passive Identity Tracking
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture	Authorization Profiles > New Authorization Profile Authorization Profile * Name Internal_user Description * Access Type ACCESS_ACCEPT * Network Device Profile Service Template Track Movement
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture	Authorization Profile *Name Internal_user Description
Authorization Authorization Profiles Downloadable ACLs Profiling Posture	* Name Internal_user Description
Authorization Authorization Profiles Downloadable ACLs Profiling Posture	Description * Access Type ACCESS_ACCEPT * Network Device Profile Service Template Track Movement 0
Authorization Profiles Downloadable ACLs Profiling Posture	* Access Type ACCESS_ACCEPT * Network Device Profile Cisco * Service Template Track Movement () Passive Identity Tracking ()
Downloadable ACLs Profiling Posture	Network Device Profile Cisco
Profiling Posture	Service Template
▶ Posture	Service Template
	Track Movement 📄 🕡
	Passive Identity Tracking 📋 🕢
Client Provisioning	
	Common Tasks
	 Advanced Attributes Settings
	Cisco:cisco-av-pair 💟 = InternalUser:sgt 💟 —
	Cisco:cisco-av-pair 📀 = InternalUser:vlan 📀
	Radius:Tunnel-Medium-Type 💟 = 802
	Radius:Tunnel-Type 🖸 = VLAN 🖸 — 🕂
	* Attribute Detaile
	Access Type = ACCESS ACCEPT
	cisco-av-pair = InternalUser:sgt cisco-av-pair = InternalUser:vian
	Tunnel-Medium-Type = :6 Tunnel Tunne - 112
	Attributes Details Access Type = ACCESS ACCEPT disco-av-pair = InternalUser:sgt disco-av-pair = InternalU

Schritt 3: Autorisierungsrichtlinie erstellen, Navigieren Sie zu **Richtlinie > Policy Sets > Policy-1 > Autorisierung.** Erstellen Sie Autorisierungsrichtlinien mit den unten genannten Bedingungen, und ordnen Sie sie den entsprechenden Autorisierungsprofilen zu.

Diese Tabelle zeigt die AuthZ-Richtlinie für interne Benutzer.

Regelname	Bedingung	Autorisierungsprofil für Ergebnisse
	Wenn	•
Interne_Benutzer_Aut hentifizierung	Netzwerkzugriff.EapChainingResults gleich Benutzer und Computer waren beide erfolgreich	Interner Benutzer
Nur-Computer- Authentifizierung	Wenn MyAD.ExternalGroups GLEICHT gdc.security.com/Users/Domain Computers	Zugriff zulassen

		onito P Gu	pritext Visibility	 Operations 	- Policy	 Administration 	 Work Centers 		License V	Varning 🔺	۹. (•
Profili	ng Posture Clier	nt Provisioning	 Policy Ele 	ements									
9	Policy-1				₽ 0	EVICE-Device Type EQ	UALS All Device Types		Default Net	work Access	х т	+	5
antion (D-E (2)												
cation	Policy (3)												
ation P	olicy - Local Except	tions											
ation P	olicy - Global Excep	ptions											
ation P	olicy (3)												
							Results						
tatus	Rule Name		Conditions				Profiles		Security Groups		н	its	Actio
Ø	Internal-users Authz		Network	vork Access-EapCha succeeded	iningResult	EQUALS User and mac	hineuser	+	Select from list	٣	+	2	¢
0	Machine Authz		A MyA	D-ExternalGroups E puters	QUALS gdd	.security.com/Users/Dor	nain PermitAccess	+	Select from list	٣	+	2	ø
Ø	Default						(×DenyAccess)	+	Select from list	Ŧ	+	3	¢
	 ation P ation P ation P ation P ation P ation P 	Policy-1 extion Policy (3) extion Policy - Local Except ation Policy - Global Except ation Policy (3) extual Rule Name extint Rule Name for Internal-users Authz for Machine Authz for Default	Policy-1 Policy (3) Policy - Local Exceptions ation Policy - Global Exceptions ation Policy (3) Rule Name Internal-users Authz Machine Authz Default Default Default	 Policy-1 ation Policy (3) ation Policy - Local Exceptions ation Policy - Global Exceptions ation Policy (3) ation Policy (4) 	 Policy-1 ation Policy (3) ation Policy - Local Exceptions ation Policy - Global Exceptions ation Policy (3) bit success EapChal both success EapChal b	Policy-1 □ ation Policy (3) □ ation Policy - Local Exceptions □ ation Policy - Global Exceptions □ ation Policy (3) □ ation Policy (3) <td>Policy-1 DEVICE: Device Type EQ ation Policy (3) ation Policy - Coal Exceptions ation Policy - Global Exceptions ation Policy (3) bth succeeded bth</td> <td>Policy-1 Image: Conditions EVICE-Device Type EQUALS AII Device Types Condition Policy - Local Exceptions ation Policy - Global Exceptions ation Policy - Glob</td> <td>Policy-1 Image: Device Type EQUALS All Device Types ation Policy (3) ation Policy - Global Exceptions ation Policy (3) ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy (3) ation Policy - Global Exceptions ation Policy - Glob</td> <td>Policy-1 DEVICE Device Type EQUALS All Device Types Default Net eation Policy - Local Exceptions stion Policy - Colal Exceptions ation Policy - Global Exceptions ation</td> <td>Policy-1 DEVICE: Device Type EQUALS All Device Types Default Network Access Telsus Default Network Access Default Network Access Defa</td> <td>Policy-1 Defue the Network Access Policy -1 Tetrant Policy (3) ation Policy - Cacal Exceptions tetran Policy - Global Exceptions ation Policy - Global Exceptions tetran Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions tetrant Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global</td> <td>Policy-1 Defuelt Network Access Policy-1 Defuelt Network Access etation Policy (3) ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions </td>	Policy-1 DEVICE: Device Type EQ ation Policy (3) ation Policy - Coal Exceptions ation Policy - Global Exceptions ation Policy (3) bth succeeded bth	Policy-1 Image: Conditions EVICE-Device Type EQUALS AII Device Types Condition Policy - Local Exceptions ation Policy - Global Exceptions ation Policy - Glob	Policy-1 Image: Device Type EQUALS All Device Types ation Policy (3) ation Policy - Global Exceptions ation Policy (3) ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy (3) ation Policy - Global Exceptions ation Policy - Glob	Policy-1 DEVICE Device Type EQUALS All Device Types Default Net eation Policy - Local Exceptions stion Policy - Colal Exceptions ation Policy - Global Exceptions ation	Policy-1 DEVICE: Device Type EQUALS All Device Types Default Network Access Telsus Default Network Access Default Network Access Defa	Policy-1 Defue the Network Access Policy -1 Tetrant Policy (3) ation Policy - Cacal Exceptions tetran Policy - Global Exceptions ation Policy - Global Exceptions tetran Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions tetrant Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global	Policy-1 Defuelt Network Access Policy-1 Defuelt Network Access etation Policy (3) ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions ation Policy - Global Exceptions

Schritt 4: Erstellen Sie mehrere Benutzeridentitäten mit benutzerdefinierten Attributen mit Benutzerdetails und den entsprechenden benutzerdefinierten Attributen in der CSV-Vorlage. Importieren Sie die CSV, indem Sie zu Administration > Identity Management > Identities > Users > Import > Choose the file > Import navigieren.

dentity Services Engine	Home	Operations Policy	Administration Vork Centers	License Warni	ng 🔺 🔍 🐵 🔿 🌣		
► System	Network Resources Device	Portal Management pxGrid Service	s + Feed Service + Threat Centric NAC				
	ity Sources Identity Source Sequ	nces					
0							
Users Selected 0 Total 5 🏀 🖗 🚽							
Latest Manual Network Scan Results	/ Edit 🕂 Add 🔀 Change	itatus 👻 🎲 Import 🔹 Export 👻	X Delete + Duplicate	Show A	· · · · · · · · · · · · · · · · · · ·		
	Status Name	 Description 	First Name Last Name	Email Address U	ser Identity Groups Admin		
	🗌 🛃 Enabled 🙎 Aravind			B	angalore		
	🗌 🗧 Enabled 🛛 🧕 Jinkle			В	angalore		
	🗌 🛃 Enabled 🙎 jitchand			B	angalore		
	🗌 🛃 Enabled 🛛 👤 Mnason			C	hennai		
	🗌 🛛 Enabled 🙎 Vinodh			В	angalore,Chennai		

Dieses Bild zeigt einen Beispielbenutzer mit benutzerdefinierten Attributdetails. Wählen Sie den Benutzer aus, und klicken Sie auf "Bearbeiten", um die benutzerdefinierten Attributdetails anzuzeigen, die dem jeweiligen Benutzer zugeordnet sind.

-shuth- case Identity Services Engine Home + Context Valuity + Operations + Policy - Administration + Work Centers I	License Warning 🔺	Q	• •	0		
System Identity Management Network Resources Device Portal Management prGrid Services Feed Service Threat Centric NAC						
Identities Groups External Identity Sources Identity Source Sequences Settings						
O Network Access Users Users Users						
Vsers V Network Access User						
Latest Manual Network Scan Results						
Ontra Restord						
Emai						
* Passwords						
Pessword Type: MyAD +						
Password Re-Enter Password						
* Login Posseerd @						
Enable Psesword Generate Recovord						
➤ User Information	▶ User Information					
Account Options						
Account Disable Policy						
▼ User Custom Attributes						
vlan = 525						
sgt = [chrisecurity-group-tag=0005-1						
* User Groups						
Densiore	Encalore O - +					

Schritt 5: Überprüfen Sie die Live-Protokolle:

CF	Refresh O Reset Repest	Counts 🕹 Expo	rt To 🕶									₹ F	iter• O
	Time	Status	Deta	ils Repe	at Identity		Endpoint	t ID	Endpoint Pr	ofile Authentication Po	Authorization Polic	y Authorizati	. IP Addres
×			٠		Identity		Endpoint	ID	Endpoint Pro	fie Authentication Policy	Authorization Policy	Authorization	IP Addres
	Oct 28, 2019 06:40:05.066	РМ 🕕	o	1	host/POD2-CLIEN	F1	00:50:56:8	0.C8:DF	VMWare-Dev	e Policy-1 >> Dot1x	Policy-1 >> Machine A	uthz PermitAccess	172.18.2.1
	Oct 28, 2019 06:40:05.048	PM 🗹	0		host/POD2-CLIEN	F1	00:50:56:8	80:C8:DF	VMWare-Dev	ce Policy-1 >> Dot1x	Policy-1 >> Machine A	uthz PermitAccess	172.16.2.1
Tim	e	Status	Details	Repeat	Identity	Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network De
		*			Identity	Endpoint ID		Endpoint Profi	Authentication	Authorization Policy	Authorization	IP Address 🔻	Network De
Oct 2	29, 2019 10:23:33.877 AM		0	1	araravic,host/POD	00:50:56:80.C8	8:DF	VMWare-De	Policy-1 >>	Policy-1 >> Internal-users Author	Internal_user	172.16.2.1	
Oct 2	29, 2019 10:23:33.877 AM	S	Q		araravic.host/POD	00:50:56:80 C8	B:DF	VMWare-De	Policy-1 >>	Policy-1 >> Internal-users Author	internal_user	172.16.2.1	POD2-ACCE

Überprüfen Sie im Abschnitt **Result** (**Ergebnis**), ob das **Vlan**- und **SGT-**Attribut als Teil von Access-Accept gesendet wird.

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	2btc0t55t87ta3t0atacta1ta2teet29t66t6etb2t0etb5t26t94t23t5dt75t45tc6t10te0t8ftd 8tbctbcte7tb0t71tcctdetc3t79tc2t85t62t4ct01t04t7et95tfeta7t66t0at8bt7dtf3t8bt4at b0te1tc5t9btbbte0tc5t73t32td1tadt48
cisco-av-pair	cts:security-group-tag=0004-00
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Schlussfolgerung

Mit dieser Lösung können einige Großkunden ihre Anforderungen erfüllen. Beim Hinzufügen/Löschen von Benutzer-IDs ist Vorsicht geboten. Werden Fehler ausgelöst, kann dies zu nicht autorisierten Zugriffen für echte Benutzer führen oder umgekehrt.

Zugehörige Informationen

Konfigurieren von Cisco ISE mit MS SQL über 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

Glossar

AAA AD	Authentifizierung, Autorisierung, Abrechnung Active Directory
AuthC	Authentifizierung
AuthZ	Autorisierung
DB	Datenbank
PUNKT 1X	802.1x
IBN	Identitätsbasiertes Netzwerk
ID	Identitätsdatenbank
ISE	Identity Services Engine
MnT	Überwachung und Fehlerbehebung

Microsoft SQL MSSQL Open DataBase-Konnektivität ODBC SCHWEN Knoten "Policy Admin" KEN Richtliniendienstknoten PSN SGT Secure Group-Tag SQL Strukturierte Abfragesprache VLAN Virtuelles LAN WAN Wide Area Network

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.