サプリカントアクセスのためのマシンの二要素 認証の設定

内容
<u>前提条件</u>
要件
使用するコンポーネント
<u>シーク図</u>
<u>C1000での設定</u>
<u>Windows PCでの設定</u>
<u>ステップ1:PCをADドメインに追加</u>
<u>ステップ2: ユーザ認証の設定</u>
<u>Windows Serverでの設定</u>
<u>ステップ1:ドメインコンピューターの確認</u>
<u>ステップ 2:ドメインユーザの追加</u>
<u>ISEでの設定</u>
<u>ステップ1:デバイスの追加</u>
<u>ステップ 2:Active Directoryの追加</u>
<u>ステップ3:マシン認証設定の確認</u>
<u>ステップ 4:アイデンティティソースシーケンスの追加</u>
<u>ステップ 5:DACLと許可プロファイルの追加</u>
<u>手順6: ポリシーセットの追加</u>
<u>手順7: 認証ポリシーの追加</u>
<u>ステップ 8:許可ポリシーの追加</u>
<u>パターン1マシン認証とユーザ認証</u>
<u>ステップ1:Windows PCからのサインアウト</u>
<u>ステップ 2:認証セッションの確認</u>
<u>ステップ 3:Windows PCへのログイン</u>
<u>ステップ4: 認証セッションの確認</u>
<u>ステップ 5:Radiusライブログの確認</u>
<u>パターン2ユーザ認証のみ</u>
<u>ステップ1:Windows PCのNICを無効および有効にする</u>
<u>ステップ 2:認証セッションの確認</u>

<u>ステップ3:Radiusライブログの確認</u>

<u>トラブルシュート</u>

<u>関連情報</u>

はじめに

このドキュメントでは、マシン認証とdot1x認証を使用した2要素認証を設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Cisco Identity Services Engineの設定
- Cisco Catalyst設定
- IEEE802.1X

使用するコンポーネント

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。

Windows Server 2019で設定されるドメイン名は、このドキュメントの例で使用するad.remxxx.comです。



ネットワーク図

背景説明

マシン認証は、ネットワークまたはシステムへのアクセスを求めるデバイスのIDを確認するセキ ュリティプロセスです。ユーザ名やパスワードなどのクレデンシャルに基づいて個人のアイデン ティティを検証するユーザ認証とは異なり、マシン認証ではデバイス自体の検証に重点が置かれ ます。これは多くの場合、デバイスに固有のデジタル証明書またはセキュリティキーを使用して 行われます。

マシン認証とユーザ認証を組み合わせて使用することで、許可されたデバイスとユーザだけがネ ットワークにアクセスできるようにすることができ、より安全な環境を実現できます。この2要素 認証方式は、機密情報を保護し、厳格な規制基準を遵守するために特に役立ちます。

コンフィギュレーション

C1000での設定

これは、C1000 CLIでの最小限の設定です。

aaa new-model

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

aaa group server radius AAASERVER server name ISE33

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

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

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

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

Windows PCでの設定

ステップ1:PCをADドメインに追加

Control Panel > System and Securityの順に移動し、Systemをクリックしてから、Advanced system settingsをクリックします。System PropertiesウィンドウでChangeをクリックし、 Domainを選択してドメイン名を入力します。

System and Security				About		
← → × ↑ 🍤 Contr	rol Panel > System and Security		v ð	Your PC is i	monitored and protected.	Related settings
Control Panel Home	Security and Mainten	sance		See details in W	Vindows Security	BitLocker settings
System and Security	Review your computer's sta	tus and resolve issues Stange User Account Control settings				Device Manager
Network and Internet Hardware and Sound	Windows Defender F	irewall		Device spe	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	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 Hardware Adv	vanced System Protection Remote	You can change the name and the membership of this computer. Changes might affect access to network resources.				
Computer description:		DESKTOP-L2IL9I5				
For exa Compu Full computer name: DESK	ample: "Ktohen Computer" or "Mary's uter". TOP-L2IL916	Full computer name: DESKTOP-L2IL396				
Workgroup: WORK	KGROUP	More				
To use a wizard to join a domain Network ID.	or workgroup, click Network ID	Member of Domain: ad rem-1, st 'm.com				
To rename this computer or chan workgroup, click Change.	nge its domain or Change	O Workgroup: WORKGROUP				

PCをADドメインに追加

Windowsのセキュリティウィンドウで、ドメインサーバのユーザ名とパスワードを入力します。

	Windows Security	×	Computer Name/Domain Changes	×	Computer Name/Domain Changes
	Computer Name/Domain Changes		Welcome to the ad.rem-s_*tm.com domain.		You must restart your computer to apply these changes
	Enter the name and password of an account with permission join the domain.	n to		_	Before restarting, save any open files and close all programs.
ſ	administrator		OK		holtente
I					ОК
l	••••••				
	OK Cancel				

ユーザ名とパスワードの入力

ステップ2:ユーザ認証の設定

Authenticationに移動し、Enable IEEE 802.1X authenticationにチェックマークを付けます。 Protected EAP PropertiesウィンドウでSettingsをクリックし、Verify the server's identity by validating the certificateのチェックマークを外して、Configureをクリックします。EAP MSCHAPv2 Propertiesウィンドウで、Automatically use my Windows logon name and password (and domain if any)にチェックマークを付けて、Windowsマシンのログイン時に入力したユーザ 名をユーザ認証に使用します。



ユーザ認証の有効化

Authenticationに移動し、Additional Settingsにチェックマークを入れます。ドロップダウンリストからユーザまたはコンピュータの認証を選択します。

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

認証モードの指定

Windows Serverでの設定

ステップ1:ドメインコンピューターの確認

Active Directory Users and Computersに移動し、Computersをクリックします。Win10 PC1がド メインにリストされていることを確認します。

	Active Directory Users and Computers		-		×
1	<u>File Action View H</u> elp				
	🗢 🔿 📶 🖬 🖾 🖓 🏟	🍸 🗾 🔽			
	Active Directory Users and Computers [winserver.ad.rem-s] Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Sim Users	Name DESKTOP-L2IL9I6	Type Comput Comput	er er	

ドメインコンピュータの確認

ステップ2:ドメインユーザの追加

Active Directory Users and Computersに移動し、Usersをクリックします。testuserをドメインユーザとして追加します。

Active Directory Users and Computers						
File Action View Help						
** 2 📷 4 🖬 🗙 🖬 2 🕞 🖬 🖬 🕉	🤽 🕼 🍸 🚨 🔍					
Active Directory Users and Computers [winserver.ad.rem-z	Name	Туре	Description			
Sound Operation S	Administrator Allowed RODC Password Replication Group Cert Publishers Cloneable Domain Controllers DefaultAccount Denied RODC Password Replication Group DesAdmins Domain RODC Password Replication Group DesAdmins Domain Admins Domain Controllers Domain Controllers Domain Controllers Domain Guests Demain Users Enterprise Admins Enterprise Key Admins	User Security Group - Domain Local Security Group - Domain Local Security Group - Global User Security Group - Global Security Group - Universal	Built-in acc al Members in al Members on A user account al DNS Admin DNS clients est user Properties Member Of Remote control General Address Set user	ount for administeri this group can hav f this group that are unt managed by the this group cannot I istrators Group who are cormitted I Dalen 8 Remote Desidop Account Profile	ng the computer their passwords hited to publish domain controlli system. ave their passwo o perform duman invironment. Senices Profile Telephones	/domain replicated to certificates to ers may be (L rds replicate nds replicate ? × Sessions COM+ Organization
	By Entroprise Read-Only Domain Controllers Group Policy Creator Owners Gereat Gereat Rey Admins Anex_user Protected Users RAS and IAS Servers RAS and IAS Servers Read-only Domain Controllers Schema Admins Schema Admins	Security Group - Onversal Security Group - Global User Security Group - Global User Security Group - Global Security Group - Domain I Security Group - Global Security Group - Universal User	Ent name: Last name: Digilay name: Qescryston: Offige:	Veer Veer Jest veer	htals:	

ドメインユーザの追加

Domain AdminsとDomain Usersのメンバにドメインユーザを追加します。

Marshar (M	Date	End	(monet	Cassions	Demote control	Demote	Daskton Canvinas Dudia	~	
Remote control	Bernstell	Remote Darkton Services Public		COM+	General Address	Account Profile Telephone		COM+	
ieneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Environment	Sessi	ons
her loose name:					Member of				
estuser		@ad.re	m-s,si.sm.com	~	Name	Active Direct	ory Domain Services Fold	er.	
lser locon name (pre-	Windows 200	0:			Domain Admins	ad rem-ortim	m.com/Users	-	
AD\	10.000	testuser	r		Domain Users	ad rem-sy "Lu	m.com/Users		
Logon Hours	Log On I	o	n	^		Zermouse			
Logon Hours Uglock account ccount gotions: User must chan User cannot cha Password never Store password	Log On I ge password a inge passworr expires using reversib	o t next logo d le encryptic	n	*	Add E Primary group: D	Bemove omain Users			
Logon Hours Uglock account ccount gotions: User must chang User cannot cha Password never Store password Account expires	Log On I ge password a inge password expires using reversib	o t next logo d le encryptic	n	~	Add E Primary group: D	gemove omain Users There is r you have	to need to change Primary	group uni	less

ドメイン管理者とドメインユーザー

ISEでの設定

ステップ1:デバイスの追加

Administration > Network Devicesの順に移動し、	AddボタンをクリックしてC1000デバイスを追
加します。	

≡	dentity Services I	Engine			Administratio	on / Netwo	rk Resources	
Щ	Bookmarks	Network Devices N	etwork Device Groups	Network Device Profiles	External RADIUS	Servers	RADIUS Server Sequences	NAC Managers
-	Dashboard	Network Devices	Network Devices L	list > C1000				
14	Context Visibility	Default Device Device Security Settings	Network Devi	ices				
*	Operations	and a second sec	Name	C1000				
0	Policy		Description					
20	Administration		Description					
nii:	Work Centers		ID Address	* ID -	/ m =			
			IF Address	1.1.1.0.101	· 32 👳			
(?)	Interactive Help		Device Profile	tte Cisco	× 0			
			Model Name		~			
			Software Versi	on	~			
			Network Devic	e Group				
			Location	All Locations	~	Set To Defau	It	
			IPSEC	No	~	Set To Defau	lt.	
			Device Type	All Device Types	~	Set To Defau	lt.	
			🗹 🗸 RAL	DIUS Authentication Settin	gs			
			RADIUS	S UDP Settings				
			Protoco	RADIUS				
			Shared	Secret cisco123		Hide		

デバイスの追加

ステップ 2: Active Directoryの追加

Administration > External Identity Sources > Active Directoryの順に移動し、Connectionタブをクリックして、Active DirectoryをISEに追加します。

- ・ [結合ポイント名]: AD_Join_Point
- ・ Active Directoryドメイン: ad.rem-xxx.com

	dentity Services I	ine Administration / identity Management
Щ	Bookmarks	ntities Groups External Identity Sources Identity Source Sequences Settings
5	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	> Certificate Authenticat * Join Point Name AD_Join_Point
-0	Policy	Active Directory * Active Directory ad.rem-st. i
80	Administration	AD_Join_Point

Groupsタブに移動し、ドロップダウンリストからSelect Groups From Directoryを選択します。

teo Identity Services E	ingine	Administration / identity Management
okmarks	Identities Groups External Identity Se	Identity Source Sequences Settings
shboard		
ontext Visibility	External Identity Sources Co	Allowed Domains PassiveID Groups Attributes Advanced Settings
perations		ste 🕂 Add - 💿 Delete Group Update SID Values
licy	Certificate Addienticat Active Directory	Selec: Groups From Directory
Iministration	AD_Join_Point	Add Group Control Assist ad.rem-sy 1m.com/S-1-5-32-579
a contraction of the second se	Control Con	Control of the second secon

ディレクトリからグループを選択

Retrieve Groups fromドロップダウンリストをクリックします。ad.rem-xxx.com/Users/Domain Computersとad.rem-xxx.com/Users/Domain Usersにチェックマークを入れて、OKをクリックし ます。

=	the identity Services	Engine					×	A 1-
н	Bookmarks	Identities Groups E	Sele	ect Directory Groups				
::	Dashboard	 Continues et Continues et 	This dial	alog is used to select groups from the Director	у.			
18	Context Visibility	1 AD_Join_Poin	Na	ane, SD, Iter Fitter	Type ALL Filter			
*	Operations	C LOAP		Retrieve Groups				
0	Administration	C RADIUS Token	0	Name A	Group SID	Group Type		
-	Work Centers	C RSA Securio	0	ad rom-aj - om com/Users/Drakdmina	5-1-5-21-4110742415-4130520126-20462399.	DOMAN LOCAL	•	
		🗇 Social Login	0	ad rem-ay rem.com/Users/DrazipdateProxy ad rem-ay rem.com/Users/Donain Admins	5-1-5-21-4110742415-4133020028-20402399 5-1-5-21-4110742415-4133020028-20402399	GLOBAL		
۲	Interactive Help			ad.rem-sy.i.m.com/Users/Domain Computers	5-1-5-21-4110742415-4100520026-20462090	61.0844		
			0	ad rem-r. stum.com/Users/Domain Controllers	8-1-8-21-4183742418-4133820828-20482399	CLOBAL		
				ad rem-a, intercontribunationale Galeria ad rem-ay - Um.contribunationale Users	5-1-5-21-4110742415-4130520024-20462399 5-1-5-21-4110742415-4130520024-20462399	GLOBAL GLOBAL		
			0	ad rem-a) / m.com/Users/Enterprise Admins	5-1-5-21-4183742415-4133520528-20482399	UNIVERSAL	1.1	
			0	ad rem-a) 7 m.com/Users/Enterprise Kay Admina	5-1-5-21-4110742415-4132520026-20462299	UNIVERSAL		
			0	ad remis, stim.com/Users/Enterprise Read-only ad remisy, am.com/Users/Enterprise Policy Creater	5-1-5-21-4193742475-4133920026-20462399 5-1-5-21-4193742475-4133920026-20462399	CLOBAL		
			×.				*	
						Cancel		

ドメインコンピューターとユーザーの追加

ステップ3:マシン認証設定の確認

Advanced Settingsタブに移動し、マシン認証の設定を確認します。

- マシン認証の有効化:マシン認証を有効にします。
- マシンアクセス制限の有効化:認証の前にユーザ認証とマシン認証を組み合わせます。



注:エージングタイムの有効範囲は1~8760です。



ステップ4:アイデンティティソースシーケンスの追加

Administration > Identity Source Sequencesの順に移動し、Identity Source Sequenceを追加します。

- 名前: Identity_AD
- ・ 認証検索リスト: AD_Join_Point

≡	alialia Identity Services I	ngine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 55	Dashboard	Identity Source Sequences List > Identity AD
1 ¹⁰	Context Visibility	Identity Source Sequence
*	Operations	
0	Policy	V Identity Source Sequence
20	Administration	Identity_AD
đi.	Work Centers	Description
?	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
		Guest Users
アイ	デンティティソース	シーケンスの追加

ステップ5:DACLと許可プロファイルの追加

Policy > Results > Authorization > Downloadable ACLsの順に移動し、DACLを追加します。

- 名前: MAR_Passed
- ・DACLコンテンツ: permit ip any host 1.x.x.101およびpermit ip any host 1.x.x.105

≡	dentity Services E	Engine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions Re	sults	
	Dashboard	Authentication >	Downloadable ACL List > MAR_Passed	
15	Context Visibility	Authorization	Downloadable ACL	
- %	Operations	Authorization Profiles	there was presed	
0	Policy	Downloadable ACLs	Description	
80	Administration	Profiling >	IP version * IPv4 © IPv6 © Agnostic	
ส้น	Work Centers	Posture >	* DACL Content 1234567 permit ip any host 1.11.3.101	
		Client Provisioning >	2131415 1617181	

DACLの追加

Policy > Results > Authorization > Authorization Profilesの順に移動し、認可プロファイルを追加 します。

- 名前:MAR_Passed
- DACL名:MAR_Passed

Identity Services E	ngine			Policy / Policy Elements
lookmarks	Dictionaries Conditions	Re	sults	
ashboard	Authentication	>	Authorization Profiles > MAR_	Passed
Context Visibility	Authorization	~	Authorization Profile	
perations	Authorization Profiles		* Name	MAR_Passed
olicy	Downloadable ACLs		Description	
dministration	Profiling	>		R
Vork Centers	Posture	>	* Access Type	ACCESS_ACCEPT V
	Client Provisioning	>	Network Device Profile	± Cisco ∨ ⊕
nteractive Help			Service Template	
			Track Movement	
			Agentless Posture	
			Passive Identity Tracking	
			✓ Common Tasks	
			DACL Name	MAR_Passed V
	view Identity Services E ashboard ontext Visibility perations alicy dministration ork Centers teractive Help	the interview of the second se	teractive Help	Dictionaries Conditions Results ashboard Authorization Authorization Profiles ontext Visibility Authorization Profiles Authorization Profiles brigg Authorization Profiles Authorization Profiles brinistration Profiling Profiling brigg Client Provisioning * Access Type Client Provisioning Network Device Profile Service Template Track Movement Agentiess Posture Passive Identity Tracking Client Provisioning Common Tasks

許可プロファイルの追加

手順6:ポリシーセットの追加

Policy > Policy Setsの順に移動し、+ をクリックしてポリシーセットを追加します。

- ・ポリシーセット名:MAR_Test
- 条件:Wired_802.1X
- •許可されるプロトコル/サーバシーケンス:デフォルトのネットワークアクセス

=	dealer Identity Services E	Engine Policy / Policy Sets		A type	ion Mode 81	9 0 m C	۵ ۵	0	01	۹
J	Bookmarks	Policy Sets		R Click h	ere to do v	isibility set	up Do n	ot show th	his agair	×
	Dashboard	Conditions	Allow	ed Protocol	s / Server	Sequence	Hits	Actions	View	
1ª	Context Visibility	Q Search								
*	Operations	MAR_Test Wired_802.1X	Defa	lt Network /	locess	× +	15	٥	>	
2.	Administration	Default Default Default	Defa	it Network i	Access	<u>×</u> +	۰	٢	•	
ñ	Work Centers									
							Reset		Save	

ポリシーセットの追加

手順7:認証ポリシーの追加

Policy Setsに移動し、MAR_Testをクリックして認証ポリシーを追加します。

- ルール名:MAR_dot1x
- 条件:Wired_802.1X
- 使用:Identity_AD

C	~Authe	ntication	Policy(2)				
	۲	Status	Rule Name	Conditions	Use	Hits	Actions
	Q	Search					
		0	MAR_dot1x	Wind_802.1X	Identity_AD //	11	¢
		0	Default		All_User_ID_Stores /	0	ŵ
			- >				

認証ポリシーの追加

Policy Setsに移動し、MAR_Testをクリックして認可ポリシーを追加します。

- ルール名: MAR_Passed
- ・条件:AD_Join_Point・ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers およびNetwork_Access_Authentication_Passed
- 結果: MAR_Passed
- ルール名: User_MAR_Passed
- 条件:ネットワークアクセス・WasMachineAuthenticated EQUALS True AND AD_Join_Point・ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Users
- 結果: PermitAccess

· Additionational Policy(3)			
		Results	
🕣 Status Rule Name	Conditions	Profiles Securi	Ity Groups Hits Actions
Q Search			
MAR_Passed	AND R AD_Join_Point External@roups EQUALS ad rem-s; ``im.com/Users/Domain Computers Network_Access_Authentication_Passed	MAR_Passed / + Select	ct from list 🥒 🕂 t 🔯
User_MAR_Pass	id AND & Network Access WasMachineAuthenticated EQUALS True A AD_Join_PointExternalGroups EQUALS ad.rem-sy tom.com/Users/Domain Users	PermitAccess	et from list 🥒 🕂 t 🚳
O Default		DenyAccess / + Select	ct from list 🥒 + 🧕 🚳

ステップ8:許可ポリシーの追加

確認

パターン1マシン認証とユーザ認証

ステップ1:Windows PCからのサインアウト

Win10 PC1からSign outボタンをクリックして、マシン認証をトリガーします。



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

ステップ3: Windows PCへのログイン

Win10 PC1にログインし、ユーザ認証をトリガーするためのユーザ名とパスワードを入力します。



Windows PCへのログイン

ステップ4:認証セッションの確認

show authentication sessions interface GigabitEthernet1/0/2 detailsコマンドを実行して、C1000でのユーザ認証セッションを確認します。

<#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

ステップ5:Radiusライブログの確認

ISE GUIで、Operations > RADIUS > Live Logsの順に移動し、マシン認証とユーザ認証のライブログを確認します。

≡	dentity Services I	Engine					Operations /	RADIUS				A Evaluation Mode	∎aya Q (۵ ۵	۵	A
н	Bookmarks	Live Lo	gs Live Sessions													
	Dashboard															
명	Context Visibility	Mit	configured Supplicants 🕕			Mis	configured Network Devices 🕕		RADIUS Drops		Client Stopped Responding			Repeat	Counter	0
*	Operations		0				0		0		0				0	
U	Policy										Defeath	Show		Webin		
2.	Administration										Never	✓ Latest	20 records 🧹	Last 3 h	lours	×
đ	Work Centers	e	E Reset Repeat Counts	\oplus Export To \vee										Filter >	< •	
			Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P	IP Address	Neta	ork De	
(?)	Interactive Help)	<	~			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	v Netw	ork Devic	£
			May 07, 2024 04:36:14	•	0	0	AD/sestuser	B4:96:91:15:84:	Intel-Devi	$MAR_Test \Rightarrow MAR_dot1x$	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess	1.1 3.9			
			May 07, 2024 04:36:13	8	ē.		ADitestuser	B4.96.91.15.84	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \Rightarrow User_MAR_Passed$	PermitAccess	1.1 0.9	C100	0	
			May 07, 2024 04:35:12	2	ò		#ACSACL#-IP-MAR_Passed-6639ba20							C100	5	
			May 07, 2024 04:35:12	2	0		host/DESKTOP-L2IL9I6.ad.rem-s_ithm	B4:96:91:15:84:	Intel-Devi	$MAR_Test \Rightarrow MAR_dot1x$	$MAR_Test \gg MAR_Pessed$	MAR_Passed	169.254.90.1	C100	5	

Radiusライブログ

マシン認証の詳細なライブログを確認します。

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 6 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 0 Extracted EAP-Response/NAK requesting to use PEAP 12301 0 instead 12300 Prepared EAP-Request proposing PEAP with challenge 0 12625 Valid EAP-Key-Name attribute received 0 Returned RADIUS Access-Challenge 0 11006 11001 Received RADIUS Access-Request 5 11018 RADIUS is re-using an existing session 0 Extracted EAP-Response containing PEAP challenge-12302 1 response and accepting PEAP as negotiated 61025 1 Open secure connection with TLS peer 12318 Successfully negotiated PEAP version 0 0 12800 Extracted first TLS record; TLS handshake started 0 0 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 0 12807 Prepared TLS Certificate message 0 12808 Prepared TLS ServerKeyExchange message 25 12810 Prepared TLS ServerDone message 0 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

マシン認証の詳細

ユーザ認証の詳細なライブログを確認します。

Cisco ISE

Overview			Steps		
Event	5200 Authentication succeeded		Step ID	Description	Latency (ms)
			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
		1	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
		1	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
			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	1.1 . 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
Authentication Drotocol	DEAD (EAD MCCHAD		11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPVZ)		12304	Extracted EAP-Response containing PEAP challenge-	0

ユーザ認証の詳細

パターン2ユーザ認証のみ

ステップ1: Windows PCのNICを無効および有効にする

ユーザ認証をトリガーするには、Win10 PC1のNICを無効および有効にします。

ステップ2:認証セッションの確認

show authentication sessions interface GigabitEthernet1/0/2 detailsコマンドを実行して、C1000でのユーザ認証セッションを確認します

0

<#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

ステップ3:Radiusライブログの確認

ISE GUIで、Operations > RADIUS > Live Logsの順に移動し、ユーザ認証のライブログを確認します。



注:MARキャッシュはISEに保存されるため、必要なのはユーザ認証だけです。

$\equiv \frac{1}{1000}$ Identity Services	Engine		Operations	/ RADIUS			🛦 Crahadian Made 🗖 Days 🔍 (0 0 0 A
JI Bookmarks	Live Logs Live Sessions							
E Dashboard								
1d Context Visibility	Misconfigured Supplicants	M	configured Network Devices 🔘	RAI	DIUS Drops 🕕	Client Stopped Responding		Repeat Counter 🕕
😤 Operations	0		0		0	0		0
Policy						Refresh Never	Show Latest 20 records	Within Last 3 hours
Administration	🖉 🖆 Reset Repeat Counts	\oplus Export To \lor						Filter V 0
	Time	Status Details Repea	Identity	Endpoint ID E	Indpoint Authentication Policy	Authorization Policy	Authorization P IP Address	Network De
(2) Interactive Help	×	v	Identity	Endpoint ID E	Endpoint Pr Authentication Policy	Authorization Policy	Authorization Profi IP Address	V Network Devic
0	May 07, 2024 04:42:05	• à •	AD/pestuser	84:96:91:15:84: In	ntel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1.1.1.9	
	May 07, 2024 04:42:04	- B 3	AD/pestuser	84:96:91:15:84: In	ntel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1	C1000
	May 07, 2024 04:36:13	- D 3	AD/destuser	84:96:91:15:84: In	ntel-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 3	host/DESKTOP-L2IL9I6.ad.rem-s 1.am	84:96:91:15:84: In	ntel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed 169.254.90.1	C1000

ユーザ認証の詳細なライブログを確認します。

Cisco ISE

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (r
LYCIN	5265 Admenterior Secreted	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
chapoint Prome	inter-benee	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
auton court	1 chimesecou	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
could innovanip	NAME OF A DESCRIPTION	12625	Valid EAP-Key-Name attribute received	0
Received Timestamp	2024-05-07 16:42:04.467	11006	Returned RADIUS Access-Challenge	0
olicy Server	ise33-01	11001	Received RADIUS Access-Request	25
vent	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
Jsername	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
indopint Id	R4-96-91-15-84-CR	61025	Open secure connection with TLS peer	0
	04100101110104100	12318	Successfully negotiated PEAP version 0	0
alling Station Id	B4-96-91-15-84-CB	12800	Extracted first TLS record; TLS handshake started	0
indpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
PvA Address	117:39	12806	Prepared TLS ServerHello message	0
14 14041000		12807	Prepared TLS Certificate message	0
Authentication Identity Store	AD_Join_Point	12808	Prepared TLS ServerKeyExchange message	26
		12810	Prepared TLS ServerDone message	0
dentity Group	Profiled	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
		11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPv2) Framed	12304	Extracted EAP-Response containing PEAP challenge- response	1
		12305	Prepared EAP-Request with another PEAP challenge	0
Network Device	C1000 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
	17/9	24432	Looking up user in Active Directory - AD\testuser	
D-Groups-Names	ad.rem-sv: m.com/Builtin/Users	24355	LDAP fetch succeeded	
		24416	User's Groups retrieval from Active Directory succeeded	
D-Groups-Names	ad.rem-sym.com/Builtin/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
D-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
D-Groups-Names	ad.rem-sjinte.in.com/Users/Domain Admins	22080	New accounting session created in Session cache	0
D-Groups-Names	ad.rem-sylfim.com/Users/Domain Users	12306	PEAP authentication succeeded	0
		61026	Shutdown secure connection with TLS peer	0
		11503	Prepared EAP-Success	1
esult		11002	Returned RADIUS Access-Accept	2

ユーザ認証の詳細

トラブルシュート

次のデバッグログ(prrt-server.log)は、ISEでの認証の詳細な動作を確認するのに役立ちます。

ランタイム設定

- ランタイムロギング
- ランタイムAAA

次に、パターン1のデバッグログの例を示します。このドキュメントの「マシン認証とユーザ認証」。

<#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,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

関連情報

マシンアクセス制限の長所と短所

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。