Configuración de la autenticación de dos factores de máquina para el acceso del suplicante

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Diagrama de la red **Antecedentes Configuraciones** Configuración en C1000 Configuración en PC con Windows Paso 1. Agregar equipo al dominio AD Paso 2. Configurar autenticación de usuario Configuración en Windows Server Paso 1. Confirmar equipos de dominio Paso 2. Agregar usuario de dominio Configuración en ISE Paso 1. Agregar dispositivo Paso 2. Agregar Active Directory Paso 3. Confirmar configuración de autenticación de equipo Paso 4. Agregar secuencias de origen de identidad Paso 5. Agregar DACL y perfil de autorización Paso 6. Agregar conjunto de políticas Paso 7. Agregar política de autenticación Paso 8. Agregar política de autorización Verificación Patrón 1. Autenticación de equipo y autenticación de usuario Paso 1. Cerrar sesión en PC con Windows Paso 2. Confirmar sesión de autenticación Paso 3. Iniciar sesión en Windows PC Paso 4. Confirmar sesión de autenticación Paso 5. Confirmar registro en directo de Radius Patrón 2. Sólo autenticación de usuario Paso 1. Desactivar y activar NIC de PC con Windows Paso 2. Confirmar sesión de autenticación Paso 3. Confirmar registro en directo de Radius **Troubleshoot** Información Relacionada

Introducción

Este documento describe los pasos necesarios para configurar la autenticación de dos factores con autenticación máquina y dot1x.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- · Configuración de Cisco Identity Services Engine
- Configuración de Cisco Catalyst
- IEEE802.1X

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.

El nombre de dominio configurado en Windows Server 2019 es ad.rem-xxx.com, que se utiliza como ejemplo en este documento.



Diagrama de la red

Antecedentes

La autenticación de equipo es un proceso de seguridad que verifica la identidad de un dispositivo que solicita acceso a una red o sistema. A diferencia de la autenticación de usuario, que comprueba la identidad de una persona basándose en credenciales como un nombre de usuario y una contraseña, la autenticación de equipo se centra en validar el propio dispositivo. Esto se suele hacer mediante certificados digitales o claves de seguridad que son únicas para el dispositivo.

Mediante el uso conjunto de la autenticación de equipo y usuario, una organización puede garantizar que solo los dispositivos y usuarios autorizados puedan acceder a su red, lo que proporciona un entorno más seguro. Este método de autenticación de dos factores es especialmente útil para proteger la información confidencial y cumplir con estándares normativos estrictos.

Configuraciones

Configuración en C1000

Esta es la configuración mínima en C1000 CLI.

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

Configuración en PC con Windows

Paso 1. Agregar equipo al dominio AD

Vaya a Panel de control > Sistema y seguridad, haga clic en Sistema y, a continuación, haga clic en Configuración avanzada del sistema. En la ventana Propiedades del sistema, haga clic en Cambiar, seleccione Dominio e ingrese el nombre de dominio.

System and Security				About		
← → ↑ ♦ ,	Control Panel > System and Security		~ õ	Your PC is r	monitored and protected.	Related settings
Control Panel Home	Security and Mainter	ance		See details in W	findows Security	bitcocker settings
System and Security	Y Review your computer's sta Troubleshoot common com	tus and resolve issues 👽 Change User Account Control settings nputer problems				Device Manager
Network and Internet 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 Appearance and Personalization	See the name of this comp	rocessor speed 😻 Allow 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	×	Computer Name/Domain Changes X				
Computer Name Hardwar	re Advanced System Protection Remote the following information to identify your computer	You can change the name and the membership of this computer, Changes might affect access to network resources.				
Computer description:		DESKTOP-L2IL916				
Full computer name:	For example: "Kitchen Computer" or "Mary's Computer". DESKTOP-L2IL916	Full computer name: DESKTOP-L2IL9/6				
Workgroup:	WORKGROUP	More				
To use a wizard to join a o Network ID.	domain or workgroup, click Network ID	Member of Domain: ad rem 4, st 'm.com				
To rename this computer workgroup, click Change.	or change its domain or Change	O Werkgroup: WORKGROUP				

Agregar equipo al dominio AD

En la ventana Seguridad de Windows, introduzca el nombre de usuario y la contraseña del servidor de dominio.



Introducir nombre de usuario y contraseña

Paso 2. Configurar autenticación de usuario

Vaya a Authentication, marque Enable IEEE 802.1X authentication. Haga clic en Configuración en la ventana Propiedades de EAP protegido, desmarque Verificar la identidad del servidor validando el certificado y luego haga clic en Configurar. En la ventana Propiedades de EAP MSCHAPv2, marque Usar automáticamente mi nombre de inicio de sesión y contraseña de Windows (y dominio si lo hubiera) para utilizar el nombre de usuario introducido durante el inicio de sesión de la máquina Windows para la autenticación de usuario.



Habilitar autenticación de usuario

Navegue hasta Autenticación, marque Configuración adicional. Seleccione Autenticación de usuario o equipo en la lista desplegable.

🖗 pciPassthru0 Properties 🛛 🕹	Advanced settings ×
Networkin; Authentication	802.1X settings
Select this option to provide authenticated network access for this Ethemet adapter. Image: Choose a network authentication method: Microsoft: Protected EAP (PEAP) Image: Choose anetwork authenticate for this connection each the Imaged on Image: Choose anetwork authenticate network access	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users Delete credentials for all users Enable single sign on for this network Perform immediately before user logon Perform immediately after 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 autenticación

Configuración en Windows Server

Paso 1. Confirmar equipos de dominio

Vaya a Usuarios y equipos de Active Directory, haga clic en Equipos. Confirme que Win10 PC1 aparezca en el dominio.



Confirmar equipo de dominio

Paso 2. Agregar usuario de dominio

Navegue hasta Usuarios y equipos de Active Directory, haga clic en Usuarios. Agregue testuser como usuario de dominio.

Active Directory Users and Computers								
File Action View Help								
** 2 📷 4 🖬 🗙 🖬 2 💀 🖥 🖬 🕉	🤽 🕼 🍸 🚨 🔍							
Active Directory Users and Computers [winserver.ad.rem-p	Name	Туре		Description				
Senad Queries Senad Queries Senad Computers Domain Controllers Demain Controllers Managed Service Accounts Uses	Administrator Allowed RODC Password Replication Group Cet Publishers Conveble Domain Controllers CetautAccount Denied RODC Password Replication Group DecAdmins DosUpdateProxy Domain Admins Domain Computers Demain Computers	User Security Group - Domain L Security Group - Domain L Security Group - Global User Security Group - Domain L Security Group - Global Security Group - Global Security Group - Global Security Group - Global	ocal ocal ocal test user F	Built-in acc Members in Members of A user acco Members in DNS Admin DNS clients Properties	ount for adm this group of this group of this group of this group of istrators Gro who are per	ninistering can have the are permitt that are do d by the sy cannot hav vip mitted to a four	the computer heir passwords ted to publish main controlle stern. e their passwo perform dunan	Idomain replicated to certificates to rs may be cl rds replicate ric updates p ? X
	B Domain Guests	Security Group - Global	Renot	te control	Renote	Desktop Se	rvices Profile	COM-
	B Domain Users	Security Group - Global	General	Address	Account	Profile	Telephones	Organization
	Benterprise Admins Benterprise Key Admins Benterprise Read-only Domain Controllers	Security Group - Universal Security Group - Universal Security Group - Universal	8	best user			_	
	Group Policy Creator Owners Guest Guest Admins nde_user Protected Users	Security Group - Global User Security Group - Global User Security Group - Global	Brist nam Last nam Digslay r	ne: ne: name:	user lest user		jotale:	
	RAS and IAS Servers Read-only Domain Controllers Schema Admins test user	Security Group - Domain I Security Group - Global Security Group - Universal User	Devolution	5041				

Agregar usuario de dominio

Agregue el usuario de dominio a un miembro de Domain Admins y Domain Users.

Member Of Dial-in		Env	ironment	Sessions	Sessions Remote control		Remote Desktop Services Profile		COM+	
Remote control	Remote I	Desktop Se	arvices Profile	COM+	General Address	Account	Profile	Telephones	Organizati	
ieneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Enviro	nment	Sessio	ons
lser logon name:					Member of:					
estuser		@ad.re	m-6,11.3m.com	\sim	Name	Active Direct	tory Domain S	iervices Folder		
lser logon name (pre	Windows 200	0):			Domain Admins	ad rem-syllin	m.com/Users			
AD\		testuser	r		Domain Users	ad.rem-sy-1.r	m.com/Users			
Unjock account ccount gations:	ge password a	t next logo	n	^	Add.	lemove				
Uglock account ccount gotions: User must chan User cannot ch Password never Store password	ge password a ange password r expires using revensib	t next logo 1 le encryptic	n	~	Add E Primary group: Do	emove				
Uglock account cocount gotions: User must chan User cannot ch Password never Store password Account expires	ge password a ange password r expires using reversib	t next logo d le encryptic	n 20	~ ~ ~	Add E Primary group: Do	emove omain Users There is r	to need to ch	ange Primary (group unit	ess
Uglock account cocunt gotions: User must chan User cannot ch Password never Store password Account expires Never	ge password a ange password expires using reversib	t next logo d le encryptic	n	~	Add E Primary group: Do Set Primary Group	emove omain Users There is n you have applicatio	to need to ch Macintosh ci ns.	ange Primary ; lients or POSID	group unk	ess
Uglock account ccount gotions: User must chan User cannot ch Password never Store password Account expires Never Ognd of:	ge password a ange password r expires using revensib Thursday ,	t next logo d le encryptic June	n on 6, 2024	×	Add E Primary group: Do Set Primary Group	emove omain Users There is n you have applicatio	no need to ch Macintosh ci ns.	ange Primary ; lients or POSD	group unie Geompliar	ess
Uglock account ccount gotions: User must chan User cannot ch Password never Store password Account expires Neyer End of:	ge password a ange password rexpires using reversib Thursday ,	t next logo d le encryptic June	n on 6, 2024	•	Add E Primary group: Do Set Primary Group	emove omain Users There is n you have applicatio	no need to ch Macintosh cl ns.	ange Primary (lents or POSD	group unk	ess
Uglock account ccount gotions: User must chan User cannot ch Password never Store password Account expires Never Ognd of:	ge password a ange password r expires using reversib Thursday ,	t next logo d le encryptic June	n on 6, 2024	•	Add E Primary group: Do Set Primary Group	emove omain Users There is n you have applicatio	no need to ch Macintosh ci ns.	ange Primary (lients or POSID	group unik Coompilar	ess

Administradores de dominio y usuarios de dominio

Configuración en ISE

Paso 1. Agregar dispositivo

Vaya a Administration > Network Devices, haga clic en el botón Add para agregar el dispositivo C1000.

≡	dentity Services Engine				Administration / Network Resources					
Щ	Bookmarks	Network Devices	Network Devic	e Groups N	etwork Device Profiles	External RAD	IUS Servers	RADIUS Server Sequences	NAC Managers	
	Dashboard	Network Devices		Network Devices Lis	at > C1000					
14	Context Visibility	Default Device Device Security Setting	s	Network Devic	ces					
×	Operations	,,	-	Name	C1000					
0	Policy			Description						
20	Administration			Description						
ni:	Work Centers			IP Address	*IP: 101000	/ 22 /	A			
						, 32	ψ.			
(?)	Interactive Help			Device Profile	tte Cisco	~ 0	D			
				Model Name						
				Software Versio	n	~				
				Network Device	Group					
				Location	All Locations		✓ Set To Defa	ult		
				IPSEC	No		✓ Set To Defa	ult		
				Device Type	All Device Types		 Set To Defa 	ult		
				🗹 🗸 RADI	US Authentication Settin	gs				
				RADIUS	UDP Settings					
				Protocol	RADIUS					
				Shared S	ecret cisco123		Hide			

Agregar dispositivo

Paso 2. Agregar Active Directory

Vaya a Administration > External Identity Sources > Active Directory, haga clic en la pestaña Connection, agregue Active Directory a ISE.

- Nombre del punto de unión: AD_Join_Point
- Dominio de Active Directory: ad.rem-xxx.com

≡	duals Identity Services	ne Administration / identity Management	
н	Bookmarks	ntities Groups External Identity Sources Identity Source Sequences Settings	
51	Dashboard		
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings	
*	Operations	Gertificate Authenticat Join Point Name AD_Join_Point	
-0	Policy	Active Directory ad.rem-st. L.m.com	
80	Administration	AD_vioin_Point	

Vaya a la pestaña Grupos, seleccione Seleccionar grupos del directorio en la lista desplegable.

=	elisite Identity Services I	Engine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
phi o	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Contribution authoritiest Contributity Contributity Contribution authority
0	Policy	Select Groups From Directory Select Groups From Directory Select Groups From Directory
å 0	Administration	Add Group Control Assist ad.rem-sy 2m.com/S-1-5-32-579

Seleccionar grupos del directorio

Haga clic en Recuperar grupos de la lista desplegable. Marque ad.rem-xxx.com/Users/Domain Computers y ad.rem-xxx.com/Users/Domain Users y haga clic en OK.

=		Engine					×	A reso
		Manthias Course #	Selec	ct Directory Groups				
1	Bookmarks) Continuer H	This dialo	g is used to select groups from the Directo	<i>ч</i> .			
55	Dashboard	Active Directed	Domai	in adven-s, r m.com				
14	Context Visibility	1 AD_Join_Poin	Nam	4, 50, r Filter	Type ALL Filter			
- 55	Operations	C3 LOAP		(Devices Course) B Devices Detrieved				
-0	Policy	C ocec						
2.	Administration	D PSA Securit	• •	iama ^	Group SID	Group Type		
2	Work Centers	SAML IN Provide	0 *	d.rem-ay i sm.com/Users/DraAdmina	5-1-5-21-4110742415-4130520126-20462399	DOMAIN LOCAL	-	
		C Social Login	0 *	direm-ay am.com/Users/Drol/pdateProxy	5-1-5-21-4193742475-4133520020-20002399	CLOBAL		
œ	Interactive Help			direm-ay rram.com/osers/bumain Admina	5-1-5-21-4193142415-4133520028-20482398	GLOBAL		
			•	diremisy, I, m.con/Users/Donain Computers	5-1-5-21-41107424/5-4100520028-20482099	GLOBAL		
			0.	aren-1, st., is convision from an controllers		CLOBAL		
				direm-a, ir sm. com/deens/domain lovents	5-1-5-21-4183/42415-4133820024-20482399.	OLOBAL COM		
			-	anen-aj un contrae donan cora		- and first av		
			0.	d namen i an anne blann fananska far kånin.	5-1-5-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	INTERNE		
			0.	direction of the second descendent and the second	5-1-5-21-41407424/15-4130820020-20442398	UNIVERSE		
			0.	drem-sy, am.com/Dens/Droug Policy Deator	5-1-5-21-8183742415-4133820028-20882398	GLOBAL		
							*	
							_	
						Cancel	ĸ	



Paso 3. Confirmar configuración de autenticación de equipo

Vaya a la pestaña Advanced Settings y confirme la configuración de la autenticación de la máquina.

- · Habilitar autenticación de equipo: para habilitar la autenticación de equipo
- Habilitar restricción de acceso de equipo: para combinar la autenticación de usuario y equipo antes de la autorización



Nota: el intervalo válido de tiempo de caducidad es de 1 a 8760.



Paso 4. Agregar secuencias de origen de identidad

Vaya a Administration > Identity Source Sequences, agregue una secuencia de origen de identidad.

- Nombre: Identity_AD
- Lista de búsqueda de autenticación: AD_Join_Point

≡	dentity Services I	Engine		Administration / le	dentity Management
Щ	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
- 55	Dashboard	Identity Source Sequence	es List > Identity_AD		
1-l	Context Visibility	Identity Source S	equence		
*	Operations				
0	Policy	✓ Identity Source	e Sequence		
20	Administration	- Name	Identity_AD		
đ	Work Centers	Description			
?	Interactive Help	✓ Certificate B ☐ Select Certificate B	ased Authentication	<u> </u>	
		✓ Authentication	on Search List		
		A set of ide	ntity sources that will be accessed	d in sequence until first authentication s	succeeds
		Available	3	Selected	
		Internal	Endpoints ^	AD_Join_Point	
		Guest U	Jsers		
		All_AD	Join_Points	(
			>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		$\overline{\Sigma}$

Agregar secuencias de origen de identidad

Paso 5. Agregar DACL y perfil de autorización

Navegue hasta Política > Resultados > Autorización > ACL descargables, agregue una DACL.

- Nombre: MAR_Passed
- Contenido DACL: permitir ip any host 1.x.x.101 y permitir ip any host 1.x.x.105

	cisco Identity Services E	ngine	Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	Results
53	Dashboard	Authentication	> Downloadsble ACL List > MAR_Passed
61	Context Visibility	Authorization	Downloadable ACL
*	Operations	Authorization Profiles	* Name MAR_Passed
0	Policy	Downloadable ACLs	Description
80	Administration	Profiling	
-fil	Work Centers	Posture	Agnostic () Agnostic () Agnostic () Agnostic ()
		Client Provisioning	0010111 permit ip any host 1.13 2.151 2131415 141783

Agregar DACL

Vaya a Policy > Results > Authorization > Authorization Profiles, agregue un perfil de autorización.

- Nombre: MAR_Passed
- Nombre de DACL: MAR_Passed

≡	diale Identity Services	Engine			Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions	Results			
	Dashboard	Authentication	> Authorization	Profiles > MAR_Passed		
15	Context Visibility	Authorization	Authorizat	on Profile		
*	Operations	Authorization Profiles	* Name	MAR_Passed		
0	Policy	Downloadable ACLs	Description		-	
a _	Administration	Profiling	>			
nii.	Work Centers	Posture	> Access T	ACCESS_ACCEPT ~	-	
		Client Provisioning	> Network De	rvice Profile 🟥 Cisco 🗸 🕀		
(?)	Interactive Help		Service Ter	nplate		
			Track Move	ment 🔲 🕠		
			Agentless I	Posture 🔲 🕡		
			Passive Ide	ntity Tracking 🔲 🚯		
			✓ Commo	on Tasks		
			DACL I	MAR_Passe	4 V	

Agregar perfil de autorización

Paso 6. Agregar conjunto de políticas

Navegue hasta Policy > Policy Sets, haga clic en + para agregar un conjunto de políticas.

- Nombre del conjunto de políticas: MAR_Test
- Condiciones: Wired_802.1X
- Protocolos / Secuencia de servidor permitidos: acceso a red predeterminado

=	dealer Identity Services Er	gine Policy / Policy Se	ta 🗴 (1997) 1999 1997 1997 1997 1997 1997 1997	ą
н	Bookmarks	Policy Sets	x Click here to do visibility setup Do not show this again.	
21	Dashboard	 Status Policy Set Name Description Conditions 	Allowed Protocols / Server Sequence Hits Actions View	
15	Context Visibility	Q Search		
*	Operations	MAR, Test	Default Network Access 🖉 + 15 🚳 🕨	
±.	Administration	Default Default policy set	Default Network Access 🥜 + o 🎄 🗲	
di.	Work Centers			
			Reset	

Paso 7. Agregar política de autenticación

Navegue hasta Conjuntos de políticas, haga clic en MAR_Test para agregar una política de autenticación.

- Nombre de regla: MAR_dot1x
- Condiciones: Wired_802.1X
- Uso: Identity_AD

Authenticatio	on Policy(2)				
🕣 Status	Rule Name	Conditions	Use	Hits	Actions
Q Searc	h				
٥	MAR_dot1x	@ Wired_802.1X	> Options		ŵ
0	Default		All_User_ID_Stores /	0	¢

Agregar política de autenticación

Paso 8. Agregar política de autorización

Navegue hasta Conjuntos de políticas, haga clic en MAR_Test para agregar una política de autorización.

- Nombre de regla: MAR_Passed
- Condiciones: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- Resultados: MAR_Passed
- Nombre de regla: User_MAR_Passed
- Condiciones: Network Access·WasMachineAuthenticated EQUALS True Y AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Usuarios
- Resultados: PermitAccess

		Results			
🕤 Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAR_Passed	AND R AD_Join_Point ExternalDroups EQUALS ad rem-syim.com/Users/Domain Computers AND Image: Computer Computers Notwork_Access_Authentication_Passed	MAR_Passed	/ + Select from list	<u>+</u> + 1	٩
User_MAR_Passed	ND B Network Access WasMachineAuthenticated EQUALS True R AD_Join_PointExternalQroups EQUALS ad.rem-sy tom.com/Users/Domain Users	PermitAccess	+ Select from list	<u>e</u> + 1	¢
Oefault		DenyAccess	+ Select from list	e + 9	



Verificación

Patrón 1. Autenticación de equipo y autenticación de usuario

Paso 1. Cerrar sesión en PC con Windows

Haga clic en el botón Sign out de Win10 PC1 para activar la autenticación del equipo.



show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de la máquina en 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:

host/DESKTOP-L2IL916.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

Paso 3. Iniciar sesión en Windows PC

Inicie sesión en Win10 PC1, introduzca el nombre de usuario y la contraseña para activar la autenticación de usuario.



Iniciar sesión en Windows PC

Paso 4. Confirmar sesión de autenticación

Ejecute show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de usuario en 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
```

Paso 5. Confirmar registro en directo de Radius

Navegue hasta **Operaciones > RADIUS > Registros en vivo** en la GUI de ISE, confirme el registro en vivo para la autenticación de máquina y la autenticación de usuario.

≡	ababa Identity Services 8	Engine					Operations / F	ADIUS				A Evaluation Mode	. D m)
Щ	Bookmarks	Live Log	gs Live Sessions											
51	Dashboard													
명	Context Visibility	Mis	configured Supplicants			Mis	configured Network Devices 🕕		RADIUS Drops	0	Client Stopped Respon	iding 💿		Repeat Counter 🕕
*	Operations		0				0		0		0			0
U	Policy										Ref	tesh Show	20 records va	Within Last 3 hours
2. Al	Administration Work Centers	ø	Sesec Repear Counts	් Export To 🗸										Fhar 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	V Network Devic
			May 07, 2024 04:36:14	•	0	0	AD/sestuser	84:96:91:15:84:	Intel-Devi	$MAR_{*}Test \mapsto MAR_{*}dot1x$	$MAR_Test \Rightarrow User_MAR_Passe$	d PermitAccess	1.1 3.9	
			May 07, 2024 04:36:13		0		AD/Jestuser	84.96.91:15.84:	Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passe	d PermitAccess	1.1 0.9	C1000
			May 07, 2024 04:35:12	2	ò		#ACSACL#-IP-MAR_Passed-6639ba20							C1000
			May 07, 2024 04:35:12	2	ò		host/DESKTOP-L2IL9I6.ad.rem-s_ithm	84:96:91:15:84:	Intel-Devi	$MAR_Test \mapsto MAR_dot1x$	$MAR_Test \Rightarrow MAR_Passed$	MAR_Passed	169.254.90.1	C1000

Registro en directo de Radius

Confirme el registro en vivo detallado de la autenticación de la máquina.

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 form.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

Detalle de autenticación de máquina

Confirme el registro en vivo detallado de la autenticación de usuario.

Cisco ISE

Overview		Steps		
o lotticu		Step ID	Description	Ŀ
Event	5200 Authentication succeeded	11001	Received RADIUS Access-Request - AD Join Point	
Username	AD\testuser	11017	RADIUS created a new session - ad.rem-syem.com	0
Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	0
Enderint Profile	latel Device	15008	Evaluating Service Selection Policy	1
Endpoint Profile	Intel-Device	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 Desult	Description	11006	Returned RADIUS Access-Challenge	0
Authorization Result	PermitAccess	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
Course Timestern	2024 05 07 16-26-12 749	12300	Prepared EAP-Request proposing PEAP with challenge	1
Source Timestamp	2024-05-07 16:36:13:748	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	1
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	R4-96-91-15-84-CB	61025	Open secure connection with TLS peer	0
chapoliti la	54.50.51.10.04.05	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	1.171.0.9	12806	Prepared TLS ServerHello message	0
		12807	Prepared TLS Certificate message	0
Authentication Identity Store	AD_Join_Point	12808	Prepared TLS ServerKeyExchange message	28
		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
Authention Destar 1	DEAD (FAD MCOUAD-2)	11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge-	0

Latency (ms)

Detalle de la autenticación de usuario

Patrón 2. Sólo autenticación de usuario

Paso 1. Desactivar y activar NIC de PC con Windows

Para activar la autenticación de usuario, inhabilite y habilite la NIC de Win10 PC1.

Paso 2. Confirmar sesión de autenticación

Ejecute show authentication sessions interface GigabitEthernet1/0/2 details el comando para confirmar la sesión de autenticación de usuario en 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

Paso 3. Confirmar registro en directo de Radius

Navegue hasta **Operaciones > RADIUS > Registros en vivo** en la GUI de ISE, confirme el registro en vivo para la autenticación del usuario.



Nota: dado que la caché MAR se almacena en ISE, solo se necesita la autenticación de usuario.

≡ dealer Identity Service	rs Engine	or of the second s	perations / RADIUS	La Evaluation Mode	Q & O Q A
JI Bookmarks	Live Logs Live Sessions				
E Dashboard					
11 Context Visibility	Misconfigured Supplicants 🕢	Misconfigured Network Devices	RADIUS Drops 💿	Client Stopped Responding 💿	Repeat Counter 💿
😤 Operations	0	0	0	0	0
Policy Administration				Rafrosh Show Later	st 20 records v Kithin Last 3 hours v
	හි 🖆 Reset Repeat Counts ර	₫) Export To ∨			Filter V 0
	Time	Status Details Repea Identity	Endpoint ID Endpoint Authentication Polic	cy 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	Q 0 AD(destuser	84:96:91:15:84: Intel-Devi MAR_Test >> MAR_do	t1x MAR_Test >> User_MAR_Passed PermitAccess	1.1.1.3.9
	May 07, 2024 04:42:04	AD/(testuser	04:96:91:15:84: Intel-Devi MAR_Test >> MAR_do	t1x MAR_Test >> User_MAR_Passed PermitAccess	1
	May 07, 2024 04:36:13	AD/destuser	04:96:91:15:84: Intel-Devi MAR_Test >> MAR_do	t1x: MAR_Test >> User_MAR_Passed PermitAccess	1.1. 0.9 C1000
	May 07, 2024 04:35:12	ACSACLE-IP-MAR_Passed-663	95420		C1000
	May 07, 2024 04:35:12	host/DESKTOP-L2IL96.ad.rem-s	C.am., 84:96:91:15:84: Intel-Devi MAR_Test >> MAR_do	ts MAR_Test >> MAR_Passed MAR_Passed	169.254.90.1 C1000

Registro en directo de Radius

Confirme el registro en vivo detallado de la autenticación de usuario.

Cisco ISE				
		Steps		
Overview		otopo		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
Username	ADitestuser	11001	Received RADIUS Access-Request - AD_Join_Point	
o semane		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
Authentication Policy	MAR_Test >> MAR_dot1x	11507	Extracted EAP-Response/Identity	16
A shared and a first start		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
Received Timestamp	2024-05-07 16:42:04.467	12625	Valid EAP-Key-Name attribute received	0
		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
		12318	Successfully negotiated PEAP version 0	0
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	1.1 7.9	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
dominy droup	FIGHER	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 (FAP-MSCHAPv2)	11018	RADIUS is re-using an existing session	0
Service Type	Framed	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	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,	24211	Found Endpoint in Internal Endpoints IDStore	3
	011que3ubjectib=32731674e52338d814807c495e1114c2e192 17f9	24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad rem-swm.com/Builtin/Licere	24355	LDAP fetch succeeded	
-uroups-reames	auten-sy: m.com/buildi/osers	24416	User's Groups retrieval from Active Directory succeeded	
AD-Groups-Names	ad.rem-sym.com/Builtin/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
AD-Groups-Names	ad.rem-sy** n.com/Users/Denied RODC Password	15016	Selected Authorization Profile - PermitAccess	5
-arouva-namea	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-sviitim.com/Users/Domain Licers	12306	PEAP authentication succeeded	0
	and all a meaning and a second a second a second	61026	Shutdown secure connection with TLS peer	0
		11503	Prepared EAP-Success	1
		11002	Returned RADIUS Access-Accept	2

Detalle de la autenticación de usuario

Troubleshoot

Estos registros de depuración (port-server.log) le ayudan a confirmar el comportamiento detallado de la autenticación en ISE.

• runtime-config

- registro en tiempo de ejecución
- Runtime-AAA

Este es un ejemplo del registro de depuración para el Patrón 1. Autenticación de máquina y Autenticación de usuario en este documento.

<#root>

// machine authentication

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

Información Relacionada

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).