ISE- und LDAP-Attributbasierte Authentifizierung

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfiguration Netzwerkdiagramm Konfigurationen LDAP konfigurieren Switch-Konfiguration ISE-Konfiguration Überprüfung Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Identity Services Engine (ISE) konfigurieren und Geräte mithilfe von LDAP-Objektattributen (Lightweight Directory Access Protocol) dynamisch authentifizieren und autorisieren.

Hinweis: Dieses Dokument gilt für Einrichtungen, die LDAP als externe Identitätsquelle für die ISE-Authentifizierung und -Autorisierung verwenden.

Beteiligt durch Emmanuel Cano und Mauricio Ramos Cisco Professional Services Engineer.

Editiert von Neri Cruz Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, die folgenden Themen zu kennen:

- Grundkenntnisse der ISE-Richtlinien, der Authentifizierungs- und Autorisierungsrichtlinien
- MAB (Mac Authentication Bypass)
- Grundkenntnisse des Radius-Protokolls
- Grundkenntnisse des Windows-Servers

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE, Version 2.4 Patch 11
- Microsoft Windows Server, Version 2012 R2 x64
- Cisco Switch Catalyst 3650-24PD, Version 03.07.05.E (15.2(3)E5)
- Microsoft Windows 7-Computer

Hinweis: 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 Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfiguration

In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkgeräte konfigurieren, die Integration zwischen ISE und LDAP vornehmen und schließlich LDAP-Attribute für die Verwendung in der ISE-Autorisierungsrichtlinie konfigurieren.

Netzwerkdiagramm

Dieses Bild zeigt die verwendete Netzwerktopologie:



Hier ist der Datenverkehrsfluss, wie im Netzwerkdiagramm veranschaulicht:

- 1. Der Benutzer verbindet seinen PC/Laptop mit dem vorgesehenen Switch-Port.
- 2. Der Switch sendet eine Radius-Zugriffsanforderung für diesen Benutzer an die ISE
- 3. Wenn die ISE die Informationen erhält, fragt sie den LDAP-Server für das spezifische Benutzerfeld ab, das die Attribute enthält, die in den Autorisierungsrichtlinienbedingungen verwendet werden.
- 4. Sobald die ISE die Attribute (Switch-Port, Switch-Name und MAC-Adresse des Geräts) erhält, vergleicht sie die vom Switch bereitgestellten Informationen.
- 5. Wenn die vom Switch bereitgestellten Attributinformationen mit denen von LDAP übereinstimmen, sendet die ISE ein RADIUS Access-Accept mit den im Autorisierungsprofil konfigurierten Berechtigungen.

Konfigurationen

In diesem Abschnitt können Sie LDAP, Switch und ISE konfigurieren.

Konfiguration LDAP

Führen Sie die folgenden Schritte aus, um den LDAP-Server zu konfigurieren:

1. Navigieren Sie zu Server Manager > Dashboard > Tools > ADSI Edit.



2. Klicken Sie mit der rechten Maustaste auf das Symbol ADSI Edit, und wählen Sie Connect to.. (Verbinden mit) aus.



3. Definieren Sie unter Verbindungseinstellungen einen Namen, und wählen Sie die Schaltfläche OK, um die Verbindung zu starten.

Connection Settings
Name: Default naming context
Path: LDAP://WIN-8G7QAP9T36L.ciscoise.lab/Default naming context
Connection Point
O Select or type a Distinguished Name or Naming Context:
×
Select a well known Naming Context:
Default naming context
Computer
 Select or type a domain or server: (Server Domain [:port])
×
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced OK Cancel

4. Klicken Sie im Menü ADSI Edit (ADSI-Bearbeiten) mit der rechten Maustaste in die Verbindung für das Rechenzentrum (DC=ciscodemo, DC=lab), wählen Sie Neu, und wählen Sie dann die Option Objekt



5. Wählen Sie die Option OrganizationalUnit als neues Objekt aus, und wählen Sie als Nächstes aus.

Create Object	X
Select a class: msPKI-Key-Recovery-Agent msSFU30MailAliases msSFU30NetId msSFU30NetworkUser msTPM-InformationObjectsContainer nisMap nisNetgroup nisObject	
organization organizationalUnit physicalLocation	= ~
< Back Next >	Cancel Help
< Back Next >	Cancel Help

6. Definieren Sie einen Namen für die neue Organisationseinheit, und wählen Sie Weiter

	Create Object X
Attribute:	ou
Syntax:	Unicode String
Description:	Organizational-Unit-Name
Value:	AppleDevices
	< Back Next > Cancel Help

7. Wählen Sie Fertig stellen, um die neue Organisationseinheit zu erstellen.

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

8. Klicken Sie mit der rechten Maustaste auf die gerade erstellte Organisationseinheit, und wählen Sie Neu > Objekt

CN=Builtin CN=Comput OU=Domain CN=Foreign:	Move New Connection from Here	 Object
CN=LostAnc CN=Manage	View Delete	
CN=NTDS Q CN=Program CN=System	Rename Refresh	
CN=TPM De CN=Users	Export List	
OU=Develop	Properties Help	

9. Wählen Sie das Gerät als Objektklasse aus, und wählen Sie Nächste

Create Object	×
Select a class:	
builtinDomain classStore computer contact container country device dfsConfiguration domainDNS domainPolicy friendlyCountry group group crounOff IniqueNames	
< Back Next > Ca	incel Help

10. Definieren Sie einen Namen im Feld Wert, und wählen Sie Weiter aus.

	Create Object X
Attribute:	an
Syntax:	Unicode String
Description:	Common-Name
Value:	LaptopTest
	< Back Next > Cancel Help

11. Wählen Sie die Option More Attributes (Mehr Attribute) aus.

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

11. Wählen Sie im Dropdown-Menü eine anzuzeigende Eigenschaft aus, wählen Sie die Option MACAddress aus, definieren Sie dann die MAC-Adresse des Endpunkts, die im Feld Edit-Attribut authentifiziert wird, und wählen Sie die Schaltfläche hinzufügen, um die MAC-Adresse des Geräts zu speichern.

Hinweis: Verwenden Sie einen doppelten Doppelpunkt anstelle von Punkten oder Bindestrich zwischen MAC-Adressenoctets.

cn=La	ptopTest ×
Attributes	
Path: Class: device	
Select which properties to view:	Optional V
Select a property to view:	macAddress 🗸
Attribute Values	
Syntax: IA5String	
Edit Attribute:	
Value(s): 6C:B2:AE:3A:68:	6C
	Add Remove
	OK Cancel

12. Wählen Sie **OK**, um die Informationen zu speichern und mit der Geräteobjektkonfiguration fortzufahren.

13. Wählen Sie Fertig stellen, um das neue Geräteobjekt zu erstellen.

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

14. Klicken Sie mit der rechten Maustaste auf das Geräteobjekt, und wählen Sie **Eigenschaften** aus.

÷		ADSI Edit
Name	Class	Distinguished Name
CN=LaptopTest	device	CN=LaptopTest,OU=AppleDevices,DC=ciscoise,DC=lab
	Move	
	Delete	
	Rename	
	Properties	
	Help	

15. Wählen Sie die **Beschreibung der** Option aus, und wählen Sie **Bearbeiten** aus, um den Switch-Namen und den Switch-Port festzulegen, an den das Gerät angeschlossen werden soll.

tribute Editor Security	
Attributes:	
Attribute	Value
adminDescription	<not set=""></not>
admin DisplayName	<not set=""></not>
bootFile	<not set=""></not>
bootParameter	<not set=""></not>
cn	Laptop Test
description	<not set=""></not>
displayName	<not set=""></not>
displayNamePrintable	<not set=""></not>
distinguishedName	CN=LaptopTest,OU=AppleDevices,DC=cisc
dSASignature	<not set=""></not>
dSCorePropagationD	0x0 = ()
extensionName	<not set=""></not>
flags	<not set=""></not>
fSMORoleOwner	<not set=""></not>
<	>
Edit	Filter
OK	Cancel Apply Help

16. Definieren Sie den Switch-Namen und den Switch-Port. Trennen Sie jeden Wert durch ein Komma. Wählen Sie Hinzufügen und dann OK, um die Informationen zu speichern.

Multi-valued String Editor		x
Attribute: description		
Value to add:		
switchapflexconnect,GigabitEthemet1/0/6	Add	
Values:		
	Remove	
		_
OK	Cancel	

- Switchapflexconnect ist der Switch-Name.
- GigabitEthernet1/0/6 ist der Switch-Port, an den das Endgerät angeschlossen ist.

Hinweis: Sie können Skripts verwenden, um einem bestimmten Feld Attribute hinzuzufügen. In diesem Beispiel definieren wir die Werte jedoch manuell

Hinweis: Beim AD-Attribut wird die Groß-/Kleinschreibung beachtet, wenn bei der LDAP-Abfrage alle MAC-Adressen in Kleinbuchstaben von ISE in Großbuchstaben konvertiert werden. Um dieses Verhalten zu vermeiden, deaktivieren Sie die Process Host Lookup-Suche unter zulässigen Protokollen. Einzelheiten hierzu finden Sie unter: <u>https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf</u>

Switch-Konfiguration

Im Folgenden wird die Konfiguration für die 802.1x-Kommunikation zwischen der ISE und dem Switch beschrieben.

aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication dot1x default group ISE aaa authorization network default group ISE aaa accounting update

newinfo aaa accounting dotlx default start-stop group ISE ! aaa server radius dynamic-author client 10.81.127.109 server-key XXXXabc ! aaa session-id common switch 1 provision ws-c3650-24pd ! dotlx system-auth-control dotlx critical eapol diagnostic bootup level minimal spanning-tree mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level 3 ! interface GigabitEthernet1/0/6 description VM for dotlx switchport access vlan 127 switchport mode access authentication event fail action next-method authentication event server dead action authorize vlan 127 authentication event server alive action reinitialize authentication host-mode multi-domain authentication open authentication order dotlx mab authentication priority dotlx mab authentication port-control auto authentication periodic authentication timer reauthenticate server authentication timer inactivity server dynamic authentication violation restrict mab dotlx pae authenticator dotlx timeout tx-period 10 spanning-tree portfast ! radius server ISE address ipv4 10.81.127.109 auth-port 1812 acct-port 1813 automate-tester username radiustest idle-time 5 key XXXabc !

Hinweis: Möglicherweise müssen die globale Konfiguration und die Schnittstellenkonfiguration in Ihrer Umgebung angepasst werden.

ISE-Konfiguration

Im Folgenden wird die Konfiguration der ISE beschrieben, um die Attribute vom LDAP-Server abzurufen und die ISE-Richtlinien zu konfigurieren.

cisco Identity Services Engine	Home	Operations Pol	- Administration	Work Centers
System Identity Management	Network Resources	Portal Management px0	Brid Services	
Identities Groups External Identity	Sources Identity Source Sequ	uences + Settings		
External Identity Sources	LDAP Identit	Duplicate X Delete	▲ Descripti	on

2.Definieren Sie auf der Registerkarte Allgemein einen Namen und wählen Sie die MAC-Adresse als Attribut für den Betreffnamen aus.

LDAP Identity Sources List > Ide	p_mab				
LDAP Identity Source					
General Conn	ection Directory Organizatio	n Groups	Attributes	Advanced Settings	
* Name	ldap_mab				
Description					
- Schema	Custom *				
• Cubiast Objectoires	desire	* Orean Objectulary	Conue		
 Subject Objectclass 	ervice	- Group Objectclass	Group		
* Subject Name Attribute	macAddress	* Group Map Attribute	member		
* Group Name Attribute	distinguishedName	Certificate Attribute			
O Publical Objects Court	in Balances To Course				
O Subject Objects Cond	an Hererence to Groups				
 Group Objects Contain 	n Reference To Subjects				
	Subjects In Groups Are Stored	In Member Attribute As	Distinguished Name	· · ·	
User Info Attributes ()					
First Name		Department			
Last Name		Organizational Unit			
Job Title		Locality			
Email		State or Province			
Telephone		Country			
Street Address					

3. Konfigurieren Sie auf der **Registerkarte Verbindung** die IP-Adresse, die Admin-DN und das Kennwort des LDAP-Servers, um eine erfolgreiche Verbindung herzustellen.

	Directory organization	Groups	Attributes	Advanced Settings	
Prima	ry Server			5	econdary Server
					Enable Secondary Server
* Hostname/IP 10.8	1.127.111			Hostname/IP	<i>x</i>
* Port 389				Port	389
Admin DN Password	Authenticated Access Cn=administrator, cn=users, dc	=c		Admin Passw	Authenticated Access DN ond
Secure Authentication	Enable Secure Authentication			Secure Authentical	ion Enable Secure Authentication
LDAP Server Root CA	Certificate Services Root CA - *	x		LDAP Server Root	CA Certificate Services Root CA - *
lances OA al IOE Configuration	Select if required (ontinnal) *	æ		Issuer CA of ISE Certifica	des Select if required (optional) * ①

Hinweis: Der verwendete Standard-Port ist Port 389.

4. Wählen Sie auf der Registerkarte Attribute die MACAddress-Attribute und die Beschreibungsattribute aus. Diese Attribute werden in der Autorisierungsrichtlinie verwendet.

LDAP Identity Sources List > Idap_mab

LDAP Identity Source

General	General Connection		Directory Organization	Groups	Attributes	Advanced Settings	
/ Edit 🕂 Add 👻 🗙	Delete Attri	bute					
Name	-	Туре	Default	Internal Name			
description		STRING		description			
distinguishedNam	distinguishedName STRING			distinguishedNam	e		
macAddress	macAddress STRING			macAddress			

5. Um ein erlaubtes Protokoll zu erstellen, gehen Sie zu Richtlinien->Richtlinienelemente->Ergebnisse->Authentifizierung->Zulässige Protokolle. Definieren und Auswählen von Process Host Lookup und Zulassen von PAP/ASCII als einzigen zulässigen Protokollen Wählen Sie abschließend Speichern

cisco Identity Services Engine	Home + C	ontext Visibility	Operations	* Policy	Administration
Policy Sets Profiling Posture	Client Provisioning	* Policy Elements			
Dictionaries + Conditions + Res	ults				
- Authentication	Allowed Protoc Allowed Protoc	ols Services List > M otocols	AB_MacAddres	•	
Allowed Protocols	Name	MAB_MacAddress]	
Authorization	Description				1
Profiling					
Posture	 Allowed Pr 	rotocols			
Client Provisioning	Auth	entication Bypass Process Host Lookur	-		
	Auth	entication Protocol			
	V	Allow PAP/ASCII			

6. Um ein Autorisierungsprofil zu erstellen, gehen Sie zu **Richtlinien->Richtlinienelemente->Ergebnisse->Autorisierung->Autorisierungsprofile.** Wählen Sie **Hinzufügen**, und definieren Sie die Berechtigungen, die dem Endpunkt zugewiesen werden.

dentity Services Engine	Home	Operations - Policy	Administration			
Policy Sets Policy Elements						
Dictionaries Conditions Results	_					
0						
Authentication	Standard Authorization	Profiles				
- Authorization	For Policy Export go to Administ	tration > System > Backup &	& Restore > Policy Expo	rt Page		
Authorization Profiles	/ Edit Add Duplicate	🗙 Delete				
Dowploadable ACLs	Name	F	Profile			
Downloadable AGEs	Blackhole_Wireless_Acces	ss a	🛱 Cisco 🕀			
▶ Profiling	Cisco_IP_Phones	□ Cisco_IP_Phones 🗰 Cisco ⊕				
▶ Posture	Cisco_Temporal_Onboard	a	📩 Cisco 🕀			

dentity Services Engine	Home	Operations Policy	Administration	► Work Centers
Policy Sets Policy Elements				
Dictionaries + Conditions - Resul	is			
Authentication	Authorization Profiles > New Auth Authorization Profile	orization Profile		
- Authorization	* Name MAC	PORTSWITCHLDAP		
Authorization Profiles	Description			
Downloadable ACLs	* Access Type ACCE	ESS_ACCEPT T		
➤ Profiling	Network Device Profile	Cisco 🔻 🕀		
▶ Posture	Service Template			
Client Provisioning	Track Movement Passive Identity Tracking ()			
	Common Tasks DACL Name	PERMIT_ALL_IPV	4_TRAFFIC 📀	

7.Gehen Sie zu Policy-> Policy Set, und erstellen Sie einen Richtliniensatz mit der vordefinierten Bedingung Wired_MAB und dem in Schritt 5 erstellten Zugelassenen Protokoll.

Policy Sets → MAB_LDAP		Reset Policyset Hitcounts Reset Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits
Search		
MAB_LDAP	Wred_MAB	MAB_MacAddress × + 0

8. Erstellen Sie unter dem neu erstellten Richtliniensatz eine Authentifizierungsrichtlinie mit der vordefinierten Wired_MAB Library und der LDAP-Verbindung als externe Identitätsquellensequenz.

✓ Authen	tication R	Policy (2)					
•	Status	Rule Name	Conditions		Use	Hits	Actions
Search							
					idap_mab	*	
				₩ Options			
				If Auth fail			
	0	Auth_MAB_LDAP	E Wred_MAB		REJECT *		۰
					If User not found		
					REJECT *		
					If Process fail		
					DROP ×		
					DenyAccess	w.	
	0	Default		¢	> Options	0	•

9. Definieren Sie unter Autorisierungsrichtlinie einen Namen, und erstellen Sie eine zusammengesetzte Bedingung mithilfe der LDAP-Attributbeschreibung, RADIUS NAS-Port-ID und NetworkDeviceName. Fügen Sie abschließend das in Schritt 6 erstellte Autorisierungsprofil hinzu.

,			Editor								
rch by Name					Carlos						o
0 4 0 ₽ 0 8		0 t 🕈		£;	Click to ad	d an attri	bute				
EAP-TLS		Ø			Equals	•	Attribute value			•	
Guest_Flow		Ø		L.	Click to ad	d an attri	bute				0
MAC_in_SAN		Ø	AND •	G	Equals	•	Attribute value				
Network_Access_Auth	entication_Passed	Ø					AND	OR			
Non_Cisco_Profiled_P	hones	Ø									2
Non_Compliant_Devices		Set to 'Is i	noť				Duplicate	Sav	•		
Switch_Local_Web_A	thentication	Ø									
Switch_Web_Authenti	ation	Ø									
Wired_802.1X		Ø									
Wind MAB		Ø									
11100_10100											
1100_1000											
	EAP-TLS Guest_Flow MAC_In_SAN Network_Access_Auth Non_Cisco_Profiled_P Non_Compliant_Device Switch_Local_Web_Ac Switch_Local_Web_Actiontic Wired_802.1X	EAP-TLS Guest_Flow MAC_In_SAN Network_Access_Authentication_Passed Non_Cisco_Profiled_Phones Non_Compilant_Devices Switch_Local_Web_Authentication Switch_Web_Authentication Wired_802.1X	EAP-TLSImage: Constraint of the constrain	EAP-TLS Image: Constraint of the set of the se	EAP-TLS Guest_Flow MAC_In_SAN Non_Cisco_Profiled_Phones Non_Compliant_Devices Switch_Local_Web_Authentication Switch_Web_Authentication Wred_802.1X	EAP-TLS Guest_Flow MAC_In_SAN Non_Cisco_Profiled_Phones Non_Compliant_Devices Switch_Local_Web_Authentication Switch_Web_Authentication Wred_802.1X	EAP-TLS Guest_Flow MAC_In_SAN Non_Cisco_Profiled_Phones Non_Compliant_Devices Switch_Local_Web_Authentication Switch_Web_Authentication Wred_802.1X	EAP-TLS Image: Click to add an attribute value Guest_Flow Image: Click to add an attribute MAC_In_SAN Image: Click to add an attribute Non_Clisco_Profiled_Phones Image: Click to add an attribute Non_Compliant_Devices Image: Click to add an attribute Switch_Uced_Web_Authentication Image: Click to add an attribute Switch_Web_Authentication Image: Click to add an attribute	EAP-TLS Image: Im	EAP-TLS Guest_Flow MAC_in_SAN O Network_Access_Authentication_Passed O Non_Cisco_Profiled_Phones O Switch_Local_Web_Authentication O Switch_Web_Authentication O Wred_802.1X	EAP-TLS Guest_Flow MAC_in_SAN O Network_Access_Authentication_Passed O Non_Cisco_Profiled_Phones O Switch_Local_Web_Authentication O Switch_Web_Authentication O Wred_802.1X

Nachdem Sie die Konfiguration angewendet haben, sollten Sie ohne Benutzereingriff eine Verbindung zum Netzwerk herstellen können.

Überprüfung

Wenn Sie mit dem designierten Switch-Port verbunden sind, können Sie **show authentication session interface GigabitEthernet X/X/X-Details** eingeben, um den Authentifizierungs- und Autorisierungsstatus des Geräts zu überprüfen.

Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session timeout: N/A Restart timeout: N/A Common Session ID: 0A517F65000013DA87E85A24 Acct session ID: 0x000015D9 Handle: 0x9300005C Current Policy: Policy_Gi1/0/6 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure Security Status: Link Unsecure Method status list: Method State mab Authc Success Auf der ISE können Sie RADIUS Live Logs zur Bestätigung verwenden.

C	🗘 Refresh 🔍 Reset Repeat Counts 🔮 Export To 🔸												
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P Authentication Policy	Server	Authorization Profiles				
×		•			Identity	Endpoint ID	Endpoint Profi Authentication Policy	Server	Authorization Profiles				
	Jan 20, 2020 06:21:47.825 PM	•	0	0	employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown	ise23-1	MACPORTSWITCHLDAP				
	Jan 20, 2020 06:21:47.801 PM		0		employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown	ise23-1	MACPORTSWITCHLDAP				

Fehlerbehebung

Überprüfen Sie auf dem LDAP-Server, ob das erstellte Gerät über eine MAC-Adresse, einen korrekten Switch-Namen und einen konfigurierten Switch-Port verfügt

CN=	LaptopTest Properties ? ×
Attribute Editor Security	
Attributes:	
Attribute	Value 🔨
lastKnownParent	<not set=""></not>
macAddress	6C:B2:AE:3A:68:6C
manager	<not set=""></not>
mS-DS-ConsistencyC	<not set=""></not>
mS-DS-ConsistencyG	<not set=""></not>
msDS-LastKnownRDN	<not set=""></not>
msDS-NcType	<not set=""></not>
msSFU30Aliases	<not set=""></not>
msSFU30Name	<not set=""></not>
msSFU30NisDomain	<not set=""></not>
name	LaptopTest
nisMapName	<not set=""></not>
0	<not set=""></not>
objectCategory	CN=Device,CN=Schema,CN=Configuration, [🗸
< 111	>
Edit	Filter
ОК	Cancel Apply Help

CN=	LaptopTest Properties ? ×			
Attribute Editor Security				
Attributes:				
Attribute	Value ^			
adminDescription	<not set=""></not>			
adminDisplayName	<not set=""></not>			
bootFile	<not set=""></not>			
bootParameter	<not set=""></not>			
cn	Laptop Test			
description	switchapflexconnect,GigabitEthemet1/0/6			
displayName	<not set=""></not>			
displayNamePrintable	<not set=""></not>			
distinguishedName	CN=LaptopTest,OU=AppleDevices,DC=cisc			
dSASignature	<not set=""></not>			
dSCorePropagationD	0x0 = ()			
extensionName	<not set=""></not>			
flags	<not set=""></not>			
fSMORoleOwner	<not set=""></not>			
< 111	> · · ·			
Edit	Filter			
ОК	Cancel Apply Help			

Auf der ISE können Sie eine Paketerfassung (**Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**) durchführen, um zu überprüfen, ob die Werte von LDAP an die ISE gesendet werden.

27	134,204090	18.81.127.189	18,81,127,111	LENP	201	searchilequest(2) "80-4ppladevices,80-classdens,80-fat?" uts/arbitras	
28	124.308017	38.40.127.111	38.81.127.300	LOW	202	ana+thleaDetry(2) *2#-LaptopText,00-AppTabes/core,80-clacintees,90-lab* asa+thleaDetext(2) accores	
29	324.303291	18.81.127.189	38,81,127,113	LENP	2783	sear-thinguest131 "Bodgetabectors,30+classione,30-fait" shefatbaltives	
- 10	314, 108083	18.81.127.111	18,81,127,189	1.010	3152	searchiedistry(3) "Ob-Lagtaphert, Ob-AppleDevices, 80-classebee, 80-lab" searchiedbee(3) eaccess	4
31	124, 101273	18.81.127.189	18,81,127,111	LEMP	208	unarthNeguet141 "BU-Applebevices,3C+cistodemo,3C+lath" wholefuldrives	
32	124,305384	10.01.127.111	18,81,127,199	LEMP	- 048	searcheobrei4) secons 12 results)	۰.
33	325,494545	14.41.127.148	34.41.127.111	1.544	5/88	searchinguest (5) "Nodepletextors, Kirclassiene, Kirlas" whethethetices	
1.4				- 81110		increased and a second the second and	
	 attribut 	tes: 3 items					
	V Parts	aMUVIAME.Ist lite	 description 				
	19	pel description					
	7.14	fact 1 sham					
		Antrobutefulues and	tchap?lexcemect_light	(ITheret)/	8.16		
	 Parts 	WATCHINGS, 111	 distinguisheddane 				
	1.0	pe: distinguishedRes	10 N				
	7 V8	fact 1 stam					
		Anti-shutafiature Ord	LaptopTest_30-AppTellev	tem. Retail	- dema	e, BOHTan	
	 Pariti 	infattoributed, but item	a manifedorean				
	1.0	pel) machildrass					
	7.14	fact 3 sham					
		AttributeValues 601	\$2:AE:3A:6E:6C				