Autenticazione basata sugli attributi ISE e LDAP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete Configurazioni Configura LDAP Configurazione degli switch Configurazione di ISE Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) e utilizzare gli attributi degli oggetti LDAP (Lightweight Directory Access Protocol) per autenticare e autorizzare i dispositivi in modo dinamico.

Nota: Questo documento è valido per le configurazioni che usano LDAP come origine identità esterna per l'autenticazione e l'autorizzazione ISE.

Contributo di Emmanuel Cano e Mauricio Ramos Cisco Professional Services Engineer.

A cura di Neri Cruz Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei set di policy, dell'autenticazione e delle policy di autorizzazione ISE
- Mac Authentication Bypass (MAB)
- Conoscenze base del protocollo Radius
- Conoscenze base di Windows Server

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE, versione 2.4 patch 11
- Microsoft Windows Server, versione 2012 R2 x64
- Cisco Switch Catalyst 3650-24PD, versione 03.07.05.E (15.2(3)E5)
- computer con Microsoft Windows 7

Nota: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione viene descritto come configurare i dispositivi di rete, l'integrazione tra ISE e LDAP e infine come configurare gli attributi LDAP da utilizzare nella policy di autorizzazione ISE.

Esempio di rete

Nell'immagine è illustrata la topologia di rete utilizzata:



Di seguito è riportato il flusso del traffico, come mostrato nello schema della rete:

- 1. L'utente collega il PC/notebook alla porta dello switch designata.
- 2. Lo switch invia una richiesta di accesso Radius per l'utente all'ISE
- 3. Quando l'ISE riceve le informazioni, interroga il server LDAP per il campo utente specifico, che contiene gli attributi da utilizzare nelle condizioni del criterio di autorizzazione.
- 4. Una volta ricevuti gli attributi (porta dello switch, nome dello switch e indirizzo MAC del dispositivo), ISE confronta le informazioni fornite dallo switch.
- 5. Se le informazioni sugli attributi fornite dallo switch sono le stesse di quelle fornite da LDAP, ISE invierà un messaggio di autorizzazione RADIUS con le autorizzazioni configurate nel profilo di autorizzazione.

Configurazioni

Utilizzare questa sezione per configurare il protocollo LDAP, lo switch e l'ISE.

Configurazione LDAP

Per configurare il server LDAP, effettuare le seguenti operazioni:

1. Passare a Server Manager > Dashboard > Strumenti > Modifica ADSI



2. Fare clic con il pulsante destro del mouse sull'icona Modifica ADSI e selezionare Connetti a...

File Action	View Help	
♦	Q 📑 🚺	
📝 ADSI Edit		
⊿ 🗎 LDA	Connect to	
	View	•
	Refresh	
	Export List	
	Help	

3. In Impostazioni connessione definire un nome e selezionare il pulsante OK per avviare la connessione.

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. Nello stesso menu Modifica ADSI, fare clic con il pulsante destro del mouse su Connessione DC (DC=ciscodemo, DC=lab), selezionare Nuovo, quindi selezionare l'opzione Oggetto

		1	1		
tin	n	New	•		Object
npute nain C eignSe tAndF naged		Rename Refresh Properties Help			
gram Da tem 1 Device rs IUsers	ata es			_	

5. Selezionare l'opzione OrganizationalUnit come nuovo oggetto e selezionare avanti.

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

6. Definire un nome per la nuova unità organizzativa e selezionare Avanti

7. Selezionare Fine per creare la nuova unità organizzativa

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. Fare clic con il pulsante destro del mouse sull'unità organizzativa appena creata e selezionare Nuovo > Oggetto

CN=Builtin CN=Comput OU=Domain	Move New Connection from Here	Object
CN=LostAnc	View +	object
CN=Manage CN=NTDS Q	Delete	-
CN=Program	Rename	
CN=System CN=TPM De	Refresh	
CN=Users	Export List	-
CN=VPNUse	Properties	
OU=Develop	Help	
🧾 OU=AppleDe		

9. Selezionare device (dispositivo) come object class (classe oggetto), quindi selezionare avanti

	Create Object X
Select a class:	
builti class comp cont court court	inDomain ∧ sStore puter ≡ act ainer htry
dfsC dom dom frien grou	P P P P P P P P P P P P P P
[< Back Next > Cancel Help

10.Definire un nome nel campo Valore e selezionare Successivo

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

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
< Back Finish Cancel Help

11. Per il menu a discesa, Selezionare una proprietà da visualizzare, selezionare l'opzione macAddress, quindi definire l'indirizzo Mac dell'endpoint che verrà autenticato nel campo Modifica attributo e selezionare Pulsante Aggiungi per salvare l'indirizzo MAC del dispositivo.

Nota: tra gli ottetti dell'indirizzo MAC è possibile utilizzare due punti anziché punti o trattini.

cn=LaptopTest ×			
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	8:6C		
	Add Remove		
	OK Cancel		

12. Selezionare OK per salvare le informazioni e continuare con la configurazione dell'oggetto dispositivo

13. Selezionare Finish (Fine) per creare il nuovo oggetto dispositivo

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. Fare clic con il pulsante destro del mouse sull'oggetto dispositivo e selezionare l'opzione **Properties**

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

15. Selezionare l'opzione **description** (Descrizione) e selezionare **Edit** (Modifica) per definire il nome dello switch e la porta dello switch a cui verrà connesso il dispositivo.

CIN=	
Security	
Attributes:	
Attribute	Value ^
adminDescription	<not set=""></not>
admin DisplayName	<not set=""></not>
boot File	<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. Definire il nome dello switch e la porta dello switch. Utilizzare una virgola per separare ciascun valore. Selezionare Aggiungi, quindi OK per salvare le informazioni.

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

- Switchapflexconnect è il nome dello switch.
- Gigabit Ethernet1/0/6 è la porta dello switch a cui è connesso l'endpoint.

Nota: È possibile utilizzare gli script per aggiungere attributi a un campo specifico. Tuttavia, in questo esempio i valori vengono definiti manualmente

Nota: L'attributo AD fa distinzione tra maiuscole e minuscole, se si utilizzano tutti gli indirizzi Mac in lettere minuscole, ISE viene convertito in lettere maiuscole durante la query LDAP. Per evitare questo comportamento, disabilitare Ricerca host processi nei protocolli consentiti. Ulteriori informazioni sono disponibili al seguente link: <u>https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf</u>

Configurazione degli switch

Di seguito viene descritta la configurazione della comunicazione 802.1x tra ISE e lo switch.

aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication dotlx 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 authenticator 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 XXXXabc !

Nota: Potrebbe essere necessario modificare la configurazione globale e dell'interfaccia nell'ambiente in uso

Configurazione di ISE

Di seguito viene descritta la configurazione di ISE per ottenere gli attributi dal server LDAP e configurare le policy ISE.

1. Ad ISE, andare in Amministrazione->Gestione delle identità->Origini delle identità esterne e selezionare la cartella LDAP e fare clic su Aggiungi per

creare una nuova connessione con LDAP				
Cisco Identity Services Engine Home	Context Visibility Operation	ns Policy	 Administration 	Work Centers
System Identity Management Network Re	esources	ement pxGrid S	ervices	
Identities Groups External Identity Sources	Identity Source Sequences + S	ettings		
External Identity Sources	LDAP Identity Sources	Y Delete		
Certificate Authentication Profile Active Directory DAP	Name		 Descripti 	on
CODBC				
SAML Id Providers				

2. In Generale, definire un nome e selezionare l'indirizzo mac come Attributo nome soggetto

LDAP Identity Sources List > Ide	p_mab				,	
LDAP Identity Source						
General Conn	ection Directory Organizatio	on Groups	Attributes	Advanced Settings		
* Name	Idan mah					
rearing	icap_meo					
Description						
- Schema	Custom .					
* Subject Objectclass	device	* Group Objectclass	Group			
* Subject Name Attribute	macilideness	* Group Map Attribute	member			
Gaugeot Harrie Philadean		Group may recover	menee			
* Group Name Attribute	distinguishedName	Certificate Attribute				
Subject Objects Cont	in Reference To Groups					
Group Objects Contai	n Reference To Subjects					
C and other course	Robieste la Casure Are Blees	d in Manhar Allahota As				
	Subjects in Groups Are Store	d in Member Attribute As	Distinguished Name	, i		
User Info Attributes						
First Name		Department				
Last Name		Omanizational Unit	[
Cash Page 14						
Job Title		Locality				
Email		State or Province				
Telephone		Country				
Street Address		1				
oreer nooress		1				

3. In Connessione configurare l'indirizzo IP, il DN di amministrazione e la password del server LDAP per ottenere una connessione riuscita.

P Identity Sources List > Idap_mab AP Identity Source					
General Connection	Directory Organization	Groups	Attributes	Advanced Settings	
Prima	ry Server				Secondary Server
				C	Enable Secondary Server
*Hostname/IP 10.81	.127.111			Hostname/IP	a.
* Port 389				Port	389
Specify server for each ISE node					
Access	Anonymous Access			Acc	cess 💿 Anonymous Access
	 Authenticated Access 				 Authenticated Access
Admin DN	* cn=administrator, cn=users, dc=	c		Admin	DN
Password	•			Passv	word
Secure & therefore	Carble Server Authentication			Constant de Marentine	tion 🗍 Easthin Conven Authoritication
Secure Authentication	Enable Secure Authentication			Secure Authentica	Enable Secure Authentication
	Cheve derver identity check				
LDAP Server Root CA	Certificate Services Root CA - *	×.		LDAP Server Root	CA Certificate Services Root CA - *
Issuer CA of ISE Certificates	Select if required (optional) *	(E)		Issuer CA of ISE Certific	ates Select if required (optional)

Nota: La porta 389 è la porta predefinita utilizzata.

4. In Attributi scheda selezionare gli attributi macAddress e description, questi attributi verranno utilizzati nel criterio di autorizzazione

LDAP Identity Sources List > Idap_mab

LDAP Identity Source

	General	Connectio	n	Directory Organization	Groups	Attributes	Advanced Settings
1	Edit 🕂 Add 👻 🗙 🛙	Delete Attri	bute				
	Name	-	Туре	Default	Internal Name		
	description		STRING		description		
	distinguishedName		STRING		distinguishedNan	ne	
	macAddress		STRING		macAddress		

5. Per creare un protocollo consentito, passare a Criterio->Elementi della policy->Risultati->Autenticazione->Protocolli consentiti. Definire e selezionare Process Host Lookup e Allow PAP/ASCII come gli unici protocolli consentiti. Infine, selezionare Salva

cisco Identity Services Engine	Home + C	ontext Visibility	Operations	* Policy	+ Administration		
Policy Sets Profiling Posture (Client Provisioning	* Policy Elements					
Dictionaries Conditions Resu	its						
• Authentication	Allowed Protoc Allowed Pro	otocols	AB_MacAddres	•			
Allowed Protocols	Name	MAB_MacAddress]			
Authorization	Description						
Profiling							
▶ Posture	 Allowed Pr 	rotocols					
Client Provisioning	Auth	Authentication Bypass					
		Process Host Lookup	Ð				
	Auth	entication Protocols	1				
		Allow PAP/ASCII					

6. Per creare un profilo di autorizzazione, passare a Criteri->Elementi criteri->Risultati->Autorizzazione->Profili di autorizzazione. Selezionare Aggiungi e definire le autorizzazioni da assegnare all'endpoint.

dentity Services Engine	lome	Operations	▼Policy	 Administration 	 Work Centers
Policy Sets Policy Elements					
Dictionaries + Conditions - Results					
G					
Authentication	Standard Authorization	n Profiles			
- Authorization	For Policy Export go to Admin	istration > Systen	n > Backup &	Restore > Policy Exp	ort Page
Authorization Profiles	/ Edit Add	e 🗙 Delete			
Downloadable ACLs	Name		Pro	ofile	
Downloadable ACLs	Blackhole_Wireless_Acc	cess	010	Cisco 🕀	
Profiling	Cisco_IP_Phones			Cisco 🕀	
▸ Posture	Cisco_Temporal_Onboa	rd	del	Cisco 🕀	

dentity Services Engine	Home + Context Visibility	Operations	Policy → Adm	inistration	Work Centers	
Policy Sets						
Dictionaries + Conditions - Resul	ts					
Authentication	Authorization Profiles > New A Authorization Profile	Authorization Profile				
- Authorization	* Name 1	MACPORTSWITCHLDAP	Þ			
Authorization Profiles	Description					/h
Downloadable ACLs	* Access Type	CCESS_ACCEPT	Ŧ			
▶ Profiling	Network Device Profile	ដ Cisco 🔻 🕀				
→ Posture	Service Template	1				
Client Provisioning	Track Movement	Ð				
	Passive Identity Tracking) Ø				
	★ Common Tasks					
	DACL Name	PERMI	IT_ALL_IPV4_TRAFF	TC 📀		

7.Andare a Policy-> Policy Set e creare un set di criteri usando la condizione predefinita Wired_MAB e il protocollo consentito creato nel passaggio 5.

Policy Sets → MAB_LDAP			Reset Policyset Hitcounts Reset	Save
Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search				
Ø MAB_LDAP		Wired_MA8	MAB_MacAddress = +	0

8.Sotto il nuovo set di criteri creato creare un criterio di autenticazione utilizzando la libreria Wired_MAB predefinita e la connessione LDAP come sequenza di origine dell'identità esterna

Aumer	tocation	Policy (2)								
•	Status	Rule Name	Con	lions		Use		Hits	Actions	
Search										
						idap_mab	ж. т			
						♥ Options				
						If Auth fail				
	0	Auth_MAB_LDAP	~ E	-	Wred_MAB		REJECT	××	0	۰
			_			If User not found				
						REJECT	**			
						If Process fail				
						DROP	* *			
					DenyAccess	**				
	Ø	Default			¢	> Options		0	0	

9. In **Criteri di autorizzazione** definire un nome e creare una condizione composta utilizzando la descrizione dell'attributo LDAP, Radius NAS-Port-Id e NetworkDeviceName. Infine, aggiungere il profilo di autorizzazione creato nel passaggio 6.

Library	Editor							
Search by Name			Click to add an attribute					o
		F.	Equals •	Attribute value				
Guest_Flow	AND .	Ŀ	Click to add an a	ittribute				0
MAC_in_SAN Ø		~	Equals •	Attribute value				
Network_Access_Authentication_Passed				+ New AND	OR			
Non_Cisco_Profiled_Phones		Set to "Is not"		Dup		uplicate	Sav	
Non_Compliant_Devices								
Switch_Local_Web_Authentication								
Switch_Web_Authentication								
Wired_802.1X								
Wired_MAB Ø								
				Results				
Rule Name Conditions				Results Profiles	Security Groups		Hits	Action
Rule Name Conditions MAB_LDAP AND L Map_mab-description CONTAINS L Map_mab-description CONTAINS L Map_mab-description CONTAINS	Radius NAS-Port-Id Vetwork Access Netw	#orkDeviceName		Results Profiles *MACPORTSWITCHLDAP	Security Groups	- 8	Hits	Action

Dopo aver applicato la configurazione, è possibile connettersi alla rete senza l'intervento dell'utente.

Verifica

Una volta connessi alla porta dello switch designata, è possibile digitare show authentication session interface Gigabit Ethernet X/X/X details per convalidare lo stato di autenticazione e autorizzazione del dispositivo.

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 ISE consente di usare Radius Live Logs per la conferma.

C	Refresh O 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			

Risoluzione dei problemi

Sul server LDAP, verificare che l'indirizzo Mac, il nome dello switch e la porta dello switch del dispositivo creato siano stati configurati correttamente

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						

Ad ISE, è possibile acquisire un pacchetto (andare a **Operazioni->Risoluzione dei problemi->Strumento diagnostico->Dump TCP**) per verificare che i valori vengano inviati da LDAP ad ISE

27	134,204090	18.81.127.189	18,81,127,111	LENP	201	searchinguest121 "Rongpladevices,80-classeen,80-lat" whilefalletime	
28	124.308017	38.40.127.111	38,81,127,300	LEMP	252	searchiesExtry(2) *OH-Laptophert,00-Applatencies,80-clacations,00-clat* searchiesDenci2) secons	
29	324.303291	16.40.127.049	38,81,127,113	LEHP	231	sear-thepast131 "Bodgstebectors,30-classion,30-fait" whitebattree	
	124, 128281	18.81.127.111	18,81,127,189	1.010	110	unard/Andistry(3) "Objaging/ext, Objaging/ext, St-ciacadess, St-cial" unard/Andisectation -	4
31	124,301373	18.81.107.189	18,81,127,111	LENP	100	overthinguestial "Budgpielewices, Dicissione, Dicist" wholeholdree	
32	124,305384	14.41.127.111	18,81,127,189	LEMP	- 18	searchicologiai accoss (2 results)	
33	121.404145	10.00.007.089	38.41.101.111	1.544	1000	searchiles.est (N) "Riskarlahevises. Nuclearates. Mulait" statistication	
					-	constant accepted accepted accepted	
	* attribut	tes: 3 items					
	V Parts	aMUVIAME.Ist lite	 description 				
	1.0	pel description					
	7.14	fail 1 sham					
		Annohulation and	tchop/Texcomect_Gaph	at the rest of	8.4		
	 Parti 	INTERNAL INCOME.	e distinguisheddane				
	14	or: distinguished an	10 C				
	F 148	fact 1 liters					
		Anto-DutaWalters (Sec.	Laster/Test_Minkas/atlev	term. Here the	-	n, Novian	
	 Pariti 	addentributed but item	a manifestration				
	1.	call machiness					
	7.10	fact 1 them					
		Attributelial are Afri	82-AP-34-AP-87				
			11				