Configurer l'authentification à deux facteurs de la machine pour l'accès demandeur

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Diagramme du réseau
Informations générales
Configurations
Configuration dans C1000
Configuration dans le PC Windows
Étape 1. Ajouter un PC au domaine AD
Étape 2. Configurer l'authentification utilisateur
Configuration dans Windows Server
Étape 1. Confirmer les ordinateurs du domaine
Étape 2. Ajouter un utilisateur de domaine
Configuration dans ISE
Étape 1. Ajouter un périphérique
Étape 2. Ajouter Active Directory
Étape 3. Confirmer le paramètre d'authentification ordinateur
Étape 4. Ajouter des séquences source d'identité
Étape 5. Ajouter une DACL et un profil d'autorisation
Étape 6. Ajouter un jeu de stratégies
Étape 7. Ajouter une stratégie d'authentification
Étape 8. Ajouter une stratégie d'autorisation
Vérifier
Modèle 1. Authentification des ordinateurs et des utilisateurs
Étape 1. Se déconnecter d'un PC Windows
Étape 2. Confirmer la session d'authentification
Étape 3. Connexion au PC Windows
Étape 4. Confirmer la session d'authentification
Étape 5. Confirmer le journal Radius en direct
Modèle 2. Authentification utilisateur uniquement
Étape 1. Désactiver et activer la carte réseau du PC Windows
Étape 2. Confirmer la session d'authentification
Étape 3. Confirmer le journal Radius en direct
<u>Dépannage</u>
Informations connexes

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs avec l'authentification machine et dot1x.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine
- Configuration de Cisco Catalyst
- IEEE802.1X

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

Le nom de domaine configuré sur Windows Server 2019 est ad.rem-xxx.com, qui est utilisé comme exemple dans ce document.



Diagramme du réseau

Informations générales

L'authentification de machine est un processus de sécurité qui vérifie l'identité d'un périphérique cherchant à accéder à un réseau ou à un système. Contrairement à l'authentification des utilisateurs, qui vérifie l'identité d'une personne en se basant sur des informations d'identification telles qu'un nom d'utilisateur et un mot de passe, l'authentification des ordinateurs se concentre sur la validation du périphérique lui-même. Cette opération est souvent effectuée à l'aide de certificats numériques ou de clés de sécurité uniques au périphérique.

En utilisant conjointement l'authentification des machines et des utilisateurs, une entreprise peut s'assurer que seuls les périphériques et les utilisateurs autorisés peuvent accéder à son réseau, offrant ainsi un environnement plus sécurisé. Cette méthode d'authentification à deux facteurs est particulièrement utile pour protéger les informations sensibles et respecter des normes réglementaires strictes.

Configurations

Configuration dans C1000

Il s'agit de la configuration minimale de l'interface de ligne de commande 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

Configuration dans le PC Windows

Étape 1. Ajouter un PC au domaine AD

Accédez à Panneau de configuration > Système et sécurité, cliquez sur Système, puis cliquez sur Paramètres système avancés. Dans la fenêtre Propriétés système, cliquez sur Modifier, sélectionnez Domaine et entrez le nom de domaine.

System and Security	Y.			About		
< -> < ∿ •	Control Panel > System and Security		v õ	Your PC is i	monitored and protected.	Related settings
Control Panel Home	Security and Mainten	ance		See details in W	findows Security	BitLocker settings
System and Security	Review your computer's sta	tus and resolve issues SC Change User Account Control settings			,	Device Manager
Network and Internet Hardware and Sound	t Windows Defender F	irewall		Device spe	cifications	Remote desktop
Programs	Check firewall status All	ow an app through Windows Firewall		Device name	DESKTOP-L2IL916	System protection
User Accounts Appearance and Personalization	view amount of RAM and p See the name of this compu	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 Hardwa	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:		Computer name: DESKTOP-L2IL9I5				
Full computer name:	For example: "Kitchen Computer" or "Mary's Computer". DESKTOP-L2IL916	Full computer name: DESKTOP-L2IL5/6				
Workgroup:	WORKGROUP	More				
To use a wizard to join a Network ID.	domain or workgroup, click Network ID	Member of Domain: ad rem-1, st 'm.com				
To rename this computer workgroup, click Change	or change its domain or Change	O Workgroup: WORKSROUP				

Ajouter un PC au domaine AD

Dans la fenêtre Sécurité Windows, entrez le nom d'utilisateur et le mot de passe du serveur de domaine.



Nom d'utilisateur et mot de passe

Étape 2. Configurer l'authentification utilisateur

Accédez à Authentication, cochez Enable IEEE 802.1X authentication. Cliquez sur Settings dans la fenêtre Protected EAP Properties, décochez Verify the server's identity by validating the certificate, puis cliquez sur Configure. Dans la fenêtre Propriétés de EAP MSCHAPv2, cochez Utiliser automatiquement mon nom d'ouverture de session Windows et mon mot de passe (et le domaine s'il y a lieu) pour utiliser le nom d'utilisateur saisi lors de la connexion de l'ordinateur Windows pour l'authentification de l'utilisateur.



Activer l'authentification utilisateur

Accédez à Authentication, cochez Additional Settings. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.

🖗 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 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

Spécifier le mode d'authentification

Configuration dans Windows Server

Étape 1. Confirmer les ordinateurs du domaine

Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Ordinateurs. Vérifiez que Win10 PC1 est répertorié dans le domaine.



Confirmer l'ordinateur du domaine

Étape 2. Ajouter un utilisateur de domaine

Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Utilisateurs. Ajoutez testuser en tant qu'utilisateur de domaine.

Active Directory Users and Computers						
File Action View Help						
💠 🔶 🙍 🛣 🦨 🖬 🖉 🖬 🖇	💐 🗊 🍸 🚨 💐					
Active Directory Users and Computers [winserver.ad.rem-a	Name	Туре	Description			
Adven-sy. sm.com Computers Domain Controllers Domain Controllers Managed Service Accounts Users	Administrator Allowed RODC Password Replication Group Controllers Controller	User Security Group - Domain Loca Security Group - Global User Security Group - Global User Security Group - Global Security Group - Global Security Group - Global Security Group - Global	Built-in acc al Members of Members of A user acco al Members in al DNS Admin DNS clients est user Properties Member Of	ount for administering t this group can have the f this group are permitte f this group that are don unt managed by the sys this group cannot have istrators Group who are permitted to p Dates Error	he computer/ eir passwords ed to publish o nain controlle tern. etheir passwo erform dwnam	domain replicated to retificates to rs may be ct rds replicate ic updates o ? × Seesione
	神見 Domain Guests 絶し Domain Users 絶し Enterprise Admins 絶し Enterprise Key Admins 絶し Enterprise Read-only Domain Controllers	Security Group - Global Security Group - Global Security Group - Universal Security Group - Universal Security Group - Universal	General Address	Account Profile	Telephones	Organization
	B, Group Policy Creator Owners & Guest B, Key Admins B, Indes, user B, Protected Users	Security Group - Global User Security Group - Global User Security Group - Global	Brit name: Last name: Digitay name:	user lest user	ydais:	
	建 RAS and IAS Servers 建 Read-only Domain Controllers 總 Schema Admins & test user	Security Group - Domain L Security Group - Global Security Group - Universal User	Description: Office:			

Ajouter un utilisateur de domaine

Ajoutez l'utilisateur du domaine aux membres Admins du domaine et Utilisateurs du domaine.

Marshar (M	Date	End	transment .	Cassions	Demote control	Demote	Daulitan Car	vices Dudie	00	
Remote control	Bemote	Deskton Se	núces Profile	COM+	General Address	Account	Profile	Telephones	Omani	antin
ieneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Envir	onment	Sessio	ns
her born name:					Mambar of:					
testused		@ad.rec	m-s_si am.com	~	Name	Active Direct	an Domain	Caninas Esidas		
has been some for	Wedness 200				Demain Admine	Active Direct	ory bornari	Services rolde		
/ser logon name (pre-	mindows 200				Domain Liters	ad remark 1	m.com/User			
] Uglock account										
Uglock account	ge password a	t next logor	n	^		Persona				
Uglock account ccount gotions: User must chan User cannot chu Password never	ge password a ange password	t next logor	n	^	Add	Bemove				
Uglock account ccount gotions: User must chan User cannot cha Password never Store password	ge password a ange password expires using revensibl	t next logor 1 le encryptio	n	*	Add I Primary group: D	Bernove omain Users				
Uglock account ccount gotions: User must chan User cannot chu Password never Store password Account expires	ge password a ange password expires using reversibl	t next logor 1 le encryptio	n	~	Add I Primary group: D	Gemove omain Users There is r	no need to c	hange Primary	group unit	555
Uglock account Account gotions: User must chan User cannot cha Password never Store password Account expires Never	ge password a ange password expires using reversibl	t next logor 5 le encryptio	n	< >	Add I Primary group: D Set Primary Group	Bernove omain Users There is r you have acclicatio	to need to c Macintosh	hange Primary (group unk	955 Y
Uglock account Account gotions: User must chan User cannot cha Password never Store password Account expires Never Sind of:	ge password a ange password expires using revensibl Thursday ,	t next logor t le encryptio June	n m 6, 2024	×	Add I Primary group: D Set Primary Group	Gemove omain Users There is r you have applicatio	to need to c Macintosh (ns.	hange Primary ; clients or POSD	group unik Compilar	855 1
Uglock account ccount gotions: User must chan User cannot chu Password never Store password Account expires Neyer Ognd of:	ge password a ange password expires using reversib Thursday ,	t next logor d le encryptio June	n m 6, 2024	•	Add I Primary group: D Set Primary Group	Bernove omain Users There is r you have applicatio	to need to c Macintosh (ns.	hange Primary ; clients or POSD	group unk	ess rt
Unjock account ccount gotions: User must chan User cannot cha Password never Store password Account expires Never End of:	ge password a ange password expires using reversibl Thursday ,	t next logor d le encryptio June	n m 6, 2024	•	Add I Primary group: D Set Primary Group	Bemove omain Users There is n you have applicatio	to need to c Macintosh ns.	hange Primary (group unk	ess rt

Administrateurs de domaine et utilisateurs de domaine

Configuration dans ISE

Étape 1. Ajouter un périphérique

≡	dentity Services I	Engine	Administration / Network Resources
Щ	Bookmarks	Network Devices Network Dev	vice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers
ा ह % 0 2 0	Dashboard Context Visibility Operations Policy Administration	Network Devices Default Device Device Security Settings	Network Devices List > C1000 Network Devices Name C1000 Description
ń.	Work Centers		IP Address v * IP: 1 · 1 · 1 10 / 22
?	Interactive Help		Device Profile 🗮 Cisco 🗸 🕐
			Model Name
			Software Version
			Network Device Group
			Location All Locations V Set To Default
			IPSEC No Set To Default
			Device Type All Device Types V Set To Default
			 RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS Shared Secret cisco123 Hide

Ajouter un périphérique

Étape 2. Ajouter Active Directory

Accédez à Administration > External Identity Sources > Active Directory, cliquez sur l'onglet Connection, ajoutez Active Directory à ISE.

- Nom du point de jointure : AD_Join_Point
- Domaine Active Directory : ad.rem-xxx.com

≡	dentity Services	ingine Administration / Identity Management
Щ	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	G Certificate Authenticat Join Point Name AD_Join_Point
-0	Policy	C Active Directory Active Directory Active Directory
20	Administration	AD_Join_Point

Ajouter Active Directory

Accédez à l'onglet Groups, sélectionnez Select Groups From Directory dans la liste déroulante.

≡	dentity Services	Engine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
15 O	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Castificate Authoriticat Castificate Authoriticat
.0	Policy	Select Groups From Directory
20	Administration	Add Group Control Assist ad.rem-sy im.com/S-1-5-32-579

Sélectionner des groupes dans le répertoire

Cliquez sur Récupérer des groupes dans la liste déroulante. Cochez ad.remxxx.com/Users/Domain Computers et ad.rem-xxx.com/Users/Domain Users et cliquez sur OK.

≡	then the services in the servi	Engine					×	A 100
	-	Identifies Groups E	Sel	ect Directory Groups				
	Desking of) LI CATURDAN AN	This di	ialog is used to select groups from the Direct	ory.			
	Cashacara	Active Directo	Do	main adrem-s r m.com				
	Context Visibility	AD_Join_Poin		lame , SiD Filter Filter	Type ALL Filter			
*	Operations	C (50)		Retrieve Groups	d.			
0	Policy	C RADIUS Token						
3.	Administration	C RSA SecuriD	0	Name ·	Group SID	Group Type		
12	Work Centers	SAML to Provide	0	ad rem-ay 'em.com/Users/Dmit/adateProxy	5-1-5-21-4183742415-4133520028-20082399	GLOBAL	-	
		C Social Login	0	ad rem-ay "em.com/Users/Domain Admina	5-1-5-21-4193742415-4133920026-20482399	GLOBAL		
	Interactive Help			ad.rem-ay, I, m.com/Users/Domain Computers	5-1-5-21-4193742415-4133520026-20462399.	GLOBAL		
			0	ad.rem-r.,st.m.com/Users/Domain Controllers	5+1-5-21-4193742415-4133520528-20482399	OLOBAL		
			0	ad.rem-a, stom.com/Users/Domain Guests	5+1-5-21+4193742415-4133520026-20062399	GLOBAL		
			•	ad.rem-aym.com/Users/Domain Users	5+1+5-21+4193742475-4130520026-20462399	GLOBAL		
			0	ad.rem-a; / m.com/Users/Diterprise Admins	5+1-5-21+4193742415-4133920028-20492399	UNIVERSAL		
			0	ad rem-ay in .com/Users/Enterprise Key Admin	5+1-5-21+4193742415-4133520126-20462399	UNIVERSAL		
			0	ad remins, stilm.com/Users/Enterprise Read-only	5-1-5-21-4193742415-4133820828-20482399.	UNIVERSAL		
			0	ad.rem-ay, am.com/Users/Group Policy Creator	. 5-1-5-21-4193742415-4133920028-20842399	GLOBAL	*	
			×					
						Cancel	OK .	

Ajouter des ordinateurs et des utilisateurs de domaine

Étape 3. Confirmer le paramètre d'authentification ordinateur

Accédez à l'onglet Advanced Settings, confirmez le paramètre de l'authentification de l'ordinateur.

- Enable Machine Authentication : pour activer l'authentification de l'ordinateur
- Enable Machine Access Restriction : pour combiner l'authentification des utilisateurs et des ordinateurs avant l'autorisation



Remarque : la plage de temps de vieillissement valide est comprise entre 1 et 8 760.



Étape 4. Ajouter des séquences source d'identité

Accédez à Administration > Identity Source Sequences, ajoutez une Identity Source Sequence.

- Nom : Identity_AD
- Liste de recherche d'authentification : AD_Join_Point

≡	dialia Identity Services I	Engine Administration / Identity Management
Ц	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	Identity Source Sequences List > Identity_AD
15	Context Visibility	Identity Source Sequence
×	Operations	
U	Policy	V Identity Source Sequence
80	Administration	Identity_AD
đi.	Work Centers	Description
		Å
?	Interactive Help	✓ Certificate Based Authentication □ Select Certificate Authentication Profile ✓
		✓ Authentication Search List
		A set of identity sources that will be accessed in sequence until first authentication succeeds
		Available Selected
		Internal Endpoints AD_Join_Point
		Internal Users
		All_AD_Join_Points
A *		

Ajouter des séquences source d'identité

Étape 5. Ajouter une DACL et un profil d'autorisation

Accédez à Policy > Results > Authorization > Downloadable ACLs, ajoutez une DACL.

- Nom : MAR_Passed
- Contenu DACL : permit ip any host 1.x.x.101 et permit ip any host 1.x.x.105

≡	diada Identity Services I	Engine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions	Results	
53	Dashboard	Authentication	> Downloadable ACL List > MAR_Passed	
명	Context Visibility	Authorization	Downloadable ACL	
*	Operations	Authorization Profiles	* Namo MAR Passar	
0	Policy	Downloadable ACLs	Description	
80	Administration	Profiling	> Duraning @ IDut @ IDuf @ Annantic @	
-fli	Work Centers	Posture	* DACL Content 1234567 permit ip any host 1.1[1].3.101	
		Client Provisioning	2131415 1617181	

Ajouter une DACL

Accédez à Policy > Results > Authorization > Authorization Profiles, ajoutez un profil d'autorisation.

- Nom : MAR_Passed
- Nom DACL : MAR_Passed

≡	dentity Services E	ngine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	Re	sults	
	Dashboard	Authentication	>	Authorization Profiles > MAR_	Passed
망	Context Visibility	Authorization	~	Authorization Profile	
*	Operations	Authorization Profiles		* Name	MAR Passed
0	Policy	Downloadable ACLs		Description	
80	Administration	Profiling	>		
nli	Work Centers	Posture	>	* Access Type	ACCESS_ACCEPT ~
		Client Provisioning	>	Network Device Profile	± Cisco v⊕
(?)	Interactive Help			Service Template	
				Track Movement	
				Agentless Posture	
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed V

Ajouter un profil d'autorisation

Étape 6. Ajouter un jeu de stratégies

Accédez à Policy > Policy Sets, cliquez sur + pour ajouter un jeu de stratégies.

- Nom du jeu de stratégies : MAR_Test
- Conditions : Wired_802.1X
- Protocoles autorisés / Séquence de serveurs : Accès réseau par défaut

=	dentity Services Er	igine Policy / Policy Sets		A Evaluatio	n Mode 89	owyo C	۵ ۵	0	0	۹
н	Bookmarks	Policy Sets		R Click her	e to do vir	sibility set	up Do n	t show t	nis agair	×.
5	Dashboard	Status Policy Set Name Description Conditions	Allow	d Protocols	Server S	equence	Hits	Actions	View	
15	Context Visibility	Q Search								
*	Operations	MAR, Test	Defas	It Network Ac	cess	1+	15	态	,	
0	Policy		Derter	0 Notwork Ar		-		-	-	
8.	Administration	Default Default policy set				<u> </u>	•	1 <u>2</u> 7	'	
ň	Work Centers							_		_
							Reset		Save	

Ajouter un jeu de stratégies

Étape 7. Ajouter une stratégie d'authentification

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'authentification.

- Nom de la règle : MAR_dot1x
- Conditions : Wired_802.1X
- Utiliser : Identity_AD

~	uthent	ication Policy(2)				
	 St 	tatus Rule Name	Conditions	Use	Hits	Actions
	Q s	Search				
	C	MAR_dot1x	Wwed_802.1X	Identity_AD //	n	ø
		O Default		All_User_ID_Stores / Options	0	¢

Ajouter une stratégie d'authentification

Étape 8. Ajouter une stratégie d'autorisation

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'autorisation.

- Nom de la règle : MAR_Passed
- Conditions : AD_Join_Point·ExternalGroups ÉGALE ad.rem-xxx.com/Users/Domain Ordinateurs ET Network_Access_Authentication_Passed
- Résultats : MAR_Passed
- Nom de la règle : User_MAR_Passed
- Conditions : Accès réseau·WasMachineAuthenticated EQUALS True ET AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Utilisateurs
- Résultats : PermitAccess

 Authonization Policy(3) 					
• Status Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
Q Search					
MAR_Passed	AND AD_Join_Point ExternalGroups EQUALS ad rem-sp : im com/Users/Domain Computers ND Network_Access_Authentication_Passed	MAR_Passed	Select from list	i.	ŵ
User_MAR_Passed	ND b Network Access WasMachineAuthenticated EQUALS True AND AD_sJoin_Point External@roups EQUALS ad rem-sy m.com/Users/Domain Users	PermitAccess		i.	ø
Oefault		DenyAccess	Select from list / +	9	٩

Ajouter une stratégie d'autorisation

Vérifier

Modèle 1. Authentification des ordinateurs et des utilisateurs

Étape 1. Se déconnecter d'un PC Windows

Cliquez sur le bouton Déconnexion de Win10 PC1 pour déclencher l'authentification de l'ordinateur.

show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification de la machine dans 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

Étape 3. Connexion au PC Windows

Connectez-vous à Win10 PC1, entrez le nom d'utilisateur et le mot de passe pour déclencher l'authentification utilisateur.

Connexion au PC Windows

Étape 4. Confirmer la session d'authentification

Exécutez show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification utilisateur dans 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 status list:
Method State
dot1x Authc Success
```

Étape 5. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de la machine et l'authentification de l'utilisateur.

≡ dentity Services	Engine		Operations / I	RADIUS			🛦 Evaluation Mode 🛋 Days 🛛 🧯	
JI Bookmarks	Live Logs Live Sessions							
E Dashboard								
Id Context Visibility	Misconfigured Supplicants	Mi	scenfigured Network Devices 🕓	RADIUS Drops	0	Client Stopped Responding		Repeat Counter 🕕
🎌 Operations	0		0	0		0		0
() Policy						Refresh	Show	Within
20 Administration						Never	Catest 20 records Q	Last 3 hours
Work Centers	😂 🏠 Reset Repeat Counts 🛆 Expon	10 \						Filter V 0
	Time Status	Details Repea	Identity	Endpoint ID Endpoint	Authentication Policy	Authorization Policy	Authorization P IP Address	Network De
(?) Interactive Help	×	~	Identity	Endpoint ID Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi IP Address	V Network Devic
	May 07, 2024 04:36:14	0 00	AD(testuser	84:96:91:15:84: Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess 1.1 \2.9	
	May 07, 2024 04:36:13	a .	AD\testuser	84.96.91.15.84: Intel-Devi	MAR_Test >> MAR_dot1s	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess 1.1 2.9	C1000
	May 07, 2024 04:35:12	a a	#ACSACL#-IP-MAR_Passed-6639ba20					C1000
	May 07, 2024 04:35:12	a .	host/DESKTOP-L2IL986.ad.rem-sj.imm	84:96:91:15:84: Intel-Devi	$MAR_Test \mapsto MAR_dottx$	$MAR_Test \mapsto MAR_Passed$	MAR_Passed 169.254.90.1	C1000

Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification de la machine.

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

Détail de l'authentification machine

Confirmez le journal en direct détaillé de l'authentification utilisateur.

Cisco ISE

	Overview		Steps		
	Event	5200 Authentication succeeded	Step ID	Description	Latency (ms
h			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
k			11507	Extracted EAP-Response/Identity	7
I	Authentication Policy	MAR_Test >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
I	Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
I	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
	boulee milestamp	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
			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
			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
			11018	RADIUS is re-using an existing session	0
	Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge-	0

Détail de l'authentification utilisateur

Modèle 2. Authentification utilisateur uniquement

Étape 1. Désactiver et activer la carte réseau du PC Windows

Afin de déclencher l'authentification de l'utilisateur, désactivez et activez la carte réseau de Win10 PC1.

Étape 2. Confirmer la session d'authentification

Exécutez show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification utilisateur dans 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

Étape 3. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de l'utilisateur.

Remarque : le cache MAR étant stocké dans ISE, seule l'authentification des utilisateurs est nécessaire.

≡ dentity Services	Engine	Operation	ns / RADIUS	👗 Evaluation Mode 🗖	
JI Bookmarks	Live Logs Live Sessions				
E Dashboard					
Id Context Visibility	Misconfigured Supplicants 🕓	Misconfigured Network Devices 💿	RADIUS Drops 💿	Client Stopped Responding 💿	Repeat Counter 💿
😤 Operations	0	0	0	0	0
Policy				Rafresh Show Never V Latest 2	Within 0 records 🗸 Last 3 hours 🗸
Work Centers	හි 🕁 Reset Repeat Counts රා); Export To \lor			Filter $\vee = 0$
	Time S	Status Details Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorization P. 1	P Address Network De
(?) Interactive Help	× _	identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization Profi	P Address 🗸 Network Devic
	May 07, 2024 04:42:05	 AD/testuser 	B4:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess 1	3.110.9
	May 07, 2024 04:42:04	AD/testuser	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/testuser	84.96.91:15.84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed PermitAccess 1	.1. 0.9 C1000
	May 07, 2024 04:35:12	ACSACL#-IP-MAR_Passed-6639ba20			C1000
	May 07, 2024 04:35:12	host/DESKTOP-L2IL96.ad.rem-sram	04:96:91:15:84: Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed MAR_Passed 1	69.254.90.1 C1000

Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification utilisateur.

Cisco ISE				
		Stone		
Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
Username	ADItestuser	11001	Received RADIUS Access-Request - AD_Join_Point	
Osemane	ALVIESIUSEI	11017	RADIUS created a new session - ad.rem-s_u.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 sharing in Ballon		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	Received RADIUS Access-Challenge	6
		11018	PADIUS is re-using an existing session	5
		11010	Extracted FAP-Response/NAK requesting to use PFAP	0
Authentication Details		12301	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 LAP-Key-Name attribute received	0
Policy Server	ice22-01	11005	Received PADIUS Access-Gnallenge	25
Policy Server	15633-01	11018	PADIUS is re-using an existing session	25
Event	5200 Authentication succeeded	11010	Extracted FAP-Response containing FAP challenge-	
Username	AD\testuser	12302	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 9.9	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	11018	PADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge-	1
Service Type	Framed		response	-
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
	011quesubjectib=92731674e52338d814607c495e1114c2e192	24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad rem-sw vm.com/Ruiltin/Lisers	24355	LDAP fetch succeeded	
		24416	User's Groups retrieval from Active Directory succeeded	
AD-Groups-Names	ad.rem-sim.com/Builtin/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
AD-Groups-Names	ad.rem-synt in.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-synthm.com/Users/Domain Users	12306	PEAP authentication succeeded	0
		61026	Shutdown secure connection with TLS peer	0
		11503	Prepared EAP-Success	1
Result		11002	Returned RADIUS Access-Accept	2

Détail de l'authentification utilisateur

Dépannage

Ces journaux de débogage (prrt-server.log) vous aident à confirmer le comportement détaillé de l'authentification dans ISE.

• runtime-config

- journalisation de l'exécution
- runtime-AAA

Ceci est un exemple du journal de débogage pour le modèle 1. Authentification de l'ordinateur et authentification de l'utilisateur dans ce document.

<#root>

// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

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

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

subject=machine

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

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

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

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

Inserting new entry to cache

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

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

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

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

user=AD\testuser

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

machine authentication confirmed locally

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

user=AD\testuser

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

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

,MARCache.cpp:316

Informations connexes

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.