# 为请求方访问配置计算机双因素身份验证

## 目录

先决条件
<u>要求</u>
使用的组件
<u>网络图</u>
<u>背景信息</u>
<u>配置</u>
<u>C1000中的配置</u>
Windows PC中的配置
步骤1:将PC添加到AD域
<u>第二步:配置用户身份验证</u>
<u>Windows Server中的配置</u>
<u>步骤1:确认域计算机</u>
<u>第二步:添加域用户</u>
I <u>SE中的配置</u>
<u>步骤1:添加设备</u>
<u>第二步:添加Active Directory</u>
<u>第三步:确认计算机身份验证设置</u>
<u>第四步:添加身份源序列</u>
<u>第五步:添加DACL和授权配置文件</u>
<u>第六步:添加策略集</u>
<u>步骤 7.添加身份验证策略</u>
<u>步骤 8添加授权策略</u>
<u>验证</u>
<u>模式1。计算机身份验证和用户身份验证</u>
<u>步骤1:注销Windows PC</u>
<u>第二步:确认身份验证会话</u>
<u>第三步:登录Windows PC</u>
<u>第四步:确认身份验证会话</u>
<u>第五步:确认Radius实时日志</u>
模式2.仅用户身份验证
<u>步骤1:禁用和启用Windows PC的网卡</u>
<u>第二步:确认身份验证会话</u>
<u>第三步:确认Radius实时日志</u>
<u>故障排除</u>
相关信息

## 简介

本文档介绍使用计算机和dot1x身份验证配置双因素身份验证所需的步骤。

## 先决条件

## 要求

Cisco 建议您了解以下主题:

- 思科身份服务引擎的配置
- Cisco Catalyst的配置
- IEEE802.1X

使用的组件

- 身份服务引擎虚拟3.3补丁1
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 网络图

下图显示本文档示例中使用的拓扑。

在Windows Server 2019上配置的域名是ad.rem-xxx.com,本文档中将其用作示例。



## 背景信息

计算机身份验证是验证寻求访问网络或系统的设备的身份的安全过程。用户身份验证根据用户名和 密码等凭证验证个人身份,而计算机身份验证则不同,它侧重于验证设备本身。这通常使用设备独 有的数字证书或安全密钥来完成。

通过将机器和用户身份验证结合使用,组织可以确保只有经过授权的设备和用户才能访问其网络 ,从而提供更加安全的环境。这种双因素身份验证方法对于保护敏感信息和遵守严格的法规标准特 别有用。

## 配置

### C1000中的配置

这是C1000 CLI中的最低配置。

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

步骤1:将PC添加到AD域

### 导航到控制面板>系统和安全,单击系统,然后单击高级系统设置。在"System Properties"窗口中 ,单击Change,选择Domain并输入域名。

🌯 System and Security		About		
← → → ↑ 💊 → Control Panel → System and Security	v	° Your PC is	monitored and protected.	Related settings
Control Panel Home Security and Mainter Review your computer's st	hance Itus and resolve issues   🚭 Change User Account Control settings	See details in V	findows Security	BitLocker settings Device Manager
System and security     Internet     Hardware and Sound     Windows Defender I	nputer problems Firewall	Device spe	cifications	Remote desktop
Programs Check firewall status Al	low an app through Windows Firewall	Device name	DESKTOP-L2IL916	System protection
Appearance and Personalization See the name of this comp	processor speed   🚱 Allow remote access   Launch remote assistance   uter	Processor	Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)	Advanced system settings
System Properties ×	Computer Name/Domain Changes X			
Computer Name Hardware Advanced System Protection Remote Windows used to following information to identify your computer on the antimode	You can change the name and the membership of this computer. Changes might affect access to network resources.			
Computer description:	Computer name: DESKTOP-L2IL9I6			
For example: "Ktchen Computer" or "Mary's Computer". Full computer name: DESKTOP-L2IL9I6	Full computer name: DESKTOP-L2IL5I6			
Workgroup: WORKGROUP	More			
To use a wizard to join a domain or workgroup, click Network ID	Member of  Domain:  ad rem+, st 'm.com			
To rename this computer or change its domain or Change Change	O Warkgroup: WORKGROUP			

将PC添加到AD域

## 在"Windows安全"窗口中,输入域服务器的用户名和密码。

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

输入用户名和密码

第二步:配置用户身份验证

导航到身份验证,选中启用IEEE 802.1X身份验证。 在"受保护的EAP属性"窗口中单击设置,取消 选中通过验证证书验证服务器身份,然后单击配置。在"EAP MSCHAPv2 Properties"窗口中,选中 Automatically use my Windows logon name and password (and domain if any),以使用在 Windows计算机登录期间输入的用户名进行用户身份验证。

pciPassthru0 Properties X	Protected EAP Properties ×	EAP MSCHAPv2 Properties X
Networking Authentication	When connecting:           Weify the server's identity by validating the certificate	When connecting:
Seect this option to provide authenticated network access for this Ethemat adapter.	Connect to these servers (examples:srv1;srv2;.*/,srv3',com):	password (and domain if any).
Choose a network authentication method:	Trusted Root Certification Authorities:	OK Cancel
Monselt: Protected EAP (PEAP) v Settings	AAA Certificate Services     A     ad-WDKSERVER-CA     Indexee CoherToust Root	
Pemember 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	DigiCert Global Root CA     DigiCert Global Root G2     V	
Additional Settings	Notifications before connecting:	
	Tell user if the server's identity can't be verified $\qquad \lor$	
	Select Authentication Method:	
	Secured password (EAP-MSCHAP v2)  V Configure	
	Enable Fast Reconnect	
OK Canoel	Enable Identity Privacy	
	OK Cancel	

启用用户验证

## 导航到身份验证,选中其他设置。从下拉列表中选择User or computer authentication。

pciPassthru0 Properties	Advanced settings ×
Networking Authentication     Select this option to provide authenticated network access for this Ethemet adapter.     Image: Choose a network authentication method:     Microsoft: Protected EAP (PEAP)     Settings     Image: Choose a network authenticate network access     Microsoft: Protected EAP (PEAP)     Settings     Image: Choose a network authentication method:     Microsoft: Protected EAP (PEAP)     Settings     Image: Choose a network authentication network access     Microsoft: Protected network access     Additional Settings	802.1X settings    Specify authentication mode   User or computer authentication   Delete credentials for all users      Delete credentials for all users      Perform immediately before user logon   Perform immediately after user logon   Maximum delay (seconds):   10   Allow additional dialogs to be displayed during single sign on   This network uses separate virtual LANs for machine and user authentication
OK Cancel	OK Cancel

## Windows Server中的配置

步骤1:确认域计算机

### 导航到Active Directory用户和计算机,单击计算机。确认域中列出了Win10 PC1。

Active Directory Users and Computers		-		×
Eile Action View Help				
🗢 🔿 📶 🔲 🖾 🖓 🚱 🖬 🖏 🎕	7 🗵 🕱	-		
Active Directory Users and Computers [winserver.ad.rem-s] Saved Queries Saved Q	Name DESKTOP-L2IL9I6	Type Comput Comput	er er	

确认域计算机

第二步:添加域用户

## 导航到Active Directory用户和计算机,单击用户。将testuser添加为域用户。

Active Directory Users and Computers File Action View Help						
Active Directory Users and Computers File Action View Help Active Directory Users and Computers (winserver.ad.rem-e) Active Directory Users and Computers (winserver.ad.rem-e) Active Directory Users and Computers Computers Domain Controllers Source Managed Service Accounts Users		Type User Security Group - Domain Local Security Group - Global User Security Group - Global Security Group - Universal Security Group - Universal Security Group - Universal	Description Built-in acco Members in Members of A user acco Members in DNS Admin DNS clients user Properties Member Of Remote contol nerel Address Stat user	ount for administering t this group can have th this group are permits this group that are dor unt managed by the sys this group cannot have istrators Group who are permitted to p Dalen Erwe Remote Desitop Ser Account Profile	the computer/ eir passwords i main controlle ttern. e their passwor erform dunam vices Profile Telephones	Vormain replicated to estificates to rs may be cl rds replicate in undates o ? X Sessions COM- Organization
	He Group Policy Creator Owners Ec Guest He Key Admins En Ades_user	Security Group - Global Bri User Security Group - Global Lai User De	nt name: at name: igilay name:	user last user	jvēsis:	
	Read-only Domain Controllers Schema Admins test user	Security Group - Global Security Group - Global Security Group - Universal User	eaclption: fige:			

添加域用户

## 将域用户添加到域管理员和域用户的成员。

a aber richernes				? X	test user Properties				?	
Member Of	Dial-in	Enviror	nment	Sessions	Remote control	Remote	Desktop Se	ervices Profile	00	M+
Remote control	Remote 0	Desktop Servi	ices Profile	COM+	General Address	Account	Profile	Telephones	Organi	zatio
General Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Env	ironment	Sessio	ons
User logon name:					Member of:					
testuser		@ad.rem-	s,si.sm.com	~	Name	Active Direct	tory Domain	Services Folder	r	
User logon name (pre	-Windows 200	0):			Domain Admins	ad rem-synthe	m.com/Use	975		
AD\		testuser			Domain Users	ad rem-synt.	m.com/Use	ers		
Uplock account										
Uglock account Account gptions: User must chan User cannot ch Password neve Store password Account expires	ge password a ange password r expires using revensibl	t next logon f		< >	Add E Primary group: D	emove	to need to	change Primary		A11
Uglock account Account 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,	. 2024	•	Add E Primary group: Do Set Primary Group	Bemove omain Users There is r you have applicatio	no need to Macintosh ms.	change Primary clients or POSD	group uni K-compilar	ess

域管理员和域用户

ISE中的配置

步骤1:添加设备

导航到管理>网络设备,点击添加按钮以添加C1000设备。

≡	alialia Identity Services	Engine				Administratio	on / Netwo	rk Resources	
Щ	Bookmarks	Network Devices	Network Devi	ce Groups	Network Device Profiles	External RADIUS	Servers	RADIUS Server Sequences	NAC Managers
	Dashboard	Network Devices		Network Devices	List > C1000				
11	Context Visibility	Default Device	05	Network Dev	ices				
×	Operations	berne beening beening	-	Name	C1000				
U	Policy			Description	01000				
20	Administration			Description					
nii.	Work Centers			ID Address	* 10 -	1			
				IP Address	1	/ 32 (g)			
?	Interactive Help			Device Profile	# Cisco	× O			
				Model Name		~			
				Software Vers	ion	~			
				Network Devic	e Group				
				Location	All Locations	~	Set To Defau	it.	
				IPSEC	No	~	Set To Defau	it.	
				Device Type	All Device Types	~	Set To Defau	it.	
				🗹 🗸 RAI	DIUS Authentication Settir	ngs			
				RADIU	S UDP Settings				
				Protoco	RADIUS				
				Shared	Secret cisco123		Hide		

添加设备

### 第二步:添加Active Directory

导航到管理>外部身份源> Active Directory,点击连接选项卡,将Active Directory添加到ISE。

- 加入点名称: AD\_Join\_Point
- Active Directory域: ad.rem-xxx.com

≡	dentity Services I	ingine Administration / identity Management
Щ	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     AD_Join_Point Name AD_Join_Point
-0	Policy	Active Directory ad.rem-st L_m.com
80	Administration	AD_Join_Point

添加Active Directory

导航到Groups选项卡,从下拉列表中选择Select Groups From Directory。

≡	diala Identity Services I	Engine Administration / identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 53	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat
-0	Policy	Select Groups From Directory
80	Administration	Add Group Control Assist ad.rem-sy 3m.com/S-1-5-32-579

从目录中选择组

从下拉列表中单击Retrieve Groups。选中ad.rem-xxx.com/Users/Domain计算机和ad.remxxx.com/Users/Domain用户,然后单击确定。

≡	the identity Services	Engine						×	
н	Bookmarks	Identities Groups E	Sel	lect Directory	/ Groups				
51	Dashboard	Common el     Common el	This d	dialog is used to select gro	ups from the Directo	ry.			
	Context Visibility	1 AD_Join_Poin		Name .	50 . fau	Type ALL			
*	Operations	C LOAP		(Berley Craws)	D Genuera Batriavant				
0	Policy	C BAOLIS Taken							
20	Administration	C ASA Securit	0	Name		Group SID	Group Type		
2	Work Centers	SAM, Id Provide	0	adven-aj i sm.com/Users	Orskánina	5-1-5-21-4110742415-4130520126-20462396	DOMAN LOCAL	-1	
		C Social Login	0	adven-ay amaten/dees	OnsUpdateProxy	5-1-5-21-4193742415-4130820028-20482399	CLOBAL	-1-1	
	Interactive Help		0	ad rem-ay rem.com/Users	Consin Admina	5-1-5-21-411037424115-41331020026-20442399	GLOBAL	- 1	
				ad rem-ay, I, m. com/Quers	/Donain Computers	5-1-5-21-4110742415-4130520026-20462096	GLOBAL	- 1	
			0	adven-c.st.m.com/Vsers	/Domain Controllers	5-1-5-21-4193742415-4133520028-20462399.	GLOBAL	-1-1	
			0	adven-a, Pim.con/Users	/Domain Guesta	5-1-5-21-4110742415-4100520026-20482398.	GLOBAL	-1-1	
			•	adventaj un conféren	/Domain Users	5-1-5-21-4193742415-4130920028-20492098	GLOBAL		
			0	adrem-aj z m.com/Users	Criterprise Admins	5-1-5-21-4193742415-4133520028-20492399.	UNIVERSAL		
			0	adven-aj v m.com/Users	Enterprise Key Admine	5-1-5-21-4110742415-4130520026-20482399.	UNIVERSAL		
			0	advenus, stim.com/Users	Criterprise Read-only	5-1-5-21-4193742415-4133920026-20462399.	UNIVERSAL		
			0	ad.rom-ay.am.com/Ubors	Group Policy Creator	5-1-5-21-4193742415-4130920028-20492399	OLOBAL		
							Cancel	~	

添加域计算机和用户

### 第三步:确认计算机身份验证设置

导航到高级设置选项卡,确认计算机身份验证的设置。

- 启用计算机身份验证:启用计算机身份验证
- Enable Machine Access Restriction:在授权之前将用户和计算机身份验证结合起来







第四步:添加身份源序列

导航到管理>身份源序列,添加身份源序列。

- 名称 : Identity\_AD
- 身份验证搜索列表: AD\_Join\_Point

≡	diale Identity Services I	Engine		Administra	ation / Identity Management	
Щ	Bookmarks	Identities Groups	External Identity Sour	ces Identity Source Sequ	uences Settings	
5	Dashboard	Identity Source Sequer	ices List > Identity_AD			
15	Context Visibility	Identity Source	Sequence			
×	Operations					
.0	Policy	<ul> <li>Identity Source</li> <li>Name</li> </ul>	destitu AD			
80	Administration	Description	Identity_AQ			
nii.	Work Centers	Description			4	
?	Interactive Help	✓ Certificate □ Select Cert	Based Authentication	~		
		✓ Authenticat A set of id	ion Search List entity sources that will be acce	ssed in sequence until first authe	intication succeeds	
		Availat	le	Selected		
		Interna	Endpoints	AD_Join_Point	<b>^</b>	
		Interna	Users			
		All_AD	_Join_Points	_		
添加	身份源序列					

## 第五步:添加DACL和授权配置文件

导航到策略>结果>授权>可下载ACL,添加DACL。

- 名称: MAR\_Passed
- DACL内容: permit ip any host 1.x.x.101和permit ip any host 1.x.x.105

≡	dualis Identity Services E	ngine		Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions Results	]		
	Dashboard	Authentication	Noadable ACL List > MAR_Passed		
망	Context Visibility	Authorization	wnloadable ACL		
~~	Operations	Authorization Profiles	* Name MAR Passed		
0	Policy	Downloadable ACLs	Description		
80	Administration	Profiling >			
nii.	Work Centers	Posture > *[	DACL Content 1234567 permit ip ar	Agnostic () hy host 1.111.0.011	
		Client Provisioning >	8910111 permit ip ar 2131415	iy host 1.133 0.151	
\ <del>∓</del> +r					

添加DACL

导航到策略>结果>授权>授权配置文件,添加授权配置文件。

- 名称: MAR\_Passed
- DACL名称: MAR\_Passed

≡	dentity Services I	Engine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	R	sults	
22	Dashboard	Authentication		Authorization Profiles > MAR_	Passed
110	Context Visibility	Authentication	·	Authorization Profile	
*	Operations	Authorization Profiles	Ť	* Name	
Û	Policy	Downloadable ACLs		0	MAR_Pessed
20	Administration	Profiling	>	Description	
ก็เ	Work Centers	Posture	>	* Access Type	ACCESS_ACCEPT V
		Client Provisioning			
?	Interactive Help	Cherk Provisioning	-	Network Device Profile	
				Track Movement	
				Agentless Posture	
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed V

添加授权配置文件

## 第六步:添加策略集

导航到策略>策略集,点击+添加策略集。

- 策略集名称 : MAR\_Test
- 条件:Wired\_802.1X
- 允许的协议/服务器序列:默认网络访问

=	dealer Identity Services Er	ngine Policy / Policy Sets	4	Evaluation	Aode 89 Cu	<b>.</b> q	۵	0	<b>0</b> I	۹
н	Bookmarks	Policy Sets	R	Click here	to do visib	ility setu	p Do no	t show th	is again	×
51	Dashboard	<ul> <li>Status Policy Set Name Description Conditions</li> </ul>	llowed F	rotocols / S	ierver Seq	uence	Hits	Actions	View	
15	Context Visibility	Q, Search								
*	Operations	MAR, Test     Wired, 802.1X	Jefault N	rtwork Acce	55	/+	15	ø	,	
0	Policy		Continuity N	stands Arrow						
10	Administration	Detault     Detault     Detault					•	102	<u> </u>	
ก็เ	Work Centers						Reset		Save	

步骤 7.添加身份验证策略

导航到策略集,点击MAR\_Test添加身份验证策略。

- 规则名称: MAR\_dot1x
- 条件:Wired\_802.1X
- 使用:Identity\_AD

~	Authentication Policy(2)				
	<ul> <li>Status Rule Name</li> </ul>	Conditions	Use	Hits	Actions
	Q Search				
	MAR_dot1x	E Wined_802.1X	Identity_AD //		ø
	O Default		All_User_ID_Stores //	0	ø
添力	口身份验证策略				

步骤 8添加授权策略

导航到策略集,点击MAR\_Test添加授权策略。

- 规则名称: MAR\_Passed
- 条件:AD\_Join\_Point·ExternalGroups 等于ad.rem-xxx.com/Users/Domain计算机和 Network\_Access\_Authentication\_Passed
- 结果: MAR\_Passed
- 规则名称: User\_MAR\_Passed
- 条件:网络访问·WasMachineAuthenticated EQUALS True 和AD\_Join\_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain用户
- 结果: PermitAccess

VAuthorization Pollcy(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	+ Select from list 🥒 +	- 1	¢
Oefault		DenyAccess 0	+ Select from list 🥒 +	. 9	٩

添加授权策略

## 验证

模式1。计算机身份验证和用户身份验证

步骤1:注销Windows PC

单击Win10 PC1的注销按钮以触发计算机身份验证。



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

第三步:登录Windows PC

登录Win10 PC1,输入用户名和密码以触发用户身份验证。



登录Windows PC

第四步:确认身份验证会话

在C1000中运行show authentication sessions interface GigabitEthernet1/0/2 details命令以确认用户身份验证会话。

#### <#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

#### 第五步:确认Radius实时日志

#### 导航到ISE GUI中的操作> RADIUS >实时日志,确认计算机身份验证和用户身份验证的实时日志。

=							Operations /	RADIUS		en le ser		Levaluation Mode	•••• Q 🏟	⊙ Q	A
н	Bookmarks	Live Lo	gs Live Sessions												
	Dashboard														
명	Context Visibility	м	isconfigured Supplicants 🕕			Mis	configured Network Devices 🕕		RADIUS Drops	• 0	<b>Client Stopped Responding</b>			Repeat Counter	• 0
*	Operations		0				0		0		0			0	
U	Policy										Refresh	Show	20	Within	
2.	Administration										Never	V Latest	20 records 🗸	Last 3 hours	<u> </u>
đ	Work Centers	6	Reset Repeat Counts	▲ Export To ∨										Filter Y 0	f
			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	c
			May 07, 2024 04:36:14	•	0	0	ADitestuser	84.96.91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \Rightarrow User_MAR_Passed$	PermitAccess	1.112.9		
			May 07, 2024 04:36:13	2	ō.		ADitestuser	B4:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess	1.1 2.9	C1000	
			May 07, 2024 04:35:12		à		#ACSACL#-IP-MAR_Passed-6639ba20							C1000	
			May 07, 2024 04:35:12	2	ò		host/DESKTOP-L2IL9I6.ad.rem-s_ithm	B4:96:91:15:84:	Intel-Devi	$MAR\_Test \mapsto MAR\_dot1x$	$MAR_Test \Rightarrow MAR_Passed$	MAR_Passed	169.254.90.1	C1000	

Radius实时日志

确认计算机身份验证的详细实时日志。

#### Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-s,s.bm.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 6 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 0 Extracted EAP-Response/NAK requesting to use PEAP 12301 0 instead 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 Extracted EAP-Response containing PEAP challenge-12302 1 response and accepting PEAP as negotiated 61025 1 Open secure connection with TLS peer 12318 Successfully negotiated PEAP version 0 0 12800 Extracted first TLS record; TLS handshake started 0 0 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 0 12807 Prepared TLS Certificate message 0 12808 Prepared TLS ServerKeyExchange message 25 12810 Prepared TLS ServerDone message 0 Prepared EAP-Request with another PEAP challenge 12305 0 11006 Returned RADIUS Access-Challenge 1 11001 Received RADIUS Access-Request 14 11018 RADIUS is re-using an existing session 0

Steps

计算机身份验证的详细信息

确认用户身份验证的详细实时日志。

#### Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess
Authentication Details	
Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.101 0.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x

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

Steps Sto

用户身份验证的详细信息

Authentication Protocol

#### 模式2.仅用户身份验证

步骤1:禁用和启用Windows PC的网卡

要触发用户身份验证,请禁用和启用Win10 PC1的NIC。

PEAP (EAP-MSCHAPv2)

#### 第二步:确认身份验证会话

在C1000中运行show authentication sessions interface GigabitEthernet1/0/2 details命令以确认用户身份验证会话。

#### <#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

第三步:确认Radius实时日志

导航到ISE GUI中的操作> RADIUS >实时日志,确认用户身份验证的实时日志。



**注意**:由于MAR缓存存储在ISE中,因此只需要用户身份验证。

≡ dentity Services 8	Engine		Operations / RADIUS		🛦 Evaluation Model	■mm Q & ® ₽   ₽
JI Bookmarks	Live Logs					
E Dashboard						
18 Context Visibility	Misconfigured Supplicants ()	Misconfigured	d Network Devices 💿	RADIUS Drops	Client Stopped Responding ()	Repeat Counter
😤 Operations	0		0	0	0	0
I) Policy					Refresh Show	Within
Administration					Never v Later	t 20 records 🗸 Last 3 hours 🗸
Work Centers	Ø to Reser Repear Counts	₫ Export To $∨$				Filter V 🛛 🗢
	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	<ul> <li>AD/destus</li> </ul>	ser 84:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	4.1.11.0.0
	May 07, 2024 04:42:04	AD/pestus	ser 84:96:91:15:84:.	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	1
	May 07, 2024 04:36:13	AD/destus	ser B4:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess	1.1 0.9 C1000
	May 07, 2024 04:35:12	a MACSAOL	H-IP-MAR_Passed-6639ba20			C1000
	May 07, 2024 04:35:12	a host/DES	KTOP-L2IL96.ad.rem-st (.am., 84:96:91:15:84:,	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed MAR_Passed	169.254.90.1 C1000

Radius实时日志

确认用户身份验证的详细实时日志。

#### Cisco ISE

Overview	
vent	5200 Authentication succeeded
Jsername	AD\testuser
indpoint Id	B4:96:91:15:84:CB ⊕
indpoint Profile	Intel-Device
authentication Policy	MAR_Test >> MAR_dot1x
authorization Policy	MAR_Test >> User_MAR_Passed
authorization Result	PermitAccess
Authentication Details	
Source Timestamp	2024-05-07 16:42:04.467
teceived Timestamp	2024-05-07 16:42:04.467
Policy Server	ise33-01
vent	5200 Authentication succeeded
Isername	AD\testuser
indpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
indpoint Profile	Intel-Device
Pv4 Address	1.1 7.9
authentication Identity Store	AD_Join_Point
dentity Group	Profiled
udit Session Id	01C2006500000049AA780D80
authentication Method	dot1x
authentication Protocol	PEAP (EAP-MSCHAPv2)
ervice Type	Framed
letwork Device	C1000
iscoAVPair	service-type=Framed, audit-session-id=01C2006500000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec- 362cec4b413dHtestuser@ad.rem-sy_te_1.com, UniqueSubjectID=92731674e52338d8f4807c495e1ff4c2ef92 17f9

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-s_t.em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
11507	Extracted EAP-Response/Identity	16
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
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
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	25
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	0
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	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge- response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
24432	Looking up user in Active Directory - AD\testuser	
24355	LDAP fetch succeeded	
24416	User's Groups retrieval from Active Directory succeeded	
15048	Queried PIP - AD_Join_Point.ExternalGroups	11
15016	Selected Authorization Profile - PermitAccess	5
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
12306	PEAP authentication succeeded	0
61026	Shutdown secure connection with TLS peer	0
11503	Prepared EAP-Success	1
11002	Returned RADIUS Access-Accept	Z

Steps

用户身份验证的详细信息

AD-Groups-Names

AD-Groups-Names

AD-Groups-Names

AD-Groups-Names

AD-Groups-Names

#### 故障排除

Result

这些调试日志(prrt-server.log)可帮助您确认ISE中身份验证的详细行为。

ad.rem-sy: m.com/Builtin/Users

ad.rem-sym.com/Builtin/Administrators

ad.rem-synte.n.com/Users/Domain Admins

ad.rem-synthm.com/Users/Domain Users

ad.rem-sy-: n.com/Users/Denied RODC Password Replication Group

- 运行时配置 ٠
- 运行日志 •
- 运行时AAA ٠

#### 这是模式1的调试日志示例。计算机身份验证和用户身份验证。

#### <#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,CPMSessionII

#### 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

#### 相关信息

<u>计算机访问限制的优缺点</u>

### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。