Configurar a Autenticação de Fator da Máquina Dois para Acesso do Candidato

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Diagrama de Rede
Informações de Apoio
Configuraçãos
Configuração no PC com Windows
Etapa 1. Adicionar computador ao Domínio do AD
Etapa 2. Configurar autenticação de usuário
Configuração no Windows Server
Etapa 1. Confirmar computadores de domínio
Etapa 2. Adicionar usuário de domínio
Configuração no ISE
Etapa 1. Adicionar dispositivo
Etapa 2. Adicionar Ative Diretory
Etapa 3. Confirmar Configuração de Autenticação do Computador
Etapa 4. Adicionar Sequências de Origem de Identidade
Etapa 5. Adicionar DACL e perfil de autorização
Etapa 6. Adicionar conjunto de políticas
Passo 7. Adicionar política de autenticação
Etapa 8. Adicionar Política de Autorização
Verificar
Padrão 1. Autenticação de máquina e autenticação de usuário
Etapa 1. Sair do Windows PC
Etapa 2. Confirmar sessão de autenticação
Etapa 3. Fazer login no Windows PC
Etapa 4. Confirmar sessão de autenticação
Etapa 5. Confirmar registro ao vivo do Radius
Padrão 2. Somente Autenticação de Usuário
Etapa 1. Desabilitar e Habilitar NIC de PC com Windows
Etapa 2. Confirmar sessão de autenticação
Etapa 3. Confirmar registro ao vivo do Radius
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve as etapas necessárias para configurar a autenticação de dois fatores com a máquina e a autenticação dot1x.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine
- Configuração do Cisco Catalyst
- IEEE802.1X

Componentes Utilizados

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

O nome de domínio configurado no Windows Server 2019 é ad.rem-xxx.com, usado como exemplo neste documento.



Diagrama de Rede

Informações de Apoio

A autenticação de máquina é um processo de segurança que verifica a identidade de um dispositivo que busca acesso a uma rede ou sistema. Diferentemente da autenticação de usuário, que verifica a identidade de uma pessoa com base em credenciais como um nome de usuário e senha, a autenticação de máquina se concentra na validação do próprio dispositivo. Isso é feito frequentemente usando certificados digitais ou chaves de segurança que são exclusivas do dispositivo.

Ao usar a autenticação de máquina e usuário em conjunto, uma organização pode garantir que apenas dispositivos e usuários autorizados possam acessar sua rede, fornecendo, assim, um ambiente mais seguro. Esse método de autenticação de dois fatores é particularmente útil para proteger informações confidenciais e estar em conformidade com padrões regulatórios rigorosos.

Configurações

Configuração no C1000

Essa é a configuração mínima na CLI do C1000.

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

Configuração no PC com Windows

Etapa 1. Adicionar computador ao Domínio do AD

Navegue para Painel de controle > Sistema e segurança, clique em Sistema e em Configurações avançadas do sistema. Na janela Propriedades do sistema, clique em Alterar, selecione Domínio e insira o nome do domínio.

System and Security			About		
←		~ ð	Your PC is r	monitored and protected.	Related settings
Control Panel Home Security and Mainten	ance		See details in W	lindows Security	BitLocker settings
System and Security Review your computer's sta Troubleshoot common com	tus and resolve issues 🌍 Change User Account Control settings aputer problems				Device Manager
Hardware and Sound Windows Defender F	irewall		Device spee	cifications	Remote desktop
Programs Check firewall status All	ow an app through Windows Firewall		Device name	DESKTOP-L2IL9I6	System protection
User Accounts System Appearance and See the name of this compu- Personalization See the name of this compu-	rocessor speed SAllow remote access Launch remote assistance ter		Processor	Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)	Advanced system settings
System Properties X	Computer Name/Domain Changes X				
Computer Name Handware Advanced System Protection Remote Windows uses the following information to identify your computer on the network.	You can change the name and the membership of this computer. Changes might affect access to network resources.				
Computer description:	Computer name: DESKTOP-L2IL9I5				
For example: "Kitchen Computer" or "Mary's Computer", Full computer name: DESKTOP-L2IL9I6	Full computer name: DESKTOP-L2IL3H6				
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 Workgroup: WORKSROUP				

Adicionar computador ao Domínio do AD

Na janela Segurança do Windows, insira o nome de usuário e a senha do servidor de domínio.



Inserir nome de usuário e senha

Etapa 2. Configurar autenticação de usuário

Navegue até Authentication, marque Enable IEEE 802.1X authentication. Clique em Settings na janela Protected EAP Properties, desmarque Verify the server's identity by validating the certificate e clique em Configure. Na janela Propriedades de EAP MSCHAPv2, marque Usar automaticamente meu nome e senha de logon do Windows (e o domínio, se houver) para usar o nome de usuário inserido durante o logon de máquina do Windows para autenticação de usuário.



Habilitar Autenticação de Usuário

Navegue até Authentication, verifique Additional Settings. Selecione User or computer authentication na lista suspensa.

🖗 pciPassthru0 Properties 🛛 🕹	Advanced settings ×
Networkin; Authentication	802.1X settings
Select this option to provide authenticated network access for this Ethemet adapter. Image: Choose an etwork authentication method: Image: Choose a network authentication method: Image: Choose an etwork authentication method: </th <th>Specify authentication mode User or computer authentication Save credentials Delete credentials for all users Central single sign on for this network 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</th>	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users Central single sign on for this network 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

Especificar Modo de Autenticação

Configuração no Windows Server

Etapa 1. Confirmar computadores de domínio

Navegue até Usuários e computadores do Ative Diretory, clique em Computadores. Confirme se o Win10 PC1 está listado no domínio.



Confirmar computador de domínio

Etapa 2. Adicionar usuário de domínio

Navegue até Usuários e computadores do Ative Diretory, clique em Usuários. Adicionar usuário de teste como usuário de domínio.

Active Directory Users and Computers						
File Action View Help						
** 2 📷 4 🖬 🗙 🖬 2 🖬 🖏	💐 🕼 🍸 🚨 💐					
Active Directory Users and Computers [winserver.ad.rem-s	Name	Туре	Description			
	Administrator Allowed RODC Password Replication Group Cert Publishers Conreable Domain Controllers Controllers Domain RODC Password Replication Group DisAdmins Domain RODC Password Replication Group Domain Admins Domain Computers Domain Controllers Domain Guests Controllers Enterprise Admins Enterprise Read-outh Domain Controllers Controllers Domain Set	User Security Group - Domain Local Security Group - Domain Local Security Group - Global User Security Group - Domain Local Security Group - Global Security Group - Global Security Group - Global Security Group - Global	Built-in account for administering the computer/domain Local Members in this group can have their passwords replicated to. Local 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. Local Members in this group cannot have their passwords replicate. Local Members in this group cannot have their passwords replicate. DNS Administrators Group DNS clients who are permitted to perform dynamic updates or test user Properties			
		Security Group - Global Security Group - Global Security Group - Global Security Group - Universal Security Group - Universal	Remote control General Address	Renote Desktop Se Account Profile	rvices Profile Telephones	COM+ Organization
	Group Policy Creator Owners Guest Key Admins ndes_user Protected Users RAS and UAS Servers Read-only Domain Controllers Schema Admins	Security Group - Global User Security Group - Global User Security Group - Global Security Group - Domain L Security Group - Global Security Group - Universal	Bist name: Last name: Display name: Description: Office:	Lee Looker Looker] yetais:	
	test user	User				

Adicionar usuário de domínio

Adicione o usuário de domínio ao membro de Admins. do Domínio e Usuários do Domínio.

				? X	test user Properties				?	
Member Of	Dial-in	Environ	ment	Sessions	Remote control	Remote (Desktop Se	rvices Profile	CO	M+
Remote control	Remote 0	Desktop Servic	es Profile	COM+	General Address	Account	Profile	Telephones	Organi	zatio
ieneral Address	Account	Profile T	elephones	Organization	Member Of	Dial-in	Envi	ronment	Sessio	ns
Jser logon name:					Member of:					
testuser		@ad.rem-s,	,si, am.com	\sim	Name	Active Direct	ory Domain	Services Folder	r	٦
Jser logon name (pre-	Windows 200	0):			Domain Admins	ad rem-sylling	m.com/Use	15		
AD\		testuser			Domain Users	ad.rem-sy-1.r	m.com/Use	rs		
Uglock account		d and leave								
Uglock account Account gotions: User must chan User cannot ch Password never Store password Account expires	ge password a ange password r expires using revensibl	t next logon d le encryption		*	Add E Primary group: D	gemove omain Users		change Primery		
Unjock account ccount gotions: User must chan User cannot ch Password never Store password Account expires Never End of:	ge password a ange password r expires using reversibl Thursday ,	t next logon d le encryption June 6, 3	2024	* · · ·	Add E Primary group: Do Set Primary Group	emove omain Users There is n you have applicatio	to need to o Macintosh ns.	change Primary (clients or POSD	group unk	195

Admins. e Usuários do Domínio

Configuração no ISE

Etapa 1. Adicionar dispositivo

Navegue até Administração > Dispositivos de rede, clique no botão Adicionar para adicionar o dispositivo C1000.

equences NAC Managers

Adicionar dispositivo

Etapa 2. Adicionar Ative Diretory

Navegue para Administração > Fontes de identidade externas > Ative Diretory, clique na guia Conexão e adicione o Ative Diretory ao ISE.

- Nome do ponto de junção: AD_Join_Point
- · Domínio do Ative Diretory: ad.rem-xxx.com

≡	dentity Services	Engine	Administration / identity Management
щ	Bookmarks	Identities Groups External Ident	ty Sources Identity Source Sequences Settings
51	Dashboard		
망	Context Visibility	External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
×	Operations	> 🖻 Certificate Authenticat	* Join Point Name AD_Join_Point
-0	Policy	Active Directory	* Active Directory ad.rem-st. I
20	Administration	AD_Join_Point	Domain

Navegue até a guia Grupos e selecione Selecionar grupos do diretório na lista suspensa.

≡	dentity Services E	gine Administration / identity Management
Л	Bookmarks	Intities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
1:I	Context Visibility	External Identity Sources Connection Allowed Domains PassivelD Groups Attributes Advanced Settings
*	Operations	2 Ger V 2 Ger
0	Policy	Active Directory Select Groups From Directory Select Groups From Directory
å 0	Administration	AD_Join_Point Add Group Control Assist ad.rem-sy im.com/S-1-5-32-579

Selecionar grupos do diretório

Clique em Recuperar grupos na lista suspensa. Marque ad.rem-xxx.com/Users/Domain Computers e ad.rem-xxx.com/Users/Domain Users e clique em OK.

≡										×	
	Fuchante	Identities Groups	Se	lect Directory	Groups					- 1	
	poormarks) Crommo	the Part This C	dialog is used to select grou	ps from the Director	у.				- 1	
55	Dashboard	U Active C	recto c.	omain adven-s rim.com						- 1	
16	Context Visibility	AD_Jok	Poin	Name . Elter	50 . Filter	T	YDE ALL			- 1	
×	Operations	C LOAP		(Berlins Course 1)	a Course Ballinese					- 1	
0	Policy	C opec		and a cope.	а сконра наслечно.					- 1	
1.	Administration	C BSA Sara	0	Name		Group SID		Group Type		- 1	
2	Work Centers	C SAME IN	0	adrem-aj - im.com/Users/D	nakénina	5-1-5-21-41107424/5-4130520026	-20462399	DOMAN LOCAL	-	- 1	
		C Social Los	. 0	adven-ay am.com/Gen/G	InsUpdateProxy	5-1-5-21-4193742415-4133520028	-20462399	CLOBAL		- 1	
(9)	Interactive Main		-	adven-syrrem.com/Users/0	lonain Admina	5-1-5-21-4193742415-4133920026	-20462299	GLOBAL		- 1	
, w			•	adven-sy.i.m.con/Vsers/S	Iomain Computers	5-1-5-21-41907424/5-4100520026	-20462399	GLOBAL		- 1	
			0	adven-r.st.m.con/Users/0	Iomain Controllers	5-1-5-21-4193742415-4133520028	-20482399	CLOBAL		- 8	
			0	adven-a, irsm.con/Users/0	Iomain Guesta	5+1-5-21+4183742415-4133520826	-20482399	GLOBAL		- 1	
			•	advenus un con/Versió	lomain Users	5-1-5-21-4193742415-4130520126	-20442399	GLOBAL		- 1	
			0	adven-a; / m.con/Users/D	interprise Admins	5-1-5-21-4183742415-41335220026	-20482399	UNIVERSAL		- 1	
			0	ad.rem-aj.v.m.com/Users/E	marprisa Kay Admina	5+1-5-21+4193742415-41339520026	-20482399	UNIVERSAL		- 1	
			0	advenue, ir m.con/Users/E	marprise Read-only	5-1-5-21-4193742415-4133520126	-20442399	UNIVERSAL		- 1	
			0	ad.rem-ay.am.com/Users/0	roup Policy Creator	5-1-5-21-4183742415-4133520026	-20482399	CLOBAL		- 1	
			18 H								
								Concest.	~	a	
								Carter	<u> </u>		

Adicionar computadores e usuários de domínio

Etapa 3. Confirmar Configuração de Autenticação do Computador

Navegue até a guia Advanced Settings, confirme a configuração de autenticação de máquina.

- Habilitar Autenticação da Máquina: para habilitar a autenticação da máquina
- Habilitar Restrição de Acesso à Máquina: para combinar autenticação de usuário e máquina antes da autorização



Observação: o intervalo válido de tempo de envelhecimento é de 1 a 8760.



Etapa 4. Adicionar Sequências de Origem de Identidade

Navegue até Administração > Sequências de origem de identidade, adicione uma Sequência de origem de identidade.

- Nome: Identity_AD
- Lista de pesquisa de autenticação: AD_Join_Point

≡	aliada Identity Services I	Engine		Administration / Id	dentity Management
Щ	Bookmarks	Identities Groups Extern	nal Identity Sources	Identity Source Sequences	Settings
53	Dashboard	Identity Source Sequences List > Ide	entity AD		
15 0	Context Visibility	Identity Source Sequence)		
×	Operations				
.0	Policy	 Identity Source Seque Name 	ence		
80	Administration	Identity_AD	7		
di.	Work Centers	Description			h
?	Interactive Help	✓ Certificate Based Aut ☐ Select Certificate Authent	thentication	~	
		✓ Authentication Search A set of identity source	h List es that will be accessed in	sequence until first authentication s	succeeds
		Available		Selected	
		Internal Endpoints	<u>^</u>	AD_Join_Point ^	
		Internal Users			
		Guest Users All AD Join Points			-
			>>>		

Adicionar Sequências de Origem de Identidade

Etapa 5. Adicionar DACL e perfil de autorização

Navegue até Policy > Results > Authorization > Downloadable ACLs e adicione um DACL.

- Nome: MAR_Passed
- Conteúdo da DACL: permit ip any host 1.x.x.101 e permit ip any host 1.x.x.105

≡	dentity Services E	Engine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions R	esults	
	Dashboard	Authentication >	Downloadable ACL List > MAR_Passed	
망	Context Visibility	Authorization	Downloadable ACL	
- %	Operations	Authorization Profiles	* Name MAR Passed	
0	Policy	Downloadable ACLs	Description	
80	Administration	Profiling >	IP version	
-fli	Work Centers	Posture >	* DACL Content 1224567 permit ip any host 1.1 (1).3.101	
		Client Provisioning >	errorist permit (plany nost 1, 13 - 7, 151 213415 1617181	

Adicionar DACL

Navegue até Política > Resultados > Autorização > Perfis de autorização, adicione um perfil de autorização.

- Nome: MAR_Passed
- Nome DACL: MAR_Passed

≡	dentity Services I	Engine	Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	Results
	Dashboard	Authentication	Authorization Profiles > MAR_Passed
망	Context Visibility	Authorization	v Authorization Profile
×	Operations	Authorization Profiles	* Name MAR_Passed
0	Policy	Downloadable ACLs	Description
80	Administration	Profiling	>
nii.	Work Centers	Posture	> ACCESS_ACCEPT V
		Client Provisioning	> Network Device Profile 🗮 Cisco 🗸 🕀
?	Interactive Help		Service Template
			Track Movement
			Agentiess Posture 🛛 🗐 🕐
			Passive identity Tracking 🔲 🕦
			V Common Tasks
			DACL Name MAR_Passed V

Adicionar perfil de autorização

Etapa 6. Adicionar conjunto de políticas

Navegue para Política > Conjuntos de políticas, clique em + para adicionar um conjunto de políticas.

- Nome do Conjunto de Políticas: MAR_Test
- Condições: Wired_802.1X
- Protocolos Permitidos/Sequência de Servidores: Acesso Padrão à Rede

• •	9	2
not show	his agai	n, ×
Actions	View	
ŵ	,	
-	,	
197	-	
	Actions	Actions View

Adicionar conjunto de políticas

Passo 7. Adicionar política de autenticação

Navegue até Policy Sets, clique em MAR_Test para adicionar uma política de autenticação.

- Nome da regra: MAR_dot1x
- Condições: Wired_802.1X
- Uso: Identity_AD

~	Authe	intication	n Policy(2)				
	⊙	Status	Rule Name	Conditions	Use	Hits	Actions
	Q	Search					
	[٥	MAR_dot1x	E Wired_802.1X	Identity_AD /		٩
		0	Default		All_User_ID_Stores /	0	ŵ

Adicionar política de autenticação

Etapa 8. Adicionar Política de Autorização

Navegue até Policy Sets, clique em MAR_Test para adicionar uma política de autorização.

- Nome da Regra: MAR_Passed
- Condições: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computadores AND Network_Access_Authentication_Passed
- Resultados: MAR_Passed
- Nome da regra: User_MAR_Passed
- Condições: Network Access·WasMachineAuthenticated EQUALS True AND AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Usuários
- Resultados: PermitAccess

 Automzation Policy(3) 					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAR_Passed	AND Antonic_Point_ExternalGroups EQUALS ad rem-sp :: im.com/Users/Domain Computers Network_Access_Authentication_Passed	MAR_Passed	+ Select from list / +	1	¢
User_MAR_Passed	b Network Access WasMachineAuthenticated EQUALS True AND AD_Join_Point ExternalGroups EQUALS ad rem-sy tom com/Users/Domain Users	PermitAccess	+ Select from list / +	1	¢
O Default		DenyAccess /	+ Select from list / +	9	٨

Adicionar política de Autorização

Verificar

Padrão 1. Autenticação de máquina e autenticação de usuário

Etapa 1. Sair do Windows PC

Clique no botão Sair do Win10 PC1 para disparar a autenticação da máquina.



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: 01C200650000049AA780D80 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

Etapa 3. Fazer login no Windows PC

Faça login no Win10 PC1, insira o nome de usuário e a senha para disparar a autenticação de usuário.



Fazer login no Windows PC

Etapa 4. Confirmar sessão de autenticação

Execute show authentication sessions interface GigabitEthernet1/0/2 details o comando para confirmar a sessão de autenticação de usuário no C1000.

<#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
```

Etapa 5. Confirmar registro ao vivo do Radius

Navegue para **Operations > RADIUS > Live Logs** na GUI do ISE, confirme o registro em tempo real para autenticação da máquina e autenticação do usuário.

\equiv $\frac{\mathrm{deale}}{\mathrm{core}}$ Identit	y Services Engine		Operations	/ RADIUS	🛕 Exclusion Mode 🖬 Bays 📿	
J. Bookmarks	Live Logs Live Sessions					
E Dashboard						
11 Context Visibil	ity Misconfigured Supplicants 🔘		Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding 📀	Repeat Counter ()
🗙 Operations	0		0	0	0	0
Delicy					Refresh Show	Within
Administration					Never V Latest 20 record	ds 🗸 Last 3 hours 🗸
Work Centers	😂 🏠 Reset Repeat Counts 🕮	L Export To 🗸				Filter V 0
	Time	Status Details	Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorization P IP Addre	ss Network De
 Interactive Hell 	×	~	Identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization Profi IP Addres	is 🗸 Network Devic
	May 07, 2024 04:36:14	o io	0 AD/testuser	04:96:91:15:84: Intel-Davi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess 1.1 2.9	
	May 07, 2024 04:36:13	0	AD\testuser	B4:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess 1.1 \: 3.9	C1000
	May 07, 2024 04:35:12	2 0	#ACSACL#-IP-MAR_Passed-6639ba20			C1000
	May 07, 2024 04:35:12	0	host/DESKTOP-L2IL96.ad.rem-s_imm	B4:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x.	MAR_Test >> MAR_Passed MAR_Passed 109.254.0	10.1 C1000

Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação da máquina.

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 rom.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

Detalhes da autenticação da máquina

Confirme o registro ao vivo detalhado da autenticação do usuário.

Cisco ISE

	Overview		Steps		
	Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
ł			11001	Received RADIUS Access-Request - AD_Join_Point	
	Username	AD\testuser	11017	RADIUS created a new session - ad.rem-sy .em.com	0
	Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	0
	Endpoint Profile	Intel-Device	15008	Evaluating Service Selection Policy	1
ł			11507	Extracted EAP-Response/Identity	7
	Authentication Policy	MAR_Test >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
	Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
	Authorization Result	PermitAccess	11006	Returned RADIUS Access-Challenge	0
ļ			11001	Received RADIUS Access-Request	8
			11018	RADIUS is re-using an existing session	0
	Authentication Details		12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
	Source Timestamp	2024-05-07 16:36:13 748	12300	Prepared EAP-Request proposing PEAP with challenge	1
	oouroo ninostamp	2024 00 07 10.00.10.740	12625	Valid EAP-Key-Name attribute received	0
	Received Timestamp	2024-05-07 16:36:13.748	11006	Returned RADIUS Access-Challenge	0
	Policy Server	ise33-01	11001	Received RADIUS Access-Request	11
	Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
	Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	0
	Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
	Lindpoint id	54100101110104100	12318	Successfully negotiated PEAP version 0	1
	Calling Station Id	B4-96-91-15-84-CB	12800	Extracted first TLS record; TLS handshake started	0
	Endpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
	IPv4 Address	1.111 0.9	12806	Prepared TLS ServerHello message	0
			12807	Prepared TLS Certificate message	0
	Authentication Identity Store	AD_Join_Point	12808	Prepared TLS ServerKeyExchange message	28
	01010		12810	Prepared TLS ServerDone message	0
	Identity Group	Profiled	12305	Prepared EAP-Request with another PEAP challenge	1
	Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
	Authentication Method	dot1x	11001	Received RADIUS Access-Request	30
		etails 2024-05-07 16:36:13.748 2024-05-07 16:36:13.748 ise33-01 5200 Authentication succeeded AD\testuser B4:96:91:15:84:CB B4:96:91-15-84-CB Intel-Device 1.*** 0.9 Ty AD_Join_Point Profiled 01C2006500000049AA780D80 2d dot1x col PEAP (EAP-MSCHAPv2)	11018	RADIUS is re-using an existing session	0
	Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge-	0

Detalhes da autenticação de usuário

Padrão 2. Somente Autenticação de Usuário

Etapa 1. Desabilitar e Habilitar NIC de PC com Windows

Para disparar a autenticação de usuário, desabilite e habilite a placa de rede do Win10 PC1.

Etapa 2. Confirmar sessão de autenticação

Execute show authentication sessions interface GigabitEthernet1/0/2 details o comando para confirmar a sessão de autenticação de usuário no C1000.

<#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

Etapa 3. Confirmar registro ao vivo do Radius

Navegue até **Operations > RADIUS > Live Logs** na GUI do ISE e confirme o registro em tempo real para a autenticação do usuário.



Observação: como o cache MAR é armazenado no ISE, somente a autenticação do usuário é necessária.

≡ deals. Identity Services B	Engine		Operations	/ RADIUS			🛦 Evaluation Mode 🖬 Days 🛛 Q	A 0 0 A
JI Bookmarks	Live Logs Live Sessions							
E Dashboard								
14 Context Visibility	Misconfigured Supplicants 📀		Misconfigured Network Devices 🔘	RADIUS Dro	eps 🕢	Client Stopped Responding	0	Repeat Counter 💿
😤 Operations	0		0	0		0		0
() Policy						Refresh Nover	Show Latest 20 records	Within Last 3 hours
Administration	🖉 🖆 Reser Repear Counts	₫ Export To ∨						Filter ~ 0
	Time	Status Details Rep	ea Identity	Endpoint ID Endpoint.	. Authentication Policy	Authorization Policy	Authorization P IP Address	Network De
(?) Interactive Help	×	×	Identity	Endpoint ID Endpoint I	Authentication Policy	Authorization Policy	Authorization Profi IP Address	V Network Devic
	May 07, 2024 04:42:05	• ā •	AD/pestuser	84:96:91:15:84: Intel-Devi.	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1.1.1.9	
	May 07, 2024 04:42:04	2 3	AD/pestuser	84:96:91:15:84: Intel-Devi.	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1	C1000
	May 07, 2024 04:36:13	2 G	AD/sestuser	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	a a	#ACSACL#-IP-MAR_Passed-6639ba20					C1000
	May 07, 2024 04:35:12	2 G	host/DESKTOP-L2IL9I6.ad.rem-sam	84:96:91:15:84: Intel-Devi.	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed 169.254.00.1.	C1000

Log ao vivo do Radius

Confirme o registro ao vivo detalhado da autenticação do usuário.

Cisco ISE					
Overview			Steps		
Event	5200 Authentication succeeded		Step ID	Description	Latenc
Lyon	S200 Addientication Successed		11001	Received RADIUS Access-Request - AD_Join_Point	
Username	AD\testuser		11017	RADIUS created a new session - ad.rem-s_t.em.com	0
Endpoint Id	B4:96:91:15:84:CB ⊕		15049	Evaluating Policy Group - AD_Join_Point	1
Endpoint Profile	Intel-Device		15008	Evaluating Service Selection Policy	0
			11507	Extracted EAP-Response/Identity	16
Authentication Policy	MAR_Test >> MAR_dot1x		12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
Authorization Policy	MAR_Test >> User_MAR_Passed		12625	Valid EAP-Key-Name attribute received	0
Authorization Result	PermitAccess		11006	Returned RADIUS Access-Challenge	0
			11001	Received RADIUS Access-Request	5
			11018	RADIUS is re-using an existing session	0
Authentication Details			12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
Source Timestamp	2024-05-07 16:42:04.467		12300	Prepared EAP-Request proposing PEAP with challenge	0
Peceived Timestamo	2024-05-07 16-42-04 467		12625	Valid EAP-Key-Name attribute received	0
Received Timestamp	2024-05-07 16.42.04.467		11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01		11001	Received RADIUS Access-Request	25
Event	5200 Authentication succeeded		11018	RADIUS is re-using an existing session	0
Username	AD\testuser		12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
Endpoint Id	B4:96:91:15:84:CB		61025	Open secure connection with TLS peer	0
Calling Station Id	D4_06_01_15_04_0D		12318	Successfully negotiated PEAP version 0	0
calling station to	D4-30-31-13-04-CD		12800	Extracted first TLS record; TLS handshake started	0
Endpoint Profile	Intel-Device		12805	Extracted TLS ClientHello message	0
Pv4 Address	1.1 1 0.9		12806	Prepared TLS ServerHello message	0
Authentication Identity			12807	Prepared TLS Certificate message	0
Store	AD_Join_Point		12808	Prepared TLS ServerKeyExchange message	26
Identity Group	Profiled		12810	Prepared TLS ServerDone message	0
			12305	Prepared EAP-Request with another PEAP challenge	0
Audit Session Id	01C2006500000049AA780D80		11006	Returned RADIUS Access-Challenge	0
Authentication Method	dot1x		11001	Received RADIUS Access-Request	14
Authentication Protocol	PEAP (EAP-MSCHAPv2)		11018	RADIUS IS re-using an existing session	0
Consist Turns	Frank		12304	Extracted EAP-Response containing PEAP challenge- response	1
Network Device	C1000		12305	Prepared EAP-Request with another PEAP challenge	0
	service-type=Framed,		24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
	audit-session-id=01C2006500000049AA780D80, method=dot1x,	1	15036	Evaluating Authorization Policy	0
CiscoAVPair	AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-		24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
	362cec4b4f3d#testuser@ad.rem-sy_te_1.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef92		24211	Found Endpoint in Internal Endpoints IDStore	3
	17/9		24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad.rem-sy: m.com/Builtin/Users		24355	LDAP fetch succeeded	
			24416	User's Groups retrieval from Active Directory succeeded	
AD-Groups-Names	ad.rem-sj:m.com/Builtin/Administrators		15048	Queried PIP - AD_Join_Point.ExternalGroups	11
AD-Groups-Names	ad.rem-synt n.com/Users/Denied RODC Password		15016	Selected Authorization Profile - PermitAccess	5
	Replication Group		22081	Max sessions policy passed	0
AD-Groups-Names	ad.rem-synte.n.com/Users/Domain Admins		22080	New accounting session created in Session cache	0
AD-Groups-Names	ad.rem-symm.com/Users/Domain Users		12306	PEAP authentication succeeded	0
			61026	Shutdown secure connection with TLS peer	0
			11503	Prepared EAP-Success	1
Decult			11002	Returned RADIUS Access-Accept	2

Detalhes da autenticação de usuário

Troubleshooting

Esses logs de depuração (prt-server.log) ajudam a confirmar o comportamento detalhado da autenticação no ISE.

• runtime-config

- runtime-logging
- runtime-AAA

Este é um exemplo do log de depuração para o Padrão 1. Autenticação de máquina e autenticação de usuário neste documento.

<#root>

// machine authentication

 $MAR, 2024-05-08\ 16:54:50, 582, DEBUG, 0x7 fb2 fd3 db700, cntx = 0000034313, sesn = ise33-01/504417979/41, CPMS essionID = 01C2006500000049 AA780 D80, cntx = 0000034313, sesn = ise33-01/504417979/41, CPMS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, cpmS essionID = 01C2006500000049 AA780 D80, sesn = ise33-01/504417979/41, sesn = ise33-01/504417979, sesn = ise33-01/504417979, sesn = ise33-01/5044179, sesn = ise33-01/504417979, sesn = ise33-01/50441799, sesn = isa30-01/50441799, sesn = isa30-01/50441799, sesn = isa30-01/50441799, sesn$

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,CPMSessionI

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

Informações Relacionadas

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.