為請求方訪問配置電腦雙因素身份驗證

目錄

<u>簡介</u>
<u>必要條件</u>
<u>需求</u>
<u>採用元件</u>
網路圖表
<u>和主义之前,</u> 組能
C1000中的配置
<u>Nindows DC中的</u> 型等
<u>WIIIdows FC中的配直</u> 先頭 4 悠口C 増加到AD 樹
少藤工府にも加当たり残
<u>ン林と前庭に加まるの歌座</u> Windows Convert的 前 要
<u>VIIIdows Server平的配直</u> 牛鹿 4
シャールの時間も図
<u>10CT1011世</u> 先骤 1 增加 洪 署
シ尿ー:11加速に 步驟 2 新増Active Directory
<u>→</u>
<u> </u>
步驟 5.增加DACL和授權配置檔案
<u>步驟 6.增加策略集</u>
<u>步驟 7.增加身份驗證策略</u>
步驟8.增加授權策略
<u>驗證</u>
<u>模式1.電腦身份驗證和使用者身份驗證</u>
步驟 1.登出Windows PC
<u>步驟 2.確認身份驗證會話</u>
步驟 3.登入Windows PC
步驟 4.確認身份驗證會話
步驟 5.確認Radius即時日誌
模式2.僅限使用者驗證
步驟 1.停用和啟用Windows PC的網絡卡
<u>步驟 2.確認身份驗證會話</u>
步驟 3.確認Radius即時日誌
疑難排解
相關資訊

簡介

本文檔介紹使用電腦和dot1x身份驗證配置雙因素身份驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題:

- 思科身份服務引擎的配置
- Cisco Catalyst的配置
- IEEE802.1X

採用元件

- 身分辨識服務引擎虛擬3.3修補程式1
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019

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。

網路圖表

下圖顯示本文檔示例中使用的拓撲。

在Windows Server 2019上配置的域名是ad.rem-xxx.com,本文檔中用作示例。



背景資訊

電腦身份驗證是驗證尋求訪問網路或系統的裝置的身份的安全過程。使用者身份驗證基於使用者名 稱和密碼等身份證明來驗證個人身份,而電腦身份驗證則不同,它側重於驗證裝置本身。這通常使 用裝置特有的數位證書或安全金鑰來完成。

透過同時使用電腦和使用者身份驗證,組織可以確保只有獲得授權的裝置和使用者才能訪問其網路 ,從而提供更加安全的環境。此雙因素身份驗證方法對於保護敏感資訊和遵守嚴格的法規標準特別 有用。

組態

C1000中的配置

這是C1000 CLI中的最小配置。

aaa new-model

radius server ISE33 address ipv4 1.x.x.191 key cisco123

aaa group server radius AAASERVER server name ISE33

aaa authentication dot1x default group AAASERVER aaa authorization network default group AAASERVER aaa accounting dot1x default start-stop group AAASERVER dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge

Windows PC中的配置

步驟 1.將PC增加到AD域

導航到控制台>系統和安全,點選系統,然後點選高級系統設定。在「System Properties」窗口中 ,按一下Change,選擇Domain並輸入域名。

a)stem and secondy.		About		
← → × ↑ 🍤 > Control Panel > System and Security	~	o Your PC is	monitored and protected.	Related settings
Control Panel Home Security and Main	tenance	See details in V	Vindows Security	bitLocker settings
System and Security Review your computer	status and resolve issues 🛛 😌 Change User Account Control settings			Device Manager
Network and Internet	< Figure Problems	Device spe	cifications	Remote desktop
Hardware and Sound	Allow an app through Windows Firewall			
Programs System		Device name	DESKTOP-L2IL9I6	System protection
Appearance and See the name of this co	nd processor speed 😻 Allow remote access Launch remote assistance mputer	Processor	Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)	Advanced system setting
tem Properties	X Computer Name/Domain Changes X			
mputer Name Hardware Advanced System Protection Remote Windows uses the following information to identify your computer	You can change the name and the membership of this computer. Changes night affect access to network resources.			
on the network. Imputer description:	Computer name: DESKTOP-L2IL9I6			
For example: "Kitchen Computer" or "Mary's Computer". ull computer name: DESKTOP-L21L916	Full computer name: DESKTOP-L2IL9I6			
Norkgroup: WORKGROUP	More			
To use a wizard to join a domain or workgroup, click Network ID	Member of Ormain: ad rem4, st im com			
o rename this computer or change its domain or Change	Warkgroup:			

將PC增加到AD域

在「Windows安全性」視窗中,輸入網域伺服器的使用者名稱和密碼。

Windows Security ×	Computer Name/Domain Changes X	Computer Name/Domain Changes
Computer Name/Domain Changes	Welcome to the ad.rem-s_* tm.com domain.	You must restart your computer to apply these changes Before restarting, save any open files and close all
join the domain.	OK	programs.
administrator		OK
•••••		
OK Cancel		
	1	

輸入使用者名稱和密碼

步驟 2.配置使用者身份驗證

導航到身份驗證,選中啟用IEEE 802.1X身份驗證。 在「受保護的EAP屬性」窗口中按一下設定 ,取消選中驗證證書以驗證伺服器的身份,然後按一下配置。在「EAP MSCHAPv2 Properties」窗 口中,選中Automatically use my Windows logon name and password(and domain if any),使用在 Windows電腦登入期間輸入的使用者名稱進行使用者身份驗證。

pciPassthru0 Properties ×	Protected EAP Properties ×	EAP MSCHAPv2 Properties X
Networking Authentication	When connecting: Weify the server's identity by validating the certificate	When connecting:
Select this option to provide authenticated network access for this Ethernet adapter.	Connect to these servers (examples:srv1;srv2;.*srv3com):	password (and domain if any).
Choose a network authentication method:	Trusted Root Certification Authorities:	OK Cancel
Monsoft: Protected EAP (PEAP)	AAA Certificate Services A ad-WINSERVER-CA Balteners CoherTauet Boot	
Remember my credentials for this connection each time I'm logged on	Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA	
Falback to unauthorized network access	DigCert Gobal Root CA DigCert Gobal Root G2 V	
Additional Settings	Notifications before connecting:	
	Tell user if the server's identity can't be verified $\qquad \qquad \lor$	
	Select Authentication Method:	
	Secured password (EAP-MSCHAP v2) V Configure	
	Enable Fast Reconnect	
OK Cancel	Enable Identity Privacy	
	OK Cancel	

啟用使用者身份驗證

導航到身份驗證,選中其他設定。從下拉選單中選擇User or computer authentication。

pciPassthru0 Properties	Advanced settings ×
 pciPassthru0 Properties Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter. Imable IEEE 802.1X authentication Choose a network authentication method: Microsoft: Protected EAP (PEAP) v Settings Remember my credentials for this connection each time I'm logged on Fallback to unauthorized network access Additional Settings 	Advanced settings
OK Cancel	OK Cancel

Windows Server中的配置

步驟 1.確認網域電腦

導航到Active Directory使用者和電腦,按一下電腦。確認Win10 PC1已列在域中。

Active Directory Users and Computers		-	o x
<u>File Action View Help</u>			
🗢 🔿 📶 🛍 🖾 🔒 🔂 📷 🐍 📚	7 🗾 🕱		
Active Directory Users and Computers [winserver.ad.rem-s] Saved Queries Builtin Computers Domain Controllers Sign Domain Controllers Managed Service Accounts Sign Users	Name DESKTOP-L2IL9I6 ISE33-01	Type Computer Computer	

確認網域電腦

步驟 2.新增網域使用者

導航到Active Directory使用者和電腦,按一下使用者。將testuser新增為網域使用者。

Active Directory Users and Computers File Action View Help ← ⊕ 2 □	k in 7 🛛 k		
Active Directory Users and Computers (minserver.ad.nem-a) Computers Domain Controllers Domain Controllers Managed Service Accounts Users	Name Administrator Allowed RODC Password Replication Group Cert Publishers Conreable Domain Controllers CertPublishers Controllers Consult Controllers Consult Controllers Consult Admins Domain Controllers Commain Controllers Commain Controllers Commain Controllers Commain Guests Commain Users Commain Users Enterprise Admins Enterprise Key Admins	Type User Security Group - Domain Local Security Group - Global User Security Group - Global Security Group - Universal Security Group - Universal	Description Built-in account for administering the computer/domain Members in this group can have their passwords replicated to Members of this group are permitted to publish certificates to Members of this group that are domain controllers may be CL. A user account managed by the system. Members in this group cannot have their passwords replicate DNS clients who are permitted to perform dynamic updates over the properties Properties Properties Properties Protein Remote Desktop Services Prote COM- Address Account Protein Control Remote Desktop Services Protein Control Remote Desktop Services Protein Dest user
	tte Enterprise Read-only Domain Controllers Group Policy Creator Owners Group Rolicy Creator Owners Guest Key Admins Notected Users ReAS and UAS Servers Read-only Domain Controllers Schema Admina Stets user	Security Group - Global User Security Group - Global User Security Group - Global Security Group - Global Security Group - Global Security Group - Global Security Group - Global User	name: US pisals:

新增網域使用者

將域使用者增加到域管理員和域使用者的成員。

				. ^	test user properties				r	
Member Of	Dial-in	Enviro	onment	Sessions	Remote control	Remote	Desktop Se	ervices Profile	00)M+
Remote control	Remote 0	Desktop Serv	vices Profile	COM+	General Address	Account	Profile	Telephones	Organ	izatio
Seneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Env	ironment	Sessi	ons
Jser logon name:					Member of:					
lestuser		@ad.rem	4,1.3m.com	~	Name	Active Direct	tory Domain	Services Folder	r	
lser logon name (pre	-Windows 200	0):			Domain Admins	ad rem-syllin	m.com/Use	113		
AD\		testuser			Domain Users	ad rem-synt.	m.com/Use	975		
Uplock account	oe password a	t pertingen		~						
Uglock account ccount gptions: User must chan User cannot ch Password neve Store password	ge password a ange password r expires using revensibl	t next logon d	1	<	Add E Primary group: D	Jemove omain Users				
Uglock account ccount gotions: User must chan User cannot ch Password neve Store password Account expires Never End of:	ge password a ange password r expires using reversib Thursday ,	t next logon d le encryption June 6	s, 2024	•	Add E Primary group: D Set Primary Group	gemove omain Users There is n you have applicatio	no need to Macintosh ins.	change Primary . clients or POSD	group uni K-compila	less

域管理員和域使用者

ISE中的配置

步驟 1.增加裝置

導航到管理>網路裝置,點選增加按鈕增加C1000裝置。

=	diale Identity Services	Engine				Administratio	on / Netwo	rk Resources	
Щ	Bookmarks	Network Devices	Network Device G	roups N	letwork Device Profiles	External RADIUS	Servers	RADIUS Server Sequences	NAC Managers
	Dashboard	Network Devices	Net	work Devices Li	st > C1000				
0	Context Visibility	Default Device	Ne	twork Devid	ces				
х	Operations	Dence occurry occur	N	ame	C1000				
U	Policy				01000				
20	Administration		D	escription					
nii.	Work Centers		- 1 e						
			L	IP Address	 ™™: 1.1100.101 	7 32 🗇			
?	Interactive Help			Destile	th Circo				
			b	evice Profile	La Cisco				
			М	odel Name		~			
			S	oftware Versio	n	~			
			N	etwork Device	Group				
			L	ocation	All Locations	~	Set To Defau	ilt	
			IP	SEC	No	~	Set To Defau	ult	
			D	evice Type	All Device Types	~	Set To Defau	ult	
				V RAD	IUS Authentication Settir	igs			
				RADIUS	UDP Settings				
				Protocol	RADIUS				
				Shared S	Secret cisco123		Hide		

增加裝置

步驟 2.新增Active Directory

導航到管理>外部身份源> Active Directory,點選連線頁籤,將Active Directory增加到ISE。

- 連線點名稱: AD_Join_Point
- Active Directory域: ad.rem-xxx.com

≡	dials Identity Services I	Engine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 55	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat * Join Point Name AD_Join_Point
0	Policy Administration	Active Directory Active Directory Active Directory Domain ad.rem-si i .m.com

新增Active Directory

導航到組頁籤,從下拉選單中選擇選擇目錄中的組。

	edualse Identity Services E	Engine Administration / Identity Management
Л	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 22	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat
0	Policy	Select Groups From Directory
20	Administration	AD_Join_Point Add Group Control Assist ad.rem-sy Im.com/S-1-5-32-579

從目錄選取群組

從下拉選單中選擇Retrieve Groups。選中ad.rem-xxx.com/Users/Domain Computers和ad.remxxx.com/Users/Domain Users,然後按一下OK。

 Identify (marks) Connect Visibility Connect Visibility	≡	then the services	Engine						×	A 11
 A conserve fixed on a conserve fixed		Backmarks	Identities Groups E	Sel	lect Directory	Groups				
0 Contract Vitability		Dashboard) - C) Cartinicate H	This d	fialog is used to select grow	ips from the Directo	ry.			
 		Context Visibility	1 AD_Join_Poin	Do	pengin adven-e r'm.com. Name	so,	Type	4.5		
Pointy 0.000 Administration BADOUS Takes BADOUS Takes BADOUS Takes B	-83	Operations	C3 LOAP		Fiber	Filter_	Fiber			
Administration Name Group 5/0 Group Type ************************************	0	Policy			Hereicke Groups	a Groups Retrieved				
More Centers More Centers State, 10 Prove Booleal Login More Centers Booleal Login More centers More center	1.	Administration	RSA Securit	0	Name	<u>^</u>	Group SID	Group Type		
* Sociel Legin * Sociel Legin * * * * * * * * * * * * * * * * * * *	-2	Work Centers	SAME IN PROVIDE	- 0	advenue; proceeding	Designations	5-1-5-21-4110742415-4100520020-2040	2199. DOMAN LOCAL	-1	
• Material Users • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4133930024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4133930024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4133930024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4133930024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4133930024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Users • 1-4-21-41183742415-4139390024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Users • 1-4-21-41183742415-4139390024-20442394. • 64.0844. • ad removag, j., m. com/javers/Domain Users • 1-4-21-41183742415-4139390024-20442394. • 04.0844. • ad removag, j., m. com/javers/Domain Users • 1-4-21-41183742415-4139390024-20442394. • 04.0844. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-4139390024-20442394. • 040024534. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-41393900242-20442394. • 040024534. • ad removag, j., m. com/javers/Domain Computers • 1-4-21-41183742415-41393900242-20442394.			🗇 Social Login	0	ad.rem-ay="am.com/Users/	Domain Admina	5-1-5-21-4193742415-4133920028-2048	2199. GLOBAL		
ad remona, in an on Viseon Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in an on Viseon Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in an on Viseon Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. GLOBAL ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-413332024-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320242-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320242-20442394. UNIVCH584L ad remona, in a conviluent Consumers bit -121 - 41183742415-4133320242-20442394. UNIVCH584L bit remonal in a conviluent Consumers bit remonal in a conviluent Consumers bit -121 - 41183742415-41331200242-20442394. UNIVCH584L bit remonal in a conviluent Consumers bit remonal in a conviluent Consumers bit -121 - 41183742415-41331200242-20442394. UNIVCH584L bit remonal in a conviluent Consumers		Interactive Help			adven-ay.1.m.com/Vacad	Domain Computers	5-1-5-21-4110742415-4130520026-2046	2199. 6L084L		
at xem-st, y zm.com//sens/Domain Goess 5-1-5-21-41182742415-4133930024-20442394. GLOBAL ad xem-st, z m.com//sens/Domain Goess 5-1-5-21-41182742415-4133930024-20442394. GLOBAL ad xem-st, z m.com//sens/Domain Goess 5-1-5-21-41182742415-4133930024-20442394. UNIVDRSAL ad xem-st, z m.com//sens/Domain Goespite Read-sensy. S-1-5-21-41182742415-4139300024-20442394. UNIVDRSAL ad xem-st, z m.com//sens/Domain G				0	adven-1.st.m.con/course	Domain Controllers	5-1-5-21-8193742415-4133920026-2046	2399 0L00AL		
ad.rem-tq. / m.com/UnertyDresh/Dresh/Dresh/Sectory st.1-5-21-41103742415-413030004-20442096. GLOBAL ad.rem-tq. / m.com/UnertyDresh/				0	adven-a, iron.com/Users/	bonain Guesta	5-1-5-21-4193742415-4133920020-2048	2399. GLOBAL		
adven-st, 2 m.com/twent/Chergine Aprilies adven-st, 2 m.com/twent/Chergine Apriles adven-st, 2 m.com/twent/Chergine Read-only. Si-1-4-21-4193742415-4133930024-20442396. UMVDRSAL adven-st, 2 m.com/twent/Chergine Read-only. Si-1-4-21-4193742415-4133930024-20442396. UMVDRSAL adven-sty, 4m.com/twent/Chergine Read-only. Si-1-4-21-4193742415-4133930024-20442396. UMVDRSAL adven-sty.					advenus un contrand	Domain Users	5-1-5-21-4193742415-4130920026-2046	2199. GLOBAL		
ad rem-a; r m.com/bens/Crears & Kay Admins 5-1-5-21-4133102415-413310242-20482395. VAVDB5AL ad rem-a; r m.com/bens/Crears Paley Creater 5-1-5-21-4133102415-4133102024-20482395. VAVDB5AL ad rem-a; r m.com/bens/Crears Paley Creater 5-1-5-21-4133102415-4133102024-20482395. VAVDB5AL c c c c c c c c c c c c c c c c c				0	adven-a; r.m.con/Usend	Onterprise Admins	5-1-5-21-4193742415-4133920026-2046	2399 UNIVERSAL		
advances, pre-services compares team very, pre-service compares team very, and team v				0	adven-aj v m.con/Users/	Onterprise Key Admins	5-1-5-21-4110742415-4130520026-2046	2199. UNIVERSAL	_	
					ad ram-ay, an confident	Croup Putcy Creator	5-1-5-21-4110742415-4130520026-2046	2198. GLOBAL		
Cancel				1						
								Cancel	ox	

增加域電腦和使用者

步驟 3.確認電腦身份驗證設定

導航到高級設定頁籤,確認電腦身份驗證的設定。

- 啟用電腦身份驗證: 啟用電腦身份驗證
- 啟用電腦存取限制:在授權前結合使用者和電腦驗證



註:有效老化時間範圍為1至8760。

步驟 4.增加身份源序列

導航到管理>身份源序列,增加身份源序列。

- 名稱: Identity_AD
- 身份驗證搜尋清單: AD_Join_Point

≡	dentity Services I	Engine		Administration / Io	dentity Management
Щ	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
5	Dashboard	Identity Source Sequen	ces List > Identity_AD		
110	Context Visibility	Identity Source	Sequence		
×	Operations		-		
U	Policy	 Identity Source * Name 	ce Sequence		
80	Administration		Identity_AD		
-fli	Work Centers	Description			h.
?	Interactive Help	✓ Certificate E ☐ Select Certi	ased Authentication	~	
		✓ Authenticati A set of ide	on Search List intity sources that will be accessed	in sequence until first authentication s	ucceeds
		Availab	e	Selected	
		Internal	Endpoints	AD_Join_Point ^	
		Internal	Users		
		Guest U	Join Points		
					$\overline{\nabla}$
增加	身份源序列				

步驟 5.增加DACL和授權配置檔案

導航到策略>結果>授權>可下載ACL,增加DACL。

- 名稱: MAR_Passed
- DACL內容: permit ip any host 1.x.x.101和permit ip any host 1.x.x.105

≡	dentity Services E	ingine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions Resul	ts	
53	Dashboard	Authentication > D	ownloadable ACL List > MAR_Passed	
15	Context Visibility	Authorization	Downloadable ACL	
×	Operations	Authorization Profiles	* Namo MAD Dassard	
0	Policy	Downloadable ACLs	Description	1
80	Administration	Profiling >		
di.	Work Centers	Posture >	PVersion © IIVe © Agnostic () *DACL Content 1234567 permit ip any host 1.1[].3.101	
		Client Provisioning >	801011 permit ip any host 1.13 2.151 213415 1437181	

增加DACL

導航到策略>結果>授權>授權配置檔案,增加授權配置檔案。

- 名稱: MAR_Passed
- DACL名稱: MAR_Passed

≡	dentity Services I	Engine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	R	esults	
	Dashboard	Authentication	>	Authorization Profiles > MAR_	Passed
15	Context Visibility	Authorization	~	Authorization Profile	
*	Operations	Authorization Profiles		* Name	MAR Passed
0	Policy	Downloadable ACLs		Description	
80	Administration	Profiling	>		
ń	Work Centers	Posture	>	* Access Type	ACCESS_ACCEPT ~
		Client Provisioning	>	Network Device Profile	± Cisco ∨⊕
?	Interactive Help			Service Template	
				Track Movement	
				Agentless Posture	
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed V

增加授權配置檔案

步驟 6.增加策略集

導航到策略>策略集,點選+增加策略集。

- 原則集名稱: MAR_Test
- 條件:Wired_802.1X
- 允許的協定/伺服器序列:預設網路訪問

≡	dentity Services Er	igine Policy / Policy Sets		🔺 Evalua	tion Mode I	19 Days (م د	0	0	۹
н	Bookmarks	Policy Sets		Click P	tere to do	visibility se	tup Do I	not show t	his agai	n. ×
51	Dashboard	 Status Policy Set Name Description Conditions 	Allower	1 Protoco	ls / Server	Sequence	Hits	Actions	View	
넝	Context Visibility	Q Search								
*	Operations	MAR, Test Wwed, 802.1X	Default	Network	Access	× +	15	¢	>	
1.	Administration	Default Default policy set	Default	Network	Access	2+	٥	٢	>	
ñ	Work Centers						Reset		Save	

步驟 7.增加身份驗證策略

導航到策略集,點選MAR_Test以增加身份驗證策略。

- 規則名稱: MAR_dot1x
- 條件:Wired_802.1X
- 使用:Identity_AD

~	Authenticatio	on Policy(2)				
	 Status 	Rule Name	Conditions	Use	Hits	Actions
	Q Searc	h				
	۰	MAR_dot1x	E Wind_802.1X	Identity_AD //		¢
	0	Default		All_User_ID_Stores	0	¢
增力	身份	驗證策略				

步驟 8.增加授權策略

導航到策略集,點選MAR_Test以增加授權策略。

- 規則名稱: MAR_Passed
- 條件: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- 結果: MAR_Passed
- 規則名稱: User_MAR_Passed
- 條件:網路訪問·WasMachineAuthenticated 等於True 且AD_Join_Point·ExternalGroups 等於 ad.rem-xxx.com/Users/Domain使用者
- 結果: PermitAccess

VAuthorization Policy(3)										
		Results								
🕂 Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions					
Q Search										
MAR_Passed	AND R AD_Join_Point ExternalGroups EQUALS ad.rem-13 1 im.com/Users/Domain Computers Domain Computers ND	MAR_Passed	+ Select from list / +	•	ø					
User_MAR_Passed	NUD R AD_uoin_Point ExternalGroups EQUALS True R AD_uoin_Point ExternalGroups EQUALS ad.remty >m.com/Users/Domain Users	PermitAccess	elect from list elect from list elect elect from list from list	- 1	命					
O Default		DenyAccess	/ + Select from list / +	. 9	٩					

增加授權策略

驗證

模式1.電腦身份驗證和使用者身份驗證

步驟 1.登出Windows PC

按一下Win10 PC1中的Sign out按鈕以觸發電腦身份驗證。

Interface: GigabitEthernet1/0/2 MAC Address: b496.9115.84cb IPv6 Address: Unknown IPv4 Address: 1.x.x.9 User-Name:

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 5s Common Session ID: 01C2006500000049AA780D80 Acct Session ID: 0x000003C Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2

Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies: ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list: Method State

dot1x Authc Success

步驟 3.登入Windows PC

登入Win10 PC1, 輸入使用者名稱和密碼以觸發使用者身份驗證。

登入Windows PC

步驟 4.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/2 details命令以確認C1000中的使用者身份驗證會話。

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:

AD\testuser

Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 85s Common Session ID: 01C200650000049AA780D80 Acct Session ID: 0x000003D Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Server Policies: Method status list: Method State

dot1x Authc Success

步驟 5.確認Radius即時日誌

導航到ISE GUI中的操作> RADIUS >即時日誌,確認電腦身份驗證和使用者身份驗證的即時日誌。

≡	the dentity Services E	Engine					Operations /	RADIUS				A Evaluation Made Ellays	\$ 6) Q A
н	Bookmarks	Live Lo	gs Live Sessions											
	Dashboard													
명	Context Visibility	м	sconfigured Supplicants 📀			Mise	configured Network Devices 📀		RADIUS Drops		Client Stopped Respond	ng 🕢	Repe	at Counter 🕕
*	Operations		0				0		0		0			0
U	Policy										Refre	h Show	Within	1
2. 1	Administration Work Centers	0	E Reset Repeat Counts	riangle Export To ee							NEW	Latest 20 record	Fher	v o
			Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P IP Addres	is Ne	twork De
0	Interactive Help		×	~			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi IP Address	- <u>N</u>	twork Devic
			May 07, 2024 04:36:14	•	0	0	AD\testuser	84:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess 1.1 \ 3.9		
			May 07, 2024 04:36:13		0		ADUestuser	84.96.91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1 = 0.9	01/	300
			May 07, 2024 04:35:12	8	à		#ACSACL#-IP-MAR_Passed-6639ba20						C1/	300
			May 07, 2024 04:35:12	8	^o		host/DESKTOP-L2IL9I6.ad.rem-s_ithm	84:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto MAR_Pessed$	MAR_Passed 169.254.90	.101/	300

Radius即時日誌

確認電腦身份驗證的詳細即時日誌。

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-s,s.sm.com
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details

Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy rem.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

Steps

電腦身份驗證的詳細資訊

確認使用者身份驗證的詳細即時日誌。

Cisco ISE

Overview		Steps
		Stee IF
Event	5200 Authentication succeeded	11001
Username	AD\testuser	11017
Endpoint Id	B4:96:91:15:84:CB ⊕	15049
Endociat Drafile	latel Davias	15008
Enapoint Profile	Intel-Device	11507
Authentication Policy	MAR_Test >> MAR_dot1x	12500
Authorization Policy	MAR_Test >> User_MAR_Passed	12625
Authorization Result	PermitAccess	11006
		11001
		11018
Authentication Details		12301
Source Timestamp	2024-05-07 16:36:13.748	12300
		12625
Received Timestamp	2024-05-07 16:36:13.748	11006
Policy Server	ise33-01	11001
Event	5200 Authentication succeeded	11018
Username	AD\testuser	12302
Endpoint Id	B4:96:91:15:84:CB	61025
		12318
Calling Station Id	B4-96-91-15-84-CB	12800
Endpoint Profile	Intel-Device	12805
IPv4 Address	1.111 0.9	12806
Authentication Identity		12807
Store	AD_Join_Point	12808
Identity Group	Profiled	12810
Audit Cassian Id	010000000000000000000000000000000000000	12305
Audit Session Id	0102006500000049AA780D80	11006
Authentication Method	dot1x	11018
Authentication Protocol	PEAP (EAP-MSCHAPv2)	11010

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

使用者身份驗證的詳細資訊

模式2.僅限使用者驗證

步驟 1.停用和啟用Windows PC的網絡卡

要觸發使用者身份驗證,請停用並啟用Win10 PC1的NIC。

步驟 2.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/2 details命令以確認C1000中的使用者身份驗證會話。

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name: AD\testuser

Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 419s Common Session ID: 01C2006500000049AA780D80 Acct Session ID: 0x000003D Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Server Policies: Method status list: Method State dot1x Authc Success

步驟 3.確認Radius即時日誌

在ISE GUI中導航到操作> RADIUS >即時日誌,確認使用者身份驗證的即時日誌。

注意:由於MAR快取儲存在ISE中,因此僅需要使用者身份驗證。

≡ dealer identity Service	rs Engline	Oper	rations / RADIUS	A Evaluation Mode	Q & ⊗ ↓ A
JI Bookmarks	Live Logs Live Sessions				
E Dashboard					
10 Context Visibility	Misconfigured Supplicants	Misconfigured Network Devices 📀	RADIUS Drops	Client Stopped Responding 🕕	Repeat Counter 🕕
😤 Operations	0	0	0	0	0
Policy Administration				Refresh Show Never v Latest	20 records v Within Last 3 hours v
Work Centers	ට් 🖆 Roser Repeat Counts රා	🕁 Export To 🗸			Filter V 0
	Time	Status Details Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorization P	IP Address Network De
(?) Interactive Help	×	identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization Profi	IP Address 🗸 Network Devic
	May 07, 2024 04:42:05	O AD/(testuser	84:96:91:15:84: Intel-DevL MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	1.1.1.1.9
	May 07, 2024 04:42:04	AD/pestuser	04:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	1
	May 07, 2024 04:36:13	AD/(testuser	84.96.91:15.84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	1.1 0.9 C1000
	May 07, 2024 04:35:12	ACSACL#-IP-MAR_Passed-6639ba	20		C1000
	May 07, 2024 04:35:12	host/DESKTOP-L2IL96.ad.rem-st/La	m 84:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed MAR_Passed	169.254.90.1 C1000

確認使用者身份驗證的詳細即時日誌。

Cisco ISE

weak2004 Addension succeeded2006 D2006 D2006 Dbrance64000 511504 CO064000 511504 CO0hogen Polic64000 511504 CO010001000hubbrictorio Robin64000 511504 CO010001000hubbrictorio Robin64000 511504 CO010001000hubbrictorio Robin64000 51 cm 20 second 2000 cm 20 second 200000hubbrictorio Robin6400 51 cm 20 second 2000 cm	Overview		Steps		
Homma ADjecture 1000 Restrict ADJOS Access-Request - AD_John_Point 0 indeper Mil Maschall ELCO 0 0 0 indeper Mil Maschall ELCO 0 0 0 0 indeper Mil Maschall ELCO 0 <t< td=""><td>Event</td><td>5200 Authentication succeeded</td><td>Step ID</td><td>Description</td><td>Latency (ms</td></t<>	Event	5200 Authentication succeeded	Step ID	Description	Latency (ms
Instance Materials Materials <th< td=""><td></td><td></td><td>11001</td><td>Received RADIUS Access-Request - AD_Join_Point</td><td></td></th<>			11001	Received RADIUS Access-Request - AD_Join_Point	
ndpindMiddleMiddleModel<	Username	AD\testuser	11017	RADIUS created a new session - ad.rem-s_b.em.com	0
ndqoid Pindiamet-bake[1000Calculating Series Selection Perior0understation PeriorMalk_Test > Malk_dott'1000Prepared CAP-Response Transmissing CAP-TLS with challings2understation PeriorPeriod Cass1000Restanced ADUIS Access-Challings0understation Details1000Restanced ADUIS Access-Challings0backed Tabuta Second ADUIS Access-Challings1001Restanced ADUIS Access-Challings0backed Tabuta Second ADUIS Access-Challings1001Restanced ADUIS Access-Challings0backed Tabuta Second ADUIS Access-Challings1001Restanced ADUIS Access-Challings0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta Second ADUIS Access-Response IDAC PERP1000Restanced ADUIS Access-Response IDAC PERP0backed Tabuta S	Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	1
Instrumentation Proley MAL_Test >> MAR_Mont X 1600 Extracted GA-Respond CAR-Request process (PAL-S with challings) 2 unnotation Real Malk_Test >> User_MAR_Passed 0 1000 Returned ADUIS Access - Challings 0 unnotation Real Malk_Test >> User_MAR_Passed 0 1000 Returned ADUIS Access - Challings 0 unnotation Real 204-05-07 16-42.04.467 1000 Returned ADUIS Access - Challings 0 unnotation Real 2024-05-07 16-42.04.467 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Challings 0 view it 3020-Aduition succeeded 1000 Returned ADUIS Access - Chalings	Endpoint Profile	Intel-Device	15008	Evaluating Service Selection Policy	0
uninefficient register Proposed EAR-Hosp strippiding EAR-Hits which calling a strippiding EAR-Hits which early a strippididing EAR-Hits which early a strippididing EAR-Hits whi			11507	Extracted EAP-Response/Identity	16
under tabel being wind wind wind wind wind wind wind wind	Authentication Policy	MAR_Test >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
undertation Result Presidances 1	Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
1000 Received RAUGUS in re-uniq an existing session 0 10110 Received RAUGUS in re-uniq an existing session 0 10100 Received RAUGUS in re-uniq an existing session 0 10100 Received RAUGUS in re-uniq an existing session 0 10100 Received RAUGUS in re-uniq an existing session 0 10100 Received RAUGUS in re-uniq an existing session 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received 0 10100 Received RAUGUS in re-uniq an existing received RAUGUS in re-uniq	Authorization Result	PermitAccess	11006	Returned RADIUS Access-Challenge	0
1118 ADD/S is re-uping a withing session 0 butherhication Details 1230 ADD/S is re-uping a withing session 0 boarde Timestamp 2924-05-07 16.42.04.457 12000 Prepared LAP-Acquest proposing PLAP with challings 0 boards Environment 2924-05-07 16.42.04.457 1000 Received Timestamp 0 boards Environment 2924-05-07 16.42.04.457 1000 Received ADD/S Access-Acquest to Using session 0 boards Environment 2920 Anternate ADD/S is re-uping an exiting session 0 0 brance 2000 Anternate ADD/S is re-uping and exiting session 0 0 brance 2000 Anternate ADD/S is re-uping and exiting session 0 0 brance 2000 Anternate ADD/S is re-uping and exiting session 0 0 brance ADD/S is re-uping and exiting session 0 0 0 brance 1111 Bad/D/S is re-uping and exiting session 0 0 brance 1111 Success/ADD repared TLS Score/TLS envices/TLS envices			11001	Received RADIUS Access-Request	5
statu Linear Linea			11018	RADIUS is re-using an existing session	0
based Timestamp 204-06-07 16.42.04.467 1000 Propert ALP-Request proposing PLAP with challenge 0 besceived Timestamp 204-06-07 16.42.04.467 1000 Recured ALDUS Access-Challenge 0 bills Station Succeeded 1000 Recured ALDUS Access-Challenge 0 wirt 500 Authentication Succeeded 1001 Recured ALDUS Access-Challenge 0 binsmare AUtestare 1000 Recured ALDUS Access-Challenge 0 binsmare Lin*1-54-00 Distaret Arritic Access Ac	Authentication Details		12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
beckeed Imestamp 224-05-07 16.42.20.4677 12005 Vuid Arean-Sample and Sample and	Source Timestamp	2024-05-07 16:42:04.467	12300	Prepared EAP-Request proposing PEAP with challenge	0
vertix 1006 Returned ADD(5 Access-Challenge 0 viday Server ka33-01 1006 Reterived RADUS Access-Request 25 viday Server ka33-01 1000 Received RADUS Access-Request 25 viday Server 1000 Received RADUS Access-Request 26 indepinit PMB B4.96-91.15-84-CB 1000 Decessivity regordinated REAV vision 0 vidag Saudin Id Id-96-91.15-84-CB 12800 Extracted first TLS record; TLS handshake started 0 vidag Saudin Id Id-96-91.15-84-CB 12800 Propared TLS ServiceDone message 0 vidag Saudin Id Id-15-96.000 11000 Returned RADUS Access-Challenge 0 vidag Saudin Id Id-160 Returned RADUS Access-Request 14 vidag Saudin Id Id-2006 Received RADUS Access-Request 10			12625	Valid EAP-Key-Name attribute received	0
biolog Server les33-01 11010 Rectived RADIUS Access-Request 25 Vent 500 Authentication succeeded 11018 RADUUS is re-using an existing session 0 Identified ADtestuser 12280 Extracted CAP-Response containing PEAP shallenge- response and accepting PEAP as regolited of the desting Station Id 14.96-91-15-84-CB 0 Jaing Station Id 49.46-91-15-84-CB 12800 Extracted first TLS record; TLS handshats started 0 Indpoint Profile Inst-Device 12800 Prepared TLS ServerHelo message 0 Vert Address 1.11 * 7.9 12807 Prepared TLS ServerHelo message 0 ubienetication Interdevice 0.1000500000043A/20080 12807 Prepared TLS ServerHelo message 0 ubienetication Stating Vert Part Id ServerHelp Charlenge message 0 12807 Prepared TLS ServerHelp message 0 ubienetication Stating Vert Part Id ServerHelp Charlenge message 0 0 0 0 ubienetication Stating Server Device 12005 Prepared TLS ServerHelp message 0 ubienetication Stating Vert Id AdverMess Id ServerHelp Charlenge message 0	Received Timestamp	2024-05-07 16:42:04.467	11006	Returned RADIUS Access-Challenge	0
went 500 Authentication succeeded 11018 RADUs is ne-using an existing session 0 kername ADisestaver 1302 Fersone and accepting PLAP as regoting of a comparison of accepting PLAP as regoting PLAP as regotin	Policy Server	ise33-01	11001	Received RADIUS Access-Request	25
Instantion AD[testuser 12302 Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated 1218 12302 Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated 1218 12302 Extracted FAP-Response containing PEAP challenge- response and accepting PEAP challenge- response and accepting PEAP challenge- testing accepting PEAP challengeAP accepting accepting PEAP	Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
Indpoint id6102500pcn secure concection with TLS peer0Jalling Station id84-96-91-15-84-CB12318Success/tilly negotiated PEAP version 00Indpoint ProfileIntel-Device1200Extracted TLS Centrificate message0Pv4 Address1.1** 7.912000Prepared TLS Server/tello message0uithentication IdentifyAp_sion_Point12005Prepared TLS Server/tello message0uithentication Identify012006Prepared EAP-Request with another PEAP challenge0uithentication Method012006Prepared EAP-Request with another PEAP challenge0uithentication Prepared Identifier Identi	Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
Image: Status Id B4-96-91-15-84-CB 1218 Successfully negatised PEAP version 0 0 Indepoint Profile Intel-Device 12800 Extracted first TLS record; TLS handshake started 0 Pv4 Address 1,1*' 1,9 12805 Extracted first TLS record; TLS handshake started 0 utile AD_Jon_Point 12805 Extracted TLS Server/Billo message 0 utile AD_Jon_Point 12805 Prepared TLS Server/Sechang message 0 utile TSS Prepared TLS Server/Sechang message 0 0 0 utile TSS Prepared TLS Server/Sechang message 0 0 0 0 utile TSS Prepared TLS Server/Sechang message 0	Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
laing Sation Id hadoin Profile hatel-Device 12000 Lass of LS Genetication message 12000 Prosted TLS Genetication message 12000 Propared TLS Genetication message 1000 Propared TLS Genetication message 1000 Propared TLS Genetication message 1000 Propared TLS Genetication for the propertication for the properise fo			12318	Successfully negotiated PEAP version 0	0
indepint Profile Inst-Device 12805 Extracted TLS ClientHolio message 0 PA4 Address 1,1 1,9 12805 Prepared TLS Centrificite message 0 uturnentication Identity itore AD_sion_Point 12805 Prepared TLS Server/KeyExchange message 0 itore 12805 Prepared TLS Server/KeyExchange message 0 itore 12805 Prepared TLS Server/KeyExchange message 0 itore 1000 Returned RADIUS Access-Request with another PEAP challenge 0 uturnentication Method itor X 11001 Received RADIUS Access-Request 14 uturnentication Method itor X 11001 Received RADIUS Access-Request with another PEAP challenge- response 12005 Prepared TLS Centrification message 0 uturnentication Method itor X 11001 Received RADIUS Access-Request with another PEAP challenge- response 12005 Prepared TLS Centrification message 0 uturnentication Method itor X 12006 Prepared TLS Centrification message 0 iservice -type - Framed, association 10C2006500000049AA780080, method-dott, PGSubjectKhane-2xe19520-06421-11ef-abec- sociation previous auccessful machine PGSubjectKhane-2xe19520-06421-11ef-abec- association for user in Active Directory - AD_testure PGSubjectKhane-2xe19520-06421-11ef-abec- association foreuser 15036 Ceaking uper in Act	Calling Station Id	B4-96-91-15-84-CB	12800	Extracted first TLS record; TLS handshake started	0
Pv4 Address 1.1* 1.9 1286 Prepared TLS Serverhelelo message 0 uthentication lefentity tore AD_sloin_Point 1280 Prepared TLS Serverhelelo message 0 uthentication lefentity tore Prepared TLS Serverhelelo message 0 0 uthentication lefentity tore Prepared TLS Serverhelelo message 0 uthentication lefentity Prepared TLS Serverhelelo message 0 uthentication Method 01/2006500000049AA780080 12800 Prepared TLS Serverhelelo message 0 uthentication Method 01/2006500000049AA780080 1000 Returned RADIUS Access-Challenge 0 uthentication Protocol PKP (KP-NSCHAPv2) 10108 Returned RADIUS Access-Challenge 0 uthentication Protocol PKP (KP-NSCHAPv2) 12304 Extracted CAP-Request with another PEAP challenge 0 uthentication Method Group 12305 Prepared TLS Serverhelelo message 0 uthentication Method service-type-Framed, audit-session-id-0102000500000049AA780080. 12304 Extracted CAP-Request with another PEAP challenge 0 iservice-type-Framed, audit-session-id-0102000500000049AA780080. 15066 Evaluating Authorization Policy 0 iservice-type-Framed, audit-session-id-0102000500000049AA780080. 12305 Looking up us in Active Dinectory and u	Endpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
12807 Propared TLS Certificate message 0 Withentication Identity Bore AD_Join_Point 12807 Propared TLS ServerXoyExchange message 26 dentity Group Profied 12808 Propared TLS ServerXoyExchange message 0 ustdt Session Id 01C2006500000049AA780080 1280 Propared TLS ServerXoyExchange message 0 ustdt Session Id 01C2006500000049AA780080 11006 Returned RADIUS Access-Challenge 0 ustdt Session Id dot1x 11018 RADIUS Is re-using an existing session 0 ustdt Session Id dot1x 11018 RADIUS Is re-using an existing session 0 ustdt Session Id dot1x 12807 Propared TLS Cerificate message 0 ustdt Session Id 01C2006500000049AA780080 14 1000 Recurred RADIUS Access-Request 14 ustdentication Returned RADIUS Access-Request 14 12805 Propared TLS Cerificate message 0 ustdentication Returned RADIUS Access-Request 12805 Propared TLS Cerificate message 0 ustdentication Returned RADIUS Access-Request 14 12805 12805 12805 12805 12805 12805 12805 12805 12805 12805 12805 12805 12805 12805	Pv4 Address	1.1 - 1.9	12806	Prepared TLS ServerHello message	0
AD_Join_Point12868Propried TLS Server(Ky)Exchange message26interportProfiled12810Propried TLS Server(Ky)Exchange message0interport12810Propried TLS Server(Ky)Exchange message0interport12808Propried TLS Server(Ky)Exchange message0interport12808Propried TLS Server(Ky)Exchange message0interport12808Propried TLS Server(Ky)Exchange message0interport012808Propried TLS Server(Ky)Exchange message0interport012808Propried TLS Server(Ky)Exchange message0interport012808Propried TLS Server(Ky)Exchange message0interport012808Propried TLS Server(Ky)Exchange message0interport011001Received RADIUS Access-Request14interport012808Propried TLS Perspections exclassing PEAP challenge0interportPropried TLS Perspections exclassing response012808Propried TLS Perspections exclassing PEAP challengeinterport012808Propried TLS Perspections exclassing response0issoch/Pair1506Cylausing Authorization Policy0issoch/Pair1506Cylausing Authorization Policy0issoch/Pair1506Cylausing Authorization Policy0issoch/Pair1506Cylausing Authorization Policy0issoch/Pair1506Cylausing Authorization Policy0issoch/Pair1			12807	Prepared TLS Certificate message	0
12810 Prepared TLS ServerDone message 0 12305 Prepared TLS ServerDone message 0 12305 Prepared EAP-Request with another PEAP challenge 0 12305 Returned RADUS Access-Acquest with another PEAP challenge 0 11008 Returned RADUS Access-Request 14 11018 RADUS Is re-using an existing session 0 12305 Prepared EAP-Request with another PEAP challenge- response 1 12305 Prepared EAP-Request with another PEAP challenge- response 1 12305 Prepared EAP-Request with another PEAP challenge- response 0 12422 Statuting Authorization Policy withertic-type-Framed, authertication fortup 0 12422 Looking up another peaper Authertication fortup 0 12420 Looking up another peaper Authertication fortup	Authentication Identity Store	AD_Join_Point	12808	Prepared TLS ServerKeyExchange message	26
dentify Group Profiled 12305 Prepared EAP-Request with another PEAP challenge 0 undit Session Id 01C2006500000049AA780D80 11006 Returned RADIUS Access-Challenge 0 utthentication Method dof1x 11001 Received RADIUS Access-Challenge 0 utthentication Protocol PEAP (EAP-MSCHAPv2) 12305 Prepared EAP-Request with another PEAP challenge- response 0 iervice Type Framed 12305 Prepared EAP-Request with another PEAP challenge- response 0 iervice Type C1000 service-type-Framed, audit-session-id-0102000650000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-01020006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-0102006500000049AA780D80, audit-session-id-010200650000000000000000, 242209 Isooking up Endpoint in Internal Endpoints IDStore - AD(testuser' 1 0.D-Groups-Names a.fem-sy: m.com/Builtin/Users 24209 Looking up user in Active Directory - AD(testuser' AD(testuser' 1 0.D-Groups-Names a.fem-sy: m.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point, ExternalGroups 1 0.D-Groups-Names a.fem-sy: m.com/Users/Domain Admins 2008 New			12810	Prepared TLS ServerDone message	0
uudit Session id 01C2006500000049AA780D80 11006 Returned RADIUS Access-Challenge 0 uuthentication Method dot1x 11001 Received RADIUS Access-Request 14 uuthentication Protocol PEAP (EAP-MSCHAPy2) 11018 RADIUS is re-using an existing session 0 tervice Type Framed 12304 Extracted EAP-Request with another PEAP challenge- response 12 tervice Type C1000 Service-type-Framed, audt-session-id-01C200650000009AA7800080, method-dot1X, audt-session-id-01C200650000009AA7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A7800080, method-dot1X, audt-session-id-01C200650000009A780080, method-dot1X, audt-session-id-01C200650000009A780080, method-dot1X, audt-session-id-01C2006000000000000000000000000000000000	Identity Group	Profiled	12305	Prepared EAP-Request with another PEAP challenge	0
uuthentication Method dot1x 11001 Received RADIUS Access-Request 14 uuthentication Protocol PEAP (EAP-MSCHAPV2) 11018 RADIUS is re-using an existing session 0 iservice Type Framed 12304 Extracted EAP-Response containing PEAP challenge 1 iservice Type C1000 C1000 12305 Prepared EAP-Request with another PEAP challenge 0 iservice -type = Framed, audit-session-id=01C2006500000049AA780D80, method-dot1x, AuthenticationidentityStore-AD_Join_Point, FQSubjectINme-Zce19620-0842-11e1-aSec- Sce2edb471ditestuser#det reme-sy, tr.com, UniqueSubjectID=92/31674e52338d8f4807c495e1ff4c2ef92 15036 Evaluating Authorization Policy 0 iSceaeAVPair adrem-sy, tr.com/Builtin/Users 24209 Clooking up Endpoint in Internal Endpoints iDStore - AD testuser 1 iD-Groups-Names adrem-sy, tr.com/Builtin/Users 24355 LDAP frech succeeded 1 iD-Groups-Names adrem-sy-tr.ncom/Users/Denied RODC Password Replication Group 15016 Selected Authorization Policy passed 6 iD-Groups-Names adrem-sy-tr.ncom/Users/Domain Admins 22081 Max session solicy passed 6 iD-Groups-Names adrem-sy-tr.ncom/Users/Domain Admins 12306 PEAP authentication succeeded 6 iD-Groups-Names adrem-sy-tr.ncom/Users/Domain Admins 12306 PEAP authorication	Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
humenication Protocol PEAP (EAP-MSCHAPy2) 11018 RADUUS is re-using an existing session 0 kervice Type Framed 12304 Extracted EAP-Regonse containing PEAP challenge- response 1 kervice Type C1000 12305 Prepared EAP-Request with another PEAP challenge 0 service-type-Framed, auth-response service-type-Framed, auth-response 15036 Evaluating Authorization Policy 0 iscoAVPair Service-type-Framed, auth-response Looking up Endpoint in Internal Endpoints IDStore - AD/testuser 0 iscoAVPair Goking up user in Active Directory - AD/testuser 0 uniqueSubjectID=9273/674652338d8f4807c495e1ff4c2er92 2420 Looking up user in Active Directory - AD/testuser 0 D-Groups-Names ad.rem-sy: im.com/Builtin/Users 24355 LOAP feth succeeded 11 D-Groups-Names ad.rem-sy: im.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 D-Groups-Names ad.rem-sy: im.com/Users/Domain Admins 22081 Max sessions goil or easted in Session cache 0 D-Groups-Names ad.rem-sy: im.com/Users/Domain Admins 22081 New accounting session creacted in Session cache 0	Authentication Method	dot1x	11001	Received RADIUS Access-Request	14
utilinetication Protocol PEAP (EAP-MSCHAPV2) 12304 Extracted EAP-Response containing PEAP challenge- response 1 Service Type Framed 12305 Prepared EAP-Request with another PEAP challenge 0 24422 Service-type-Framed, audit-session-id-01C2006500000049AA780D80, method-dottx, 15E has confirmed previous successful machine authentication for user in Active Directory 0 25cooAVPair AuthenticationIdentifyStore-AD_Join_Point, FGSubjectNames-2ce19620-0842-11ef-45ec- 362cectbdf3ditestuser@ad.rem-sy is 1.com, UniqueSubjectID-9273f674652338d8f4807c495e1ff4c2ef92 1779 24209 Looking up Endpoint in Internal Endpoints IDStore - AD(testuser 1 20-Groups-Names ad.rem-sy: m.com/Builtin/Users 24355 LDAP fetch succeeded 1 LD-Groups-Names ad.rem-sy: m.com/Justers/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 LD-Groups-Names ad.rem-sy: th. n.com/Users/Denied RODC Password Replication Group 22080 New accounting session created in Session created 0 LD-Groups-Names ad.rem-sy: th. n.com/Users/Domain Users 12306 PEAP uthentication succeeded 0 LD-Groups-Names ad.rem-sy: th. n.com/Users/Domain Users 12306 New accounting session created in Session created in Session created in Session created in Sessi			11018	RADIUS is re-using an existing session	0
Autory Autory Autory Autory Construction for user in Active Directory 0 Vetwork Device C1000 service-type-Framed, audft-session-id-01C2006500000049AA780D80, method-dot1x, AutoriticationIdentityStore-AD_Join_Point, FGSubjectMane-2ce19620-0842-11ef-aSec- 3262eeetM3/3ditestuser@ad.rem-sy: te 1.com, UniqueSubjectD=92731674e52338dif4807c495e1ff4c2ef92 17/9 15036 Evaluating Authorization Policy 0 24209 Looking up Endpoint In Internal Endpoints IDStore - 3262eeetM3/3ditestuser@ad.rem-sy: te 1.com, UniqueSubjectD=92731674e52338dif4807c495e1ff4c2ef92 17/9 24211 Found Endpoints IDStore - 4D\testuser 1 24211 Found Endpoints In Internal Endpoints IDStore 4d155 LDAP fetch succeeded 3 20-Groups-Names ad.rem-sy: m.com/Builtin/Users 15046 Queried PIP - AD_Join_Point.ExternalGroups 11 20-Groups-Names ad.rem-sy: tr.ncom/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 2006 New accounting session cacted in Session cacted 0 0 20-Groups-Names ad.rem-sy: tr.ncom/Users/Domain Mamins 2080 New accounting session created in Session cacted 0 20-Groups-Names ad.rem-sy: tr.ncom/Users/Domain Users 12306 PEAP authentication succeeded 0 20-Groups-Names ad.rem	Authentication Protocol	PEAP (EAP-MSCHAPV2)	12304	Extracted EAP-Response containing PEAP challenge- response	1
detwork Device C1000 service-type=Framed, audit-session-id=01C200650000049AA780D80, method-dottx, AuthenticationidentityStore-AD_Join_Point, FQSubject/Dava-Zce192620-0842-111e-4.sec 362cec4b4f3dttestuse@ad.rem-sy_te_b.com, UniqueSubject/D-92731674e52338d8f4807c495e1ff4c2ef92 15036 Evaluating Authorization Policy 0 AuthenticationidentityStore-AD_Join_Point, FQSubject/D-92731674e52338d8f4807c495e1ff4c2ef92 Looking up Endpoint in Internal Endpoints IDStore - AD/testuser 1 AD-Groups-Names ad.rem-sy: m.com/Builtin/Users 24325 LDAP fetch succeeded 3 LD-Groups-Names ad.rem-sy: m.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point.ExternalGroups 11 DD-Groups-Names ad.rem-sy: m.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 DD-Groups-Names ad.rem-sy: m.com/Users/Domain Users 22080 New accounting session created in Session cache 0 DD-Groups-Names ad.rem-sy: m.com/Users/Domain Users 12306 PEAP authentication succeeded 0 LD-Groups-Names ad.rem-sy: m.com/Users/Domain Users 11330 Prepared EAP-Success 1 LD-Groups-Names ad.rem-sy: m.com/Users/Domain Users 2080 New accounting session created in Session cache 0 <t< td=""><td></td><td></td><td>12305</td><td>Prepared EAP-Request with another PEAP challenge</td><td>0</td></t<>			12305	Prepared EAP-Request with another PEAP challenge	0
audit-session-id=01C200650000049AA780D80, method=dot1x, AuthentizationIdentityStore-AD_Join_Point, FOSubjectName=2ce19620-0842-11ef-a5ec- 362cec4b413dHtestuse@ad.rem-sy te h.com, UniqueSubjectID=9273f674e52338d8H807c495e1ff4c2ef92 17f9 15036 Evaluating Authorization Policy 0 24209 Looking up Endpoint in Internal Endpoints IDStore - AD\testuser 1 24209 Looking up user in Active Directory - AD\testuser 3 24211 Found Endpoint in Internal Endpoints IDStore 3 24325 Looking up user in Active Directory - AD\testuser 3 24416 User's Groups retrieval from Active Directory succeeded 3 2416 User's Groups retrieval from Active Directory succeeded 11 20-Groups-Names ad.rem-sy::m.com/Builtin/Administrators 15016 Selected Authorization Profile - PermitAccess 5 20-Groups-Names ad.rem-sy::th n.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 20-Groups-Names ad.rem-sy::th n.com/Users/Domain Users 12306 PEAP authentication succeeded 0 20-Groups-Names ad.rem-sy::th n.com/Users/Domain Users 12306 PEAP authentication succeeded 0 20-Groups-Names ad.rem-sy::th n.com/Users/Domain Users 12306 PEAP authentica	Network Device	C1000 service-type=Framed,	24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
International coding, AuthenticationIdentityStore-AD_Join_Point, FOStobleCtName-2ce19620-0842-11ef-a5ec- 362cec4b413dHtestuse@ad.rem-sy te.h.com, UniqueStubjectID=9273f674e52338d8H807c495e1ff42ef92 17f9 24209 Looking up Endpoint in Internal Endpoints IDStore - AD\testuser 1 D-Groups-Names ad.rem-sy::m.com/Builtin/Users 2435 LDAP fetch succeeded 1 LD-Groups-Names ad.rem-sy::m.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point, ExternalGroups 11 LD-Groups-Names ad.rem-sy::m.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point, ExternalGroups 11 LD-Groups-Names ad.rem-sy::m.com/Builtin/Administrators 15016 Selected Authorization Profile - PermitAccess 5 LD-Groups-Names ad.rem-sy::m.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 LD-Groups-Names ad.rem-sy::m.com/Users/Domain Users 12306 PEAP authentication succeeded 0 LD-Groups-Names ad.rem-sy::m.com/Users/Domain Users 12306 PEAP authentication succeeded 0 LD-Groups-Names ad.rem-sy::m.com/Users/Domain Users 11002 Returned RADIUS Access-Accept 0		audit-session-id=01C2006500000049AA780D80,	15036	Evaluating Authorization Policy	0
S52ccc4b473ditestuser@ad.rem-sy.tc.com, UniqueSubjectID-9273f674e52338df4807c495e1ff422ef92 24211 Found Endpoints InIternal Endpoints IDStore 3 LD-Groups-Names ad.rem-sy.tm.com/Builtin/Users 2432 Looking up user In Active Directory - AD/testuser 1 LD-Groups-Names ad.rem-sy.tm.com/Builtin/Users 24416 User's Groups retrieval from Active Directory succeeded 1 LD-Groups-Names ad.rem-sy.tm.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point.ExternalGroups 1 LD-Groups-Names ad.rem-sy.tt.n.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 LD-Groups-Names ad.rem-sy.tt.n.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 LD-Groups-Names ad.rem-sy.tt.n.com/Users/Domain Users 12306 PEAP authentication succeeded 0 LD-Groups-Names ad.rem-sy.tt.n.com/Users/Domain Users 1102 Returned RADIUS Access-Accept 0	CiscoAVPair	AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-	24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
Intersection desizes addread of the size state of the		362cec4b4f3d#testuser@ad.rem-sy_tc_1.com,	24211	Found Endpoint in Internal Endpoints IDStore	3
Ad.rem-sy:::m.com/Builtin/Users 2435 LDAP fetch succeeded D-Groups-Names ad.rem-sy::m.com/Builtin/Administrators 24416 User's Groups retrieval from Active Directory succeeded D-Groups-Names ad.rem-sy::m.com/Users/Denied RODC Password 15048 Queried PIP - AD_Join_Point.ExternalGroups 11 D-Groups-Names ad.rem-sy::m.com/Users/Denied RODC Password 15016 Selected Authorization Profile - PermitAccess 5 D-Groups-Names ad.rem-sy::tr.n.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 D-Groups-Names ad.rem-sy::tr.m.com/Users/Domain Users 12060 Shutdown secure connection with TLS peer 0 D-Groups-Names ad.rem-sy::tr.m.com/Users/Domain Users 1102 Replication SACtive Directory succeeded 0		17/9	24432	Looking up user in Active Directory - AD\testuser	
Addrem synthetic addrem synthetic balance outs 24416 User's Groups retrieval from Active Directory succeeded DD-Groups-Names ad.rem-synth.com/Users/Denied RODC Password Replication Group 15048 Queried PIP - AD_Join_Point.ExternalGroups 11 DD-Groups-Names ad.rem-synth.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 DD-Groups-Names ad.rem-synth.n.com/Users/Domain Admins 2080 New accounting session created in Session cache 0 DD-Groups-Names ad.rem-synth.n.com/Users/Domain Users 12306 PEAP authentication succeeded 0 DD-Groups-Names ad.rem-synth.n.com/Users/Domain Users 1102 Returned RADIUS Access-Accept 1	AD-Groups-Names	ad rem-sw vm.com/Ruiltin/Lisers	24355	LDAP fetch succeeded	
DD-Groups-Names ad.rem-symm.com/Builtin/Administrators 15048 Queried PIP - AD_Join_Point.ExternalGroups 11 DD-Groups-Names ad.rem-symm.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 DD-Groups-Names ad.rem-symm.com/Users/Domain Admins 2008 Max sessions policy passed 0 DD-Groups-Names ad.rem-symm.com/Users/Domain Users 22080 New accounting session created in Session cache 0 DD-Groups-Names ad.rem-symm.com/Users/Domain Users 12306 PEAP authentication succeeded 0 DD-Groups-Names ad.rem-symm.com/Users/Domain Users 1102 Prepared EAP-Success 1	in the second se		24416	User's Groups retrieval from Active Directory succeeded	
Ad.rem-syntin.com/Users/Denied RODC Password Replication Group 15016 Selected Authorization Profile - PermitAccess 5 D-Groups-Names ad.rem-syntin.com/Users/Domain Admins 2081 Max sessions policy passed 0 D-Groups-Names ad.rem-syntin.com/Users/Domain Users 2080 New accounting session created in Session cache 0 D-Groups-Names ad.rem-syntin.com/Users/Domain Users 12306 PEAP authentication succeeded 0 102 Prepared EAP-Success 1 Notes 11002 Returned RADIUS Access-Accept 2	AD-Groups-Names	ad.rem-sim.com/Builtin/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
Replication Group 22081 Max sessions policy passed 0 AD-Groups-Names ad.rem-synth n.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 AD-Groups-Names ad.rem-synth n.com/Users/Domain Users 12306 PEAP authentication succeeded 0 ID-Groups-Names ad.rem-synth n.com/Users/Domain Users 61026 Shutdown secure connection with TLS peer 0 ISD-Groups-Names Info3 Prepared EAP-Success 1 Result 11002 Returned RADIUS Access-Accept 2	AD-Groups-Names	ad.rem-synthesis n.com/Users/Denied RODC Password	15016	Selected Authorization Profile - PermitAccess	5
AD-Groups-Names ad.rem-syntum.com/Users/Domain Admins 22080 New accounting session created in Session cache 0 AD-Groups-Names ad.rem-syntum.com/Users/Domain Users 12306 PEAP authentication succeeded 0 61026 Shutdown secure connection with TLS peer 0 11503 Prepared EAP-Success 1 Result 11002 Returned RADIUS Access-Accept 2		Replication Group	22081	Max sessions policy passed	0
AD-Groups-Names ad.rem-sy"1m.com/Users/Domain Users 12306 PEAP authentication succeeded 0 61026 Shutdown secure connection with TLS peer 0 11503 Prepared EAP-Success 1 Result 11002 Returned RADIUS Access-Accept 2	AD-Groups-Names	ad.rem-synte.n.com/Users/Domain Admins	22080	New accounting session created in Session cache	0
61026 Shutdown secure connection with TLS peer 0 11503 Prepared EAP-Success 1 11002 Returned RADIUS Access-Accept 2	AD-Groups-Names	ad.rem-sylfim.com/Users/Domain Users	12306	PEAP authentication succeeded	0
11503 Prepared EAP-Success 1 11002 Returned RADIUS Access-Accept 2			61026	Shutdown secure connection with TLS peer	0
tesult 11002 Returned RADIUS Access-Accept 2			11503	Prepared EAP-Success	1
	Result		11002	Returned RADIUS Access-Accept	2

使用者身份驗證的詳細資訊

疑難排解

這些調試日誌(prrt-server.log)可幫助您確認ISE中身份驗證的詳細行為。

• runtime-config

- 執行階段記錄
- runtime-AAA

以下是模式1的調試日誌示例。Machine Authentication和User Authentication。

<#root>

// machine authentication

 $MAR, 2024-05-08\ 16:54:50, 582, DEBUG, 0x7 fb2 fd3 db700, cntx = 0000034313, sesn = ise33-01/504417979/41, CPMS ession ID = 01C2006500000049 AA780D8 (2000) and (20$

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com, IDStore=AD_Join_Point an MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionII

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222 MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6\$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

相關資訊

電腦存取限制的優缺點

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)。