為FDM管理的FTD上的RAVPN配置LDAP屬性對 映

目錄
· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
採用元件
身份驗證流程
LDAP屬性對映流說明
<u>設定</u>
FDM的配置步驟
LDAP屬性對映的配置步驟
疑難排解
相關資訊

簡介

本文檔介紹使用輕量級目錄訪問協定(LDAP)伺服器對遠端訪問VPN(RA VPN)使用者進行身份驗證 和授權,並根據使用者在LDAP伺服器上的組成員資格授予他們不同的網路訪問許可權的過程。

必要條件

需求

- 防火牆裝置管理器(FDM)上的RA VPN配置基礎知識
- 有關FDM上的LDAP伺服器配置的基本知識
- 演示狀態傳輸(REST)應用程式介面(API)和FDM Rest API資源管理器的基本知識
- 由FDM管理的Cisco FTD 6.5.0版或更高版本

採用元件

使用了下列應用程式/裝置的硬體和軟體版本:

- Cisco FTD版本6.5.0,內部版本115
- Cisco AnyConnect版本4.10
- Microsoft Active Directory(AD)伺服器
- Postman或任何其他API開發工具

Ŷ 注意:思科不提供對Microsoft AD Server和Postmal工具的配置支援。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

身份驗證流程



LDAP屬性對映流說明

- 1. 使用者發起與FTD的遠端存取VPN連線,並為其Active Directory(AD)帳戶提供使用者名稱和密 碼。
- 2. FTD透過連線埠389或636(透過SSL的LDAP)將LDAP要求傳送到AD伺服器
- 3. AD會使用與該使用者相關聯的所有屬性回覆FTD。
- 4. FTD將接收的屬性值與在FTD上建立的LDAP屬性對映相匹配。這是授權過程。
- 5. 然後,使用者連線並繼承與LDAP屬性對映中的memberOf屬性匹配的Group-Policy的設定。

在本文檔中,使用memberOf LDAP屬性對AnyConnect使用者進行授權。

- 每個使用者的LDAP伺服器中的memberOf屬性被對映到FTD上的IdapValue實體。如果使用者 屬於匹配的AD組,則使用者將繼承與該IdapValue關聯的組策略。
- 如果使用者的memberOf屬性值與FTD上的任何IdapValue實體不匹配,則會繼承所選連線配置檔案的預設Group-Policy。在本示例中,NOACCESS Group-Policy繼承到。

設定

FDM管理的FTD的LDAP屬性對映配置了REST API。

FDM的配置步驟

步驟 1.驗證裝置是否已註冊到智慧許可。



步驟 2.驗證FDM上是否已啟用AnyConnect許可證。

wice Summary mart License		
CONNECTED Last sync: 11 Oct 2019 09:33 AM SUFFICIENT LICENSE Next sync: 11 Oct 2019 09:43 AM	0	Go to Cloud Services O
BSCRIPTION LICENSES INCLUDED		
Threat	DISABLE	Malware
S Enabled		Disabled by user
This License allows you to perform intrusion detection and prevention and file must have this license to apply intrusion policies in access rules. You also mu license to apply file policies that control files based on file type.	e control. You ist have this	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🖏 Intrusion Policy		Includes: C File Policy
URL License	DISABLE	RA VPN License Type PLUS V DISABLE
C Enabled		C Enabled
This license allows you to control web access based on URL categories and in than by individual URL alone. You must have this license to deploy access rule traffic based on category and reputation.	reputations, rather es that filter web	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: URL, Reputation		Includes: RA-VPN
RPETUAL LICENSES INCLUDED		
Base License	ENABLED ALWAYS	
C Enabled		
This perpetual license is included with the purchase of the system. You must	have this license	

步驟 3.驗證權杖中是否啟用匯出控制功能Enabled。

CISCO. Firepower D	evice Manager Monitoring Polic	es Objects Device: firepower
	Device Summary Smart License	Assigned Virtual Account: Export-controlled features: Enabled Go to Cisco Smart Software Manager.
	CONNECTED Last SUFFICIENT LICENSE Next	sync: 11 Oct 2019 09:33 AM sync: 11 Oct 2019 09:43 AM
	SUBSCRIPTION LICENSES INCLUDED	
	Threat	DISABLE
	This License allows you to perform intr	sion detection and prevention and file control. You
	must have this license to apply intrusio license to apply file policies that contro	policies in access rules. You also must have this files based on file type.
	Includes: 🌯 Intrusion Policy	

✤ 注意:本文檔假設RA VPN已配置。有關如何在FDM管理的FTD上配置<u>RAVPN的詳細資訊</u> <u>,請參閱以下文檔。</u>

步驟 4.導航到Remote Access VPN > Group Policies。

CISCO. Firepower Device Manager Monitoring Police	s Objects Device: firepower	S. 🚑 🕲 ? : admin Administrator	. ×
و ب	01 Cisco ASA5545-X Threat Defense @ Marr 0/7 0/5 0 @ Condoxt 0/6 0/4 0 000	AC2 0/1 CONS Server CMS Server CMS Server CMS Server CMS Server CMS Server CMS Server CMS Server	
Interfaces Connected Enabled 3 of 9 View All Interfaces	Routing 2 routes View Configuration	Updates System Settings Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds Logging Settings View Configuration DHCP Server	
Smart License Registered View Configuration	Backup and Restore	Troubleshoot No files created yet REQUEST FILE TO BE CREATED RECOURST FILE TO BE CREATED URL Filtering Preferences	
Site-to-Site VPN 1 connection View Configuration	Remote Access VPN Configured 2 connections 5 Group Policies View Configuration >	Advanced Configuration Device Administration Includes: FlexConfig. Smart CLI Audit Events, Deployment History, Download Configuration View Configuration >	>

步驟 5.導航到組策略。按一下「+」為每個AD組配置不同的組策略。在本示例中,將組策略 Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy配置為可以訪問不同的子網。

Firepower Device Ma	mar 🔊		~ ~	admin 🗸
cisco.	Add Group Policy			* Administrator
RA VPN ← Connection Profiles	Q, Search for attribute	Name Finance-Group-Policy		
a Group Policies	Basic	I manifed Group I olicy	- 1	+
	General	Description	- 1	CLIENT PROFILES ACTIONS
	Session Settings	I mance caer croop	11	
	Advanced	DNS Server	- 1	
	Address Assignment	Select DNS Group	~	
	AnyConnect	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session	- 1	
	Traffic Filters			
	windows browser Proxy	Default domain		
		AnyConnect client profiles		
		CANCEL	ок	

Finance-Group-Policy具有以下設定:

<#root>

firepower#

show run group-policy Finance-Group-Policy

group-policy Finance-Group-Policy internal

group-policy Finance-Group-Policy attributes banner value You can access Finance resource dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelspecified ipv6-split-tunnel-policy tunnelall

split-tunnel-network-list value Finance-Group-Policy|splitAcl

split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
<output omitted>

同樣,HR-Group-Policy具有以下設定:

<#root>

firepower#

show run group-policy HR-Group-Policy

```
group-policy HR-Group-Policy internal
group-policy HR-Group-Policy attributes
banner value You can access Finance resource
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy tunnelall
```

split-tunnel-network-list value HR-Group-Policy|splitAcl

```
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
```

最後, IT-Group-Policy具有下一個設定:

<#root>

firepower#

show run group-policy IT-Group-Policy

```
group-policy IT-Group-Policy internal
group-policy IT-Group-Policy attributes
banner value You can access Finance resource
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy tunnelall
```

split-tunnel-network-list value IT-Group-Policy splitAcl

```
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
<output omitted>
```

步驟 6.建立組策略NOACCESS並導航到Session Settings,然後取消選中Simultaneous Login per User選項。這會將vpn-simultaneous-logins值設定為0。

設定為0時,Group-Policy中的vpn-simultaneous-logins值將立即終止使用者的VPN連線。 此機制 用於防止屬於任何AD使用者組(已配置使用者組除外)(在本例中為Finance、HR或IT)的使用者 建立到FTD的成功連線,並訪問僅可用於允許的使用者組帳戶的安全資源。

屬於正確AD使用者組的使用者匹配FTD上的LDAP屬性對映並繼承對映的組策略,而不屬於任何允 許組的使用者則繼承連線配置檔案的預設組策略,在本例中為NOACCESS。

Add Group Policy		3	\times	
Q Search for attribute	NoACCESS			
Basic	Description			I
General Session Settings	To avoid users not belonging to correct AD group from connecting to VPN	/	4	
Advanced	DNS Server			I
Address Assignment	Select DNS Group	~		I
Split Tunneling AnyConnect Traffic Filters	Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session	/	1	
Windows Browser Proxy	Default domain			
	AnyConnect client profiles + CANCEL	OK		,

Edit Group Policy				@ X
Q Search for attribute	Maximum Connection Time	minutes	Connection Time Alert Interva	al minutes
Basic	1-4473924		1-30; (Default: 1)	
General	Idle Time		Idle Alert Interval	
Session Settings	30	minutes	1	minutes
Advanced	1-35791394; (Default: 30)		1-30; (Default: 1)	
Address Assignment	Simultaneous Login per U	ser		
Split Tunneling				
AnyConnect	1-2147483647; (Default: 3)			
Traffic Filters				
Windows Browser Proxy				
			CANCEL	ок

NOACCESS Group-Policy具有以下設定:

<#root>

firepower# show run group-policy NOACCESS group-policy NOACCESS internal group-policy NOACCESS attributes dhcp-network-scope none vpn-simultaneous-logins 0 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-dns none split-tunnel-all-dns disable client-bypass-protocol disable msie-proxy method no-modify vlan none address-pools none ipv6-address-pools none webvpn anyconnect ssl dtls none anyconnect mtu 1406 anyconnect ssl keepalive 20 anyconnect ssl rekey time 4 anyconnect ssl rekey method new-tunnel anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect profiles none anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting

步驟 7.導航到Connection Profiles並建立Connection-Profile。在此示例中,配置檔名稱為Remote-Access-LDAP。選擇Primary Identity Source AAA Only,然後建立新的身份驗證伺服器類型AD。



輸入AD伺服器的資訊:

- 目錄使用者名稱
- 目錄密碼
- 基本DN
- ・ AD主域
- 主機名/IP地址
- 連接埠
- 加密型別

Add Identity Realm

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре
LDAP-AD	Active Directory (AD)
Directory Username	Directory Password
administrator@example.com	
e.g. user@example.com	
Base DN	AD Primary Domain
dc=example,dc=com	example.com
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
192.168.100.125:389	•
Hostname / IP Address	Port
192.168.100.125	389
192.168.100.125 e.g. ad.example.com	389
192.168.100.125 e.g. ad.example.com Interface	389
192.168.100.125 e.g. ad.example.com Interface inside_25 (GigabitEthernet0/1)	389
192.168.100.125 e.g. ad.example.com Interface inside_25 (GigabitEthernet0/1) ~ Encryption	389 Trusted CA certificate
192.168.100.125 e.g. ad.example.com Interface inside_25 (GigabitEthernet0/1) Encryption NONE	389 Trusted CA certificate Please select a certificate ✓
192.168.100.125 e.g. ad.example.com Interface inside_25 (GigabitEthernet0/1) Encryption NONE TEST	389 Trusted CA certificate Please select a certificate
192.168.100.125 e.g. ad.example.com Interface inside_25 (GigabitEthernet0/1) Encryption NONE TEST Add another configuration	389 Trusted CA certificate Please select a certificate ✓

按一下Next,然後選擇NOACCESS作為此連線配置檔案的預設組策略。

altalta cisco.	Firepower Device Manager	Monitoring	Policies	Objects	Device: firepower	(Σ)		?	:	admin Administrator	~
		A group policy is a VP!	R collection of connection	emote Use user-oriented ses is established. Se	er Experience ssion attributes which an lect or create a Group Pi	e assigned to client wher olicy object.	а				
		View Group Policy]		_		′				
		Finance-Gr	oup-Policy			0	^				
		HR-Group-	Policy			0					
		IT-Group-P	olicy			0					
		NOACCESS				0					
		SSLVPN				0					
		Create new Group P	olicy								
				BACK	NEXT Unlimited 7.1 Min						

儲存所有更改。連線配置檔案Remote-Access-LDAP現在在RA VPN配置下可見。

cisco.	Firepower Devi	ce Manag	er Monitoring	Ø Policies	∺. Objects	Device: firepower		admin Administrator
RA	VPN	← [Device Summary Remote Acc	ess VPN	Connec	tion Profiles		
Co	nnection Profiles		ablaat				O Saarah	
e9	Group Policies		object				Q Search	Ť
			# NAME			АЛА	GROUP POLICY	ACTIONS
			1 Remote-Acce	ss-LDAP		Authentication: AAA O Authorization: None Accounting: None	NOACCESS]

LDAP屬性對映的配置步驟

步驟 1. 啟動FTD的API Explorer。

API Explorer包含FTD上可用的API的完整清單。導覽至https://<FTD Management IP>/api-explorer 向下滾動到LdapAttributeMap部分,然後按一下它以檢視所有支援的選項。

 	⊙ 👽 🏡 https://	😇 🛧 Q. Search
CISCO. Firepower Devi	ce Manager Monitoring Policies Objects Device:	: firepower
FTD REST API 🗧 🗧	LdapAttributeMap	Show/Hide List Operations Expand Operations
	GET /object/idapattributemaps	
API Explorer	POST /object/ldapattributemaps	
Error Catalog	/object/ldapattributemaps/{objld}	
	<pre>/object/ldapattributemaps/{objld}</pre>	
	PUT /object/ldapattributemaps/{objld}	

✤ 注意:在本示例中,我們使用Postman作為API工具來配置LDAP屬性對映。

步驟 2.為LDAP授權新增Postman集合。



輸入此集合的名稱。

Runner	🖡 🔻 👪 My Workspace 👻 🚑 Invite		e ¢			
Q Filter	CREATE A NEW COLLECTION		× on	nent	• O	*
History Collections /	Name					
+ New Collection	FTD-6.5.0 LDAP Authorization					
-	Description Authorization Pre-request Scripts Tests Variables					
	This description will show in your collection's documentation, along with the descriptions of its folders and requests.					
You don't have any collection	Make things easier for your teammates with a complete collection description.					
Collections let you group related requination making them easier to access and r						
+ Create a collection						
	Descriptions support Markdown					
	Cancel	Create				
	ô Boot	tcamp	Build		/se 🔹 🛀	0

編輯 Authorization 頁籤並選擇 OAuth 2.0型別

Collections History Collections Name FTD-6.5.0 LDAP Authorization Description This authorization method will be used for every request in this collection. You can override this by specifying one in the request. Type Outh 2.0 The authorization data will be automatically generated when working in a collaborative environment, we recommend using variables. Authorization Authorization Authorization	*
TYPE Image: Constraint of the second sec	
Request Headers Get New Access Token	
Cancel Update	

步驟3. 導覽至File > Settings,關閉SSL憑證驗證,以避免在向FTD傳送API要求時發生SSL交握失 敗。如果FTD使用自簽名的憑證,則會完成此操作。



File Edit View Help	
New	Ctrl+N
New Tab	Ctrl+T
New Postman Window	Ctrl+Shift+N
New Runner Window	Ctrl+Shift+R
Import	Ctrl+O
Settings	Ctrl+Comma
Close Window	Ctrl+Shift+W
Close Tab	Ctrl+W
Force Close Tab	Alt+Ctrl+W
Exit	

SETTINGS

G	eneral	Themes	Shortcuts	Data	Add-ons	Certificates	Proxy	Update	About	
	REQUES	т				HEADERS				
	Trim key	s and values i	n request body	0	OFF	Send no-cache he	ader		C ON	
	New Coo	le Generation	Mode) ON	Send Postman To	ken header		C ON	
	Use next	generation U	RL processing	a) OFF	Retain headers w	hen clicking	on links	OFF	
[SSL certi	ficate verificat	sion	0	OFF	Automatically foli	ow redirect	s	C ON	
	Always o	pen requests	in new tab	0	OFF	Send anonymous	usage data	to Postman	C ON	
	Always a	sk when closi	ng unsaved tab) ON	USER INTERFACE				
	Languag	e detection		AL	no 🔻	Editor Font Size (g	200)		12	
	Request	timeout in ms		0		Two-pane view			OFF	
	Set how	long a reques	t should wait fo	ra		Show icons with t	ab names		C ON	
	time out	, set to 0.	8 over 10 nevel			Variable autocom	plete			
	Max resp	oonse size in M	ЛВ	51	0	Enable Launchoa	d			
	Set the n	naximum stae	of a response t	0						

或者,FTD使用的憑證可以作為CA憑證新增到設定的「憑證」一節中。

SETTINGS								×
General	Themes	Shortcuts	Data	Add-ons	Certificates	Proxy	Update	About
CA Certificates The file should consist of one or more trusted certificates in PEM format. PEM file Select File						OFF		
Client Cer	tificates							Add Certificate

Learn more about working with certificates at our Learning Center.

×

步驟 4. 新增一個POST要求Auth,以建立到FTD的登入POST要求,從而取得權杖來授權任何 POST/GET要求。



Add Head	eader Preset			
	KEY	VALUE	DESCRIPTION	••• Bulk Edit
	Content-Type	application/json		
	Accept	application/json		
	Кеу	Value	Description	
			C	ancel Add

對於所有其他請求,請導航到相應的報頭頁籤,然後選擇此「預設報頭」值:Header-LDAP,使 REST API請求使用json作為主要資料型別。

要獲取令牌的POST請求正文必須包含下一個:

類型	raw - JSON(application/json)
grant_type	密碼
使用者名稱	用於登入FTD的管理員使用者名稱
密碼	與管理員使用者帳戶關聯的密碼

{	
	"grant_type": "password",
	"username": "admin",
	"password": " <enter password="" the="">"</enter>
}	



×

按一下send後,回應的主體就會包含存取權杖,用於向FTD傳送任何PUT/GET/POST請求。

Body Cool	okies (1) Headers (16) Test Results Statu	us: 200 OK	Time: 430 ms	Size: 1.52 KB	Save Response	•
Pretty	Raw Preview Visualize JSON 👻 📅					2
1 ~ { 2	"access token":				10 M 100 1 C3	ľ
	TeyJhb6c101J1 leHAi0jE100k3				S0xMWVhLTgw	
	ZGItNzk4NjAzNm W0d2uzeKNU 30FSWTvmxeS0dkr]akCXvP4Lvzdr-xap0".	luIn0.				L
3	"expires in": 1800,					1.
4	"token_type": "Bearer",					
5	"refresh_token":					
	"eyJhbGci0iJIU:				NzA4NDEyLCJ	
	leHAiOjE10Dk3M1				WlkIjoiZWNi	
	NzY1ZjMtNTUyZS(luIn0.		
	lHcHKAx7LhPfDNO_IyUxDxN-9U1h18Uhq0wp9aRJHHk",					
6	"refresh_expires_in": 2400					
7 }						

{
 "access_token": "eyJhbGci0iJIUzI1[...output omitted...]dkrJakCXvP4Lyzdr-xap0",
 "expires_in": 1800,
 "token_type": "Bearer",
 "refresh_token":"eyJhbGci0iJIUzI1[...output omitted...]dkrJakCXvP4Lyzdr-xap0",
 "refresh_expires_in": 2400
}

然後,此令牌用於授權所有後續請求。

導航到每個新請求的Authorization頁籤,然後選擇下一個請求:

類型	OAuth 2.0
權杖	通過運行登入POST請求接收的訪問令牌

Params	Authorization	Headers (13)	Body 鱼	Pre-request Script	Tests	Settings Cooki	as Code
TYPE OAuth	2.0		•	Heads up! These pa variables. Learn mo	rameters hole re about varia	l sensitive data. To keep this data secure while working in a collaborative environment, we recommend us ibles	ng X
The auth generate about au Add auth Reques	orization data will be au d when you send the re thorization norization data to st Headers	utomatically equest. <mark>Learn more</mark>	Ŧ	Access Token		eyjhbGciOiJlUz11Nij9.eyjpYXQiOjE1ODk3MDg0MTIsinN1YiI6imFkbWluli wianRpijoiNjgwM2EyWzMtOTgyMi0xMWVhLWJhNzct0DFmYjYzYmE1N2 MxliwibmjmijoxTg5Nz4AND5yLCJlEHAIOjE1ODk3MTAyMTisinJIZnJL2 hUb2tlbkV4cGlyZXNBdCI6MTU4OTcxMDgxMjk2MCwidG9rZW5UeXBiljo ISIdUXOFJYZVzcylsinVzZXJVdWikijoiZWNINzY1ZJMtNTUyZS0xMWVhLTg wZGItkzk4NJAZNmMyZmUwlwidXNLIQhGCU07KXR0FETUOliwib3Jp Z2luljoIcGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.W0d2uzeKWL3p FSWTymxgSOdkrJakCXvP4Lyzdr-xap0	¥
Body Co	okies (3) Headers (1	7) Test Results				Status: 200 OK Time: 328 ms Size: 2.29 KB Save Resp	onse 🔻

步驟 5.新增新的GET請求Get Group-Policies以獲取Group-Policy狀態和設定。收集每個已配置的組 策略的名稱和ID(在本例中為: Finance-Group-Policy、HR-Group-Policy和IT-Group-Policy),以便 在下一步中使用。

獲取已配置的組策略的URL為:<u>https://<FTD Management</u> IP>/api/fdm/latest/object/ravpngrouppolicies

在下一個示例中,將突出顯示Group-Policy Finance-Group-Policy。



步驟 6.新增新的POST請求建立LDAP屬性對映以建立LDAP屬性對映。在本文檔中,使用模型 LdapAttributeMapping。其他模型也有類似的操作和方法,用於建立屬性對映。這些型號的示例可 以在本文檔前面提到的api-explorer中找到。

FTD REST API	LdapAttributeMap	Show/Hide	List Operations	Expand Operations
API Explorer	GET /object/ldapattributemaps			
	Posr /object/ldapattributemaps			
Error Catalog				
	Implementation Notes This API call is not allowed on the standby unit in an HA pair.			
	Response Class (Status 200)			
	Model Example Value			
	LdapAttributeMapping description: Nested Entity which includes common objects for LdapAttributeMapping (Note: The field level constraints listed here might not co	over all the const	raints on the field.	Additional
	constraints might exist.)			
	Field level constraints: cannot be null, must match pattern ^((?!;).)*\$. (Note: Additional constraints might exist),			
	ciscoName (string): An enum value that is the Cisco attribute name that maps to the customer-specific attribute name.			
	Field level constraints: cannot be null. (Note: Additional constraints might exist) = l'access Hourse' (all ow network extension Mone: 'auth service type' 'authenticated user interout' 'autheout	RIZATION REOL	IRED' AUTHORIZA	ATION TYPE
	'BANNERT', 'BANNERZ', 'CISCO_AV_PAIR', 'CISCO_IP_PHONE_BYPASS', 'CISCO_LEAP_BYPASS', 'CLIENT_BYPASS_PROTOCOL', 'CLIENT_	INTERCEPT_DHC	P_CONFIGURE_M	SG',
	'CLIENT_TYPE_VERSION_LIMITING', 'CONFIDENCE_INTERVAL', 'DHCP_NETWORK_SCOPE', 'DN_FIELD', 'DISABLE_ALWAYS_ON_VPN', 'FIRI	EWALL_ACL_IN',	'FIREWALL_ACL_O	OUT',
	'GATEWAY_FQDN', 'GROUP_POLICY', 'IE_PROXY_BVPASS_LOCAL', 'IE_PROXY_EXCEPTION_LIST', 'IE_PROXY_METHOD', 'IE_PROXY_SERV'	ER', 'IETF_RADIU	S_CLASS',	
	IET_KADIOS_FILTER_ID, IET_KADIOS_FKAMEU_IP_ADURESS, IET_KADIOS_FKAMEU_IP_NETMASK, IET_KADIOS_FKAMEU_IP_VO_TKETA, IE IFTE RADIUS_INTERPEACE ID'IETE RADIUS_FKAMEU_IP'_ADURESS, IETERADUS_FKAMEU_IP'_NETMASK, IETE/KADIOS_INTERADIOS_F	IF_RADIUS_IDLE	LIOW PASSWD S	TORF'
	IPSEC_AUTH_ON_REKEY, IPSEC_AUTHENTICATION, IPSEC_BACKUP_SERVER_LIST, IPSEC_BACKUP_SERVERS', IPSEC_CLENT_FIREV	WALL_FILTER_NA	ME',	
	'IPSEC_CLIENT_FIREWALL_FILTER_OPTIONAL', 'IPSEC_DEFAULT_DOMAIN', 'IPSEC_EXTENDED_AUTH_ON_REKEY', 'IPSEC_IKE_PEER_ID_(CHECK', 'IPSEC_I	P_COMPRESSION	s
	"IPSEC_IPV6_SPLIT_TUNNELING_POLICY", "IPSEC_MODE_CONFIG", "IPSEC_OVER_UDP", "IPSEC_OVER_UDP", "IPSEC_REQUIRED_LL	IENT_FIREWALL	CAPABILITY',	
	IPSEC_SMLI_DNS_NAMES, IPSEC_SMLI_TUNNEL_ALL_DNS, IPSEC_SMLI_TUNNEL_LIST, IPSEC_SMLI_TUNNELING_PULICY, IPSEC IPVE DEIMARY DNS' IPVE SCONDARY DNS'' I 27D ENCRYPTION' 127D MDC COMPRESSION' MS CHENT SHRNET MASK' PES	REQUIRED' 'PP	TP ENCRYPTION	ROUP_LOCK',
	"PTP_MPPC_COMPRESSION", WEBVPN_VLAN",	_nedonep , 11	in _choich hold,	
	valueMappings (Array[LdapToCiscoValueMapping]): A list of LdapToCiscoValueMapping objects, which specify the value mappings for this L	DAP attribute.		
	Field level constraints: cannot be null. (Note: Additional constraints might exist),			
	type (string): loapatributemapping			
	LapAttributeToGroupPolicyMapping			
	description: An LDAP attribute to group policy mapping defines a customer-specific LDAP attribute name and maps it to a specific group poli	cy object. Use th	is nested entity in a	an LDAP attribute
	map. (Note: The field level constraints listed here might not cover all the constraints on the field. Additional constraints might exist.)			
	IdapName (string): The customer-specific LDAP attribute name that is being mapped.			
	Hero lever constraints: cannot be null, must match pattern "(17:1).75. (Note: Additional constraints might exist), unauthorations (destroyunghterouthorationation): A list of Lidor Consumption objects which especify the value to or	un nolicu manni	one for this I DAD a	ttribute
	Field level constraints: cannot be null. (Note: Additional constraints might exist),	rop poncy mappi	ingo non unio EDAP di	concere.
	type (string): Idapattributetogrouppolicymapping			
)			

LDAP屬性對映的URL為: <u>https://<FTD Management IP>/api/fdm/latest/object/ldapattributempps</u>

POST請求正文必須包含以下內容:

名稱	LDAP屬性對映的名稱
類型	Idapattributeapping
ldap名稱	memberOf
ciscoName	GROUP_POLICY
ldap值	來自AD的使用者的memberOf值
ciscoValue	FDM中每個使用者組的組策略名稱



POST請求的主體包含根據memberOf值將特定組策略對映到AD組的LDAP屬性映射信息:

```
{
  "name": "Attribute-Map",
  "ldapAttributeMaps":
  Ε
      ł
      "ldapName": "memberOf",
"ciscoName": "GROUP_POLICY",
      "valueMappings":
      Ε
        {
          "ldapValue": "CN=Finance-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "Finance-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=HR-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "HR-Group-Policy",
          "type": "ldaptociscovaluemapping"
        },
        {
          "ldapValue": "CN=IT-Group,CN=Users,DC=cisco,DC=com",
          "ciscoValue": "IT-Group-Policy",
          "type": "ldaptociscovaluemapping"
        }
      ],
        "type": "ldapattributemapping"
      }
 ],
    "type": "ldapattributemap"
 }
```

此POST請求的響應看起來與下一個輸出類似:



步驟 7.新增新的GET請求以獲取FDM上的當前AD領域配置。

獲取當前AD領域配置的URL為: <u>https://<FTD Management IP>/api/fdm/latest/object/realms</u>



步驟 8.建立新的PUT請求以編輯AD領域。 複製上一步的GET響應輸出,並將其新增到此新PUT請 求的正文中。此步驟可用於對當前AD領域設定進行任何修改,例如:更改密碼、IP地址或新增任何 鍵(如IdapAttributeMap)的新值。

注意:複製專案清單的內容,而不是複製整個GET響應輸出非常重要。PUT請求的「請求 URL」必須附加有對其進行了更改的對象的專案ID。在本例中,值為:bf50a8ab-9819-11eaba77-d32ecc224295

用於編輯當前AD領域配置的URL為:<u>https://<FTD Management</u> IP>/api/fdm/latest/object/realms/<realm ID>

PUT請求的主體必須包含以下內容:

版本	從之前的GET請求的響應獲取的版本
id	從之前的GET請求的響應獲取的ID
ldap屬性對映	來自建立LDAP屬性對映請求的響應的Idap-id



此範例中的組態主體為:

<#root>

```
"version": "ks3p4he5ixiyy",
   "name": "LDAP-AD",
   "directoryConfigurations": [
     {
       "hostname": "<IP Address>",
       "port": 389,
       "encryptionProtocol": "NONE",
       "encryptionCert": null,
       "type": "directoryconfiguration"
     }
   ],
   "enabled": true,
   "systemDefined": false,
   "realmId": 3,
   "dirUsername": "administrator@example.com",
   "dirPassword": "*******",
   "baseDN": "dc=example, dc=com",
    "ldapAttributeMap" :
{
   "id": "b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c",
   "type": "ldapattributemap"
},
   "adPrimaryDomain": "example.com",
   "id": "bf50a8ab-9819-11ea-ba77-d32ecc224295",
   "type": "activedirectoryrealm",
   "links": {
     "self": "https://
```

/api/fdm/latest/object/realms/bf50a8ab-9819-11ea-ba77-d32ecc224295"

} }

驗證IdapAttributeMap id是否與此請求的響應正文中匹配。



(可選)。可以使用PUT請求修改LDAP屬性對映。建立新的PUT請求Edit Attribute-Map,並進行 任何更改,如Attribute-Map或memberOf值的名稱。T

在下一個示例中,所有三個組的Idapvalue的值都已從CN=Users更改為CN=UserGroup。

* B	6 requests	PUT	https://www.interestoligent/departs/bugen	Send • Sav	ve +
N	er Auch	Param	ns Authonization Headers (11) Body Pre-request Script Tests Settings	Cookie	es Code
•	If Get Group-Policies	0 n	one @ form.data @ xwww.form.unlencoded @ raw @ binary @ GraphQL j50N *		leautity
6	Create LDAP Attribute Map				
	GET AD Realm	÷.	"nert (with a statistic)"		- 1
	Edit AD Realm	- 4	name : Activitetes app, 1		
	# Edit Attribute-Map	5	E.		
_		7	"Ldsphane": "memberOf",		
			Clscower' Discoversity Clscr,		
		10	E.		
		12	"Ideovalue": "ON-Enance-Group.CH-UserGroup.DC+cisco.DC+com".		
		13	"Cisconalue": "#Leance-Group-Policy",		
		14	"type": "Isoptociscovaluemopiling"		
		16			
		17	"lagvalue": "Count_droup_ChuiserGroup_ChuiserGroup_Chuises, to the second secon		
		19	"type": "Lawtociscowaluewapsig"		
		20) e 		
		22	"ldsp/slue": "CH=IT-Group,Ch=UserGroup,Ct=Clsco,Ct=Com",		
		23	"cisconlag": "I'-decop-Policy",		
		25			
		26	b'		
		27	"type": "Lispattributemapping"		
		29			
		30	"18": "82347000-9844-1182-0877-50265544000",		
		31	<pre>"type:"logpetrigouremap", "lnest"</pre>		
		33	"st1f": "https://10.197.224.99/ap1/fdm/latest/object/ldapattributemaps/b2147cde-904a-11ea-ba77-5b2ed5c4abdc"		
		34			

(可選)。要刪除現有LDAP屬性對映,請建立DELETE請求刪除屬性對映。包括來自上一個 HTTP響應的map-id,並將其與刪除請求的基本URL附加。

н	istory Collections	APIs	> Delete Attribute-Map			Comments 0	Examples (0) +
+	New Collection FTD-6.5.0 LDAP Authorization	Trash	DELETE * Propulsi Papinom/latest/object/dapattributemaps/s/2147cde-884a-11ea-ba7	77-So2euScAeu8c		Send •	Save +
7 requests			Params Authorization Headers (7) Body Pre-request Script Tests Settings				Cookies Code
*0	ar Auth		Query Params				
- 64	Get Group-Policies		KEY .	VALUE	DESCRIPTION		+++ Buik Edit
*0	Create LDAP Attribute Map		Key	Value	Description		
	GET AD Realm		Response				
2	Edit AD Realm						
	Delate Attribute-Andp						

◆ 註:如果memberOf屬性包含空格,則必須對屬性進行URL編碼,以便Web伺服器對其進行分析。否則會收到400錯誤要求HTTP回應。對於包含空格字元的字串,「%20」或「+」可用於避免此錯誤。

步驟 9.導航回到FDM,選擇「部署」圖示,然後按一下「立即部署」。

Pending Changes	8 ×
Last Deployment Completed Successfully 17 May 2020 07:46 PM. See Deployment History	
Deployed Version (17 May 2020 07:46 PM)	Pending Version (LEGEND
Idapattributemap Added: Attribute-Map	•
- - - - - - -	<pre>ldapAttributeMaps[0].ldapName: memberOf ldapAttributeMaps[0].valueMappings[0].ldapValue: CN=IT-Gr ldapAttributeMaps[0].valueMappings[0].ciscoValue: IT-Grou ldapAttributeMaps[0].valueMappings[1].ldapValue: CN=HR-Gr ldapAttributeMaps[0].valueMappings[1].ciscoValue: HR-Grou ldapAttributeMaps[0].valueMappings[2].ldapValue: CN=Finan ldapAttributeMaps[0].valueMappings[2].ciscoValue: Finance ldapAttributeMaps[0].ciscoName: GROUP_POLICY name: Attribute-Map</pre>
Active Directory Realm Edited: LDAP-AD ldapAttributeMap: -	Attribute-Map
MORE ACTIONS V	CANCEL DEPLOY NOW V

驗證

可以在FDM的部署歷史記錄部分驗證部署更改。

Firepower Device Manager	Monitoring Policies Objects Device: firepower	S admin Administrator
Device ← Administration	Deployment Completed: User (admin) Triggered Deployment Summary Differences View	t
Audit Log Download Configuration	Deployed Version	Pending Version
	Idapattributemap Added: Attribute-Map Entity ID: b2147c0e-984a-11ea-ba77-5b2ed5c4ab8c	
	- - - - - - - - - - - - -	<pre>ldapAttributeMaps[0].ldapName: memberOf ldapAttributeMaps[0].valueMappings[0].ldapValue: CN-Finan ldapAttributeMaps[0].valueMappings[0].ciscoValue: Finance_ ldapAttributeMaps[0].valueMappings[1].ciscoValue: CN-IT-Gr ldapAttributeMaps[0].valueMappings[2].ciscoValue: TN-Grou ldapAttributeMaps[0].valueMappings[2].ciscoValue: CN-RR-Gr ldapAttributeMaps[0].valueMappings[2].ciscoValue: NR-Grou ldapAttributeMaps[0].valueMappings[2].ciscoValue: NR-Grou ldapAttributeMaps[0].valueMappings[2].ciscoValue: NR-Grou ldapAttributeMaps[0].ciscoName: GROUP_POLICY name: Attribute-Map</pre>
	Active Directory Realm Edited: LDAP-AD Entity ID: 0f50a8ab-9819-11ea-ba77-d32ecc224295	
	Idapattributenap: -	Attribute-Map

為了測試此配置,請在使用者名稱和密碼欄位中提供AD憑據。

當屬於AD組Finance-Group的使用者嘗試登入時,該嘗試按預期成功。

		Scisco AnyConnect Secure Mobility Client –	\times
Cisco AnyConnect 10.197.22	3.149 ×	VPN: Contacting Connect	
Password: ******	OK Cancel	Roaming Security: You are protected by Umbrella. DNS queries are encrypted.	
		\$ (i)	

	Sisco AnyConnect Secure Mobility Client	- 🗆 X
	AnyConnect Secure Mobility Client	0
Sisco AnyConnect Secure Mobility Client − □ ×	Status Overview Virtual Private Network (VPN)	
VPN: Connected to 1 00:01:17 Disconnect 00:01:17 IPv4 Roaming Security: Disabled while your VPN is active.	VPN Preferences Statistics Route Details Firewall Message Hill Connection Information Statistics Route Details Firewall Message Hill Connection Information State: Connected Tunnel Mode (IPv4): Tunnel All Traffic Tunnel Mode (IPv6): Drop All Traffic Dynamic Tunnel Exclusion: None Dynamic Tunnel Inclusion: None Duration: 00:01:17 Session Disconnect: None Management Comparison State: Disconnected (user tunnel all	tory
‡ 0	Collect diagnostic information for all installed components.	Reset Export Stats

當屬於AD中Management-Group的使用者嘗試連線到Connection-Profile Remote-Access-LDAP時 ,由於沒有LDAP屬性對映返回匹配項,因此此使用者在FTD上繼承的組策略是NOACCESS,其 vpn-simultaneous-logins設定為0。因此,此使用者的登入嘗試失敗。

	🚱 Cisco AnyConnect Secure Mobility Client — 🗆 🗙
Cisco AnyConnect 10.197.223.149 × Login failed. Group: Remote-Access-LDAP Username: Management-User	VPN: Login failed.
Password: OK Cancel	Roaming Security: You are protected by Umbrella. DNS queries are encrypted.
	\$ (i)

可從FTD CLI使用下一個show命令驗證設定:

<#root>

firepower#

show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username

Finance-User

:

Index : 26 Assigned IP : 192.168.10.1 Public IP : 10.1.1.1 : AnyConnect-Parent SSL-Tunnel Protocol : AnyConnect Premium License : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Encryption Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 22491197 Bytes Rx : 14392 Group Policy :

Finance-Group-Policy

Tunnel Group : Remote-Access-LDAPLogin Time : 11:14:43 UTC Sat Oct 12 2019Duration : 0h:02m:09sInactivity : 0h:00m:00sVLAN Mapping : N/AVLAN : noneAudt Sess ID : 0000000001a0005da1b5a3Security Grp : noneTunnel Zone : 0

<#root>

firepower#

```
aaa-server LDAP-AD protocol ldap
realm-id 3
aaa-server AD1 host 192.168.1.1
server-port 389
ldap-base-dn dc=example, dc=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn Administrator@example.com
server-type auto-detect
```

ldap-attribute-map Attribute-Map

show run aaa-server LDAP-AD

<#root>

```
firepower#
```

show run ldap attribute-map

ldap attribute-map Attribute-Map map-name memberOf Group-Policy map-value memberOf CN=Finance-Group,CN=Users,DC=cisco,DC=com Finance-Group-Policy map-value memberOf CN=HR-Group,CN=Users,DC=cisco,DC=com HR-Group-Policy map-value memberOf CN=IT-Group,CN=Users,DC=cisco,DC=com IT-Group-Policy

配置REST API的最常見問題之一就是不時更新持有者令牌。令牌到期時間在身份驗證請求的響應中 給出。如果此時間過期,則可以使用額外的刷新令牌更長時間。刷新令牌也到期後,必須傳送新的 身份驗證請求,以檢索新的訪問令牌。

💊 附註:使用 debug 指令之前,請先參閱有關 Debug 指令的重要資訊。

✤ 您可以設定各種偵錯層級。預設情況下,使用級別1。如果更改調試級別,調試的詳細程度可 能會增加。請謹慎執行此操作,尤其是在生產環境中。

FTD CLI上的以下調試有助於解決與LDAP屬性對映相關的問題

debug ldap 255 debug webvpn condition user <username> debug webvpn anyconnect 255 debug aaa common 127

在此示例中,收集了下一個調試,以演示連線前提及測試使用者時從AD伺服器接收的資訊。

Finance-User的LDAP調試:

<#root>

```
[48] Session Start
[48] New request Session, context 0x00002b0482c2d8e0, reqType = Authentication
[48] Fiber started
[48] Creating LDAP context with uri=ldap://192.168.1.1:389
[48] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[48] supportedLDAPVersion: value = 3
[48] supportedLDAPVersion: value = 2
[48] LDAP server192.168.1.1 is Active directory
[48] Binding as Administrator@cisco.com
[48] Performing Simple authentication for Administrator@example.com to192.168.1.1
[48] LDAP Search:
       Base DN = [dc=cisco, dc=com]
        Filter = [sAMAccountName=Finance-User]
       Scope = [SUBTREE]
[48] User DN = [CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com]
[48] Talking to Active Directory server 192.168.1.1
[48] Reading password policy for Finance-User, dn:CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48] Read bad password count 0
[48] Binding as Finance-User
[48] Performing Simple authentication for Finance-User to 192.168.1.1
[48] Processing LDAP response for user Finance-User
[48] Message (Finance-User):
[48]
Authentication successful for Finance-User to 192.168.1.1
[48] Retrieved User Attributes:
[48]
       objectClass: value = top
[48]
       objectClass: value = person
[48]
       objectClass: value = organizationalPerson
```

```
objectClass: value = user
[48]
        cn: value = Finance-User
[48]
        givenName: value = Finance-User
[48]
[48]
        distinguishedName: value = CN=Finance-User,OU=Finance,OU=VPN,DC=cisco,DC=com
[48]
        instanceType: value = 4
        whenCreated: value = 20191011094454.0Z
[48]
[48]
        whenChanged: value = 20191012080802.0Z
        displayName: value = Finance-User
[48]
        uSNCreated: value = 16036
[48]
[48]
memberOf: value = CN=Finance-Group,CN=Users,DC=cisco,DC=com
[48]
mapped to Group-Policy: value = Finance-Group-Policy
[48]
mapped to LDAP-Class: value = Finance-Group-Policy
[48]
        memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]
                mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]
                mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com
[48]
        uSNChanged: value = 16178
[48]
        name: value = Finance-User
[48]
        objectGUID: value = .J.2...N....X.OQ
        userAccountControl: value = 512
[48]
        badPwdCount: value = 0
[48]
        codePage: value = 0
[48]
[48]
        countryCode: value = 0
[48]
        badPasswordTime: value = 0
        lastLogoff: value = 0
[48]
[48]
        lastLogon: value = 0
        pwdLastSet: value = 132152606948243269
[48]
        primaryGroupID: value = 513
[48]
[48]
        objectSid: value = .....B...a5/ID.dT...
[48]
        accountExpires: value = 9223372036854775807
[48]
        logonCount: value = 0
[48]
        sAMAccountName: value = Finance-User
[48]
        sAMAccountType: value = 805306368
[48]
        userPrincipalName: value = Finance-User@cisco.com
[48]
        objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
        dSCorePropagationData: value = 20191011094757.0Z
[48]
[48]
        dSCorePropagationData: value = 20191011094614.0Z
[48]
        dSCorePropagationData: value = 16010101000000.0Z
[48]
        lastLogonTimestamp: value = 132153412825919405
[48] Fiber exit Tx=538 bytes Rx=2720 bytes, status=1
[48] Session End
```

Management-User的LDAP調試:

<#root>

[51]	Session Start
[51]	New request Session, context 0x00002b0482c2d8e0, reqType = Authentication
[51]	Fiber started
[51]	Creating LDAP context with uri=ldap://192.168.1.1:389
[51]	Connect to LDAP server: <pre>ldap://192.168.1.1:389</pre> , status = Successful

```
[51] supportedLDAPVersion: value = 3
```

[51] supportedLDAPVersion: value = 2 [51] LDAP server 192.168.1.1 is Active directory [51] Binding as Administrator@cisco.com [51] Performing Simple authentication for Administrator@example.com to 192.168.1.1 [51] LDAP Search: Base DN = [dc=cisco, dc=com] Filter = [sAMAccountName=Management-User] Scope = [SUBTREE] [51] User DN = [CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com] [51] Talking to Active Directory server 192.168.1.1 [51] Reading password policy for Management-User, dn:CN=Management-User,OU=Management,OU=VPN,DC=cisco,D [51] Read bad password count 0 [51] Binding as Management-User [51] Performing Simple authentication for Management-User to 192.168.1.1 [51] Processing LDAP response for user Management-User [51] Message (Management-User): [51] Authentication successful for Management-User to 192.168.1.1 [51] Retrieved User Attributes: [51] objectClass: value = top [51] objectClass: value = person [51] objectClass: value = organizationalPerson [51] objectClass: value = user [51] cn: value = Management-User [51] givenName: value = Management-User [51] distinguishedName: value = CN=Management-User,OU=Management,OU=VPN,DC=cisco,DC=com [51] instanceType: value = 4 [51] whenCreated: value = 20191011095036.0Z [51] whenChanged: value = 20191011095056.0Z [51] displayName: value = Management-User [51] uSNCreated: value = 16068 [51] memberOf: value = CN=Management-Group,CN=Users,DC=cisco,DC=com [51] mapped to Group-Policy: value = CN=Management-Group,CN=Users,DC=cisco,DC=com [51] mapped to LDAP-Class: value = CN=Management-Group,CN=Users,DC=cisco,DC=com memberOf: value = CN=Users,CN=Builtin,DC=cisco,DC=com [51] [51] mapped to Group-Policy: value = CN=Users,CN=Builtin,DC=cisco,DC=com [51] mapped to LDAP-Class: value = CN=Users,CN=Builtin,DC=cisco,DC=com [51] uSNChanged: value = 16076 [51] name: value = Management-User [51] objectGUID: value = i._(.E.0.....Gig userAccountControl: value = 512 [51] [51] badPwdCount: value = 0 [51] codePage: value = 0 [51] countryCode: value = 0 [51] badPasswordTime: value = 0 [51] lastLogoff: value = 0 lastLogon: value = 0[51] [51] pwdLastSet: value = 132152610365026101 [51] primaryGroupID: value = 513 [51] objectSid: value =B...a5/ID.dW... [51] accountExpires: value = 9223372036854775807 [51] logonCount: value = 0 [51] sAMAccountName: value = Management-User

- [51] sAMAccountType: value = 805306368
- [51] userPrincipalName: value = Management-User@cisco.com
- [51] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=cisco,DC=com
- [51] dSCorePropagationData: value = 20191011095056.0Z
- [51] dSCorePropagationData: value = 16010101000000.0Z
- [51] Fiber exit Tx=553 bytes Rx=2688 bytes, status=1
- [51] Session End

相關資訊

如需其他協助,請聯絡思科技術協助中心(TAC)。需要有效的支援合約: <u>思科全球支援聯絡人.</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。