Machine tweefactorverificatie configureren voor toegang door aanvrager

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Netwerkdiagram
Achtergrondinformatie
Configuraties
Configuratie in C1000
Configuratie in Windows-pc
Stap 1. PC toevoegen aan AD-domein
Stap 2. Gebruikersverificatie configureren
Configuratie in Windows-server
Stap 1. Domeincomputers bevestigen
Stap 2. Domeingebruiker toevoegen
Configuratie in ISE
Stap 1. Apparaat toevoegen
Stap 2. Actieve map toevoegen
Stap 3. Instellingen voor machineverificatie bevestigen
Stap 4. Identity Source Sequences toevoegen
Stap 5. DACL-profiel en autorisatieprofiel toevoegen
Stap 6. Beleidsset toevoegen
Stap 7. Verificatiebeleid toevoegen
Stap 8. Toepassingsbeleid toevoegen
Verifiëren
Patroon 1. Machine-verificatie en gebruikersverificatie
Stap 1. Uitloggen op Windows-pc
Stap 2. Verificatiesessie bevestigen
<u>Stap 3. Aanmelden bij Windows-pc</u>
Stap 4. Verificatiesessie bevestigen
Stap 5. Radius live log bevestigen
Patroon 2. Alleen gebruikersverificatie
Stap 1. NIC van Windows-pc uitschakelen en inschakelen
Stap 2. Verificatiesessie bevestigen
Stap 3. Radius live log bevestigen
Problemen oplossen
Gerelateerde informatie

Inleiding

Dit document beschrijft de stappen die nodig zijn om Twee-Factor-verificatie te configureren met machine- en dot1x-verificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco Identity Services Engine
- Configuratie van Cisco Catalyst
- IEEE 802.1X

Gebruikte componenten

- Identity Services Engine virtuele 3.3-patch 1
- C100-48FP-4G-L 15.2(7)E9 switch
- Windows Server 2019

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.

De domeinnaam ingesteld op Windows Server 2019 is ad.rem-xxx.com, die wordt gebruikt als voorbeeld in dit document.



Netwerkdiagram

Achtergrondinformatie

Machineverificatie is een beveiligingsproces dat de identiteit verifieert van een apparaat dat toegang zoekt tot een netwerk of systeem. In tegenstelling tot gebruikersverificatie, die de identiteit van een persoon verifieert op basis van referenties zoals een gebruikersnaam en wachtwoord, concentreert de machine-verificatie zich op het valideren van het apparaat zelf. Dit gebeurt vaak met behulp van digitale certificaten of beveiligingssleutels die uniek zijn voor het apparaat.

Door machine- en gebruikersverificatie samen te gebruiken, kan een organisatie ervoor zorgen dat alleen bevoegde apparaten en gebruikers toegang hebben tot haar netwerk, waardoor een veiligere omgeving wordt gecreëerd. Deze tweeledige verificatiemethode is bijzonder nuttig voor het beschermen van gevoelige informatie en het voldoen aan strikte regulerende normen.

Configuraties

Configuratie in C1000

Dit is de minimale configuratie in 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

Configuratie in Windows-pc

Stap 1. PC toevoegen aan AD-domein

Navigeer naar Configuratiescherm > Systeem en beveiliging, klik op Systeem en klik vervolgens op Geavanceerde systeeminstellingen. Klik in het venster Systeemeigenschappen op Wijzigen, selecteer Domein en voer de domeinnaam in.



PC toevoegen aan AD-domein

Voer in het venster Windows Beveiliging de gebruikersnaam en het wachtwoord van de domeinserver in.



Gebruikersnaam en wachtwoord invoeren

Stap 2. Gebruikersverificatie configureren

Navigeer naar verificatie en controleer IEEE 802.1X-verificatie inschakelen. Klik op Instellingen in het venster met beschermde EAP-eigenschappen, uncheck Controleer de identiteit van de server door het certificaat te valideren en klik vervolgens op Configureren. Selecteer in het venster EAP MSCHAPv2 Properties de optie Automatisch mijn Windows-aanmeldingsnaam en -wachtwoord (en eventueel een domein) om de gebruikersnaam te gebruiken die is ingevoerd tijdens de aanmelding bij de Windows-machine voor gebruikersverificatie.



Gebruikersverificatie inschakelen

Navigeer naar Verificatie en controleer Extra instellingen. Selecteer Gebruiker- of computerverificatie in de vervolgkeuzelijst.

🖗 pciPassthru0 Properties 🛛 🕹	Advanced settings ×
Networkin; Authentication	802.1X settings
Select this option to provide authenticated network access for this Ethemet adapter.	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users
Microsoft: Protected EAP (PEAP) Settings	Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon
 ☐ Remember my credentials for this connection each time I'm logged on ☑ Fallback to unauthorized network access Additional Settings 	Maximum delay (seconds): 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

Verificatiemodus opgeven

Configuratie in Windows-server

Stap 1. Domeincomputers bevestigen

Navigeer naar Active Directory-gebruikers en -computers, klik op Computers. Bevestig dat Win10 PC1 in het domein wordt vermeld.



Domain Computer bevestigen

Stap 2. Domeingebruiker toevoegen

Navigeer naar Active Directory-gebruikers en -computers, klik op Gebruikers. Voeg testuser toe als domeingebruiker.

Active Directory Users and Computers									
File Action View Help									
◆ → 2 📷 4 C 🗙 🖬 2 🖬 3	🎗 🗊 🍸 🚨 🐍								
Active Directory Users and Computers [winserver.ad.rem-p	Name	Type		Description					
Computers Computers Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts	Administrator Allowed RODC Password Replication Group Coneable Domain Controllers Coneable Domain Controllers DefailtAccount Denied RODC Password Replication Group DisAdmins	User Built-in account for admini Security Group - Domain Local Members of this group can Security Group - Global Members of this group tar Security Group - Global A user account managed by Security Group - Domain Local DNS Administrators Group				ninistering can have t are permit that are do d by the s cannot has wp	the computer heir passwords ted to publish- imain controlli ystem. ve their passwo	/domain replicated to certificates to ers may be cl ords replicate	
	B DnsUpdateProxy S Domain Admins S	Security Group - Global Security Group - Global	test user	DNS clients Properties	clients who are permitted to perform dynamic updat rties ?				
	Domain Controllers Domain Controllers Domain Guests Domain Users Enterprise Admins Enterprise Read-only Domain Controllers	Security Group - Grobal Security Group - Global Security Group - Global Security Group - Global Security Group - Universal Security Group - Universal	Men Renc General	Member Of Dalin Environment Remote control Remote Desistop Services Profile General Address Account Profile Telephones best user					
	Group Policy Creator Owners Guett Key Admins ndes_user Protected Users RAS and IAS Servers Read-only Domain Controllers	Security Group - Global User Security Group - Global User Security Group - Global Security Group - Domain I Security Group - Global	Brit name: Last name: Digsky name: Description:		user Jest user		htain:		
	總 Schema Admins 名 test user	Security Group - Universal User							

Domeingebruiker toevoegen

Voeg de domeingebruiker toe aan lid van Domain Admins en Domain Gebruikers.

				? ×	test user Properties				?	>
Member Of Dial-in Environment			Sessions	Remote control	Remote	Desktop Se	rvices Profile	CO	M+	
Remote control	Remote 0	Remote Desktop Services Profile		COM+	General Address	Account	Profile	Telephones	Organi	zatio
General Address	Account	Profile Tel	ephones	Organization	Member Of	Dial-in	Envi	ronment	Sessio	ns
User logon name:					Member of:					
testuser		@ad.rem-s,s	m.com	~	Name	Active Direct	tory Domain	Services Folder	r	
User logon name (pre	-Windows 200	0):			Domain Admins	ad rem-syllin	m.com/Use	rs 🛛		
AD\	_	testuser			Domain Users	ad.rem-sy"L.r	m.com/Use	rs 🛛		
Account gations:		t and lance		^						
Account getons:	nge password a ange password r expires I using revensib	t next logon d le encryption		< ×	Add I Primary group: D	gemove omain Users	to pead to c	hanne Primary		
User must char User cannot ch Password neve Store password Account expires Never End of:	nge password a ange password r expires I using reversib Thursday ,	t next logon d le encryption June 6, 20	124	×	Add I Primary group: D Set Primary Group	Gemove omain Users There is r you have applicatio	no need to o Macintosh ns.	change Primary (clients or POSD	group unk	ess

Domain Admins en domeingebruikers

Configuratie in ISE

Stap 1. Apparaat toevoegen

Navigeer naar Beheer > Netwerkapparaten en klik op de knop Toevoegen om C1000-apparaat toe te voegen.

≡	alada Identity Services E	Ingine		Administration / Network Resources						
Щ	Bookmarks	Network Devices	Network Device	e Groups N	letwork Device Profiles	External RADIUS	Servers	RADIUS Server Sequences	NAC Managers	
-	Dashboard	Network Devices		Network Devices Li	st > C1000					
1 ¹ 0	Context Visibility	Default Device Device Security Setting	15	Network Devi	ces					
*	Operations			Name	C1000					
0	Policy			Description						
20	Administration			Coorpiton						
nii:	Work Centers			IP Address		/ 22 👼				
						ол ф				
Ŷ	Interactive Help			Device Profile	🏥 Cisco	× 0				
				Model Name		~				
				model Name						
				Software Versio	n	~				
				Network Device	Group					
				Location	All Locations	~	Set To Defai	ult		
				IPSEC	No	~	Set To Defai	ult		
				Device Type	All Device Types	~	Set To Defai	ult		
				🗹 🗸 RAD	IUS Authentication Settir	igs				
				RADIUS	UDP Settings					
				Protocol	RADIUS					
				Shared S	ecret cisco123		Hide			

Apparaat toevoegen

Stap 2. Actieve map toevoegen

Navigeer naar Beheer > Externe Identiteitsbronnen > Active Directory, klik op tabblad Connection en voeg Active Directory toe aan ISE.

- Lid worden Naam: AD_Join_Point
- Active Directory-domein: ad.rem-xxx.com

	dials Identity Services I	gine Administration / identity Management
Щ	Bookmarks	dentities Groups External Identity Sources Identity Source Sequences Settings
53	Dashboard	
망	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat Join Point Name AD_Join_Point
-0	Policy	Active Directory
20	Administration	AD_Join_Point

Navigeer naar het tabblad Groepen en selecteer Groepen uit map uit vervolgkeuzelijst.

≡	dentity Services E	Engine Administration / Identity Mana	gement
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings	
	Dashboard		
망	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Adv	anced Settings
*	Operations	Continue of the second se	
0	Policy	Select Groups From Directory Select Groups From Directory SID	
80	Administration	AD_Join_Point Add Group Control Assist ad.rem-sy am.com/	-1-5-32-579

Groepen uit map selecteren

Klik op Groepen ophalen uit vervolgkeuzelijst. Controleer ad.rem-xxx.com/Users/Domain Computers en ad.rem-xxx.com/Users/Domain Gebruikers en klik op OK.

				~	
	Backmarks	Identities Groups E	Select Directory Groups		
	Dashinard) L/ Certinicate Al	This dialog is used to select groups from the Directory.		
		- C Active Directe	Domain adven-e r m.com		
14	Context Visibility	T AD_Join_Poin	Name SD Type ALL		
~~	Operations	C) LOAP	[Barden Course] A Course Patrice of		
0	Policy	C coec		. 1	
2.	Administration	C REA Securit	Name		
2	Work Centers	C SAME M Provide	advenus; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	•	
		C Social Login	ad rem-sy tem com/overs/DimopdateProxy 5-1-5-21-41103122415-4133120028-20482399. 0L0844		
			adven-ay**en.com/Users/Domain Admine 5+1-5-21-4113142415-4133120024-20482209 GLOBAL		
	Interactive Help		ad rem-sy, L.m.com/Users/Domain Computers 5+1-5-21-4150742415-4130520026-20462099 6L084L		
			adventi, st. n. controlets/Domain Controllets 5+1-0-21-4132132415-4132322028-20412298. 0L0844		
			adven-s, iron.com/bars/bars/bars/bars/ 5-1-5-21-4110/N2415-413052024-204822986L084L		
			advenires, Um.com/Veens/Domain Veens 5+1-5-21+4193742415+4133520028+20442399 GL0844		
			adven-e; / m.con/Week/Decores Advess 5-1-5-21-6132742415-413352028-2042239. UNVDRAL		
			ad rem-ey it im.com/Uners/Emergina Key Admini 5+1-5-21+6110742415-413052028-20482299 UNIVERSAL		
			advenus, stim.com/livers/Drocurise Readvery		
			adven-sy, am.com/tees/deep Petry Ceansr 5-1-5-21-6132742415-413252028-2042299 0L0844		
				1	
			Cancel	•	

Domeincomputers en -gebruikers toevoegen

Stap 3. Instellingen voor machineverificatie bevestigen

Navigeer naar het tabblad Geavanceerde instellingen en bevestig de instelling van de verificatie van de machine.

- · Machine-verificatie inschakelen: automatische verificatie inschakelen
- Beperking machinetoegang inschakelen: gebruikers- en machineverificatie combineren vóór autorisatie



Opmerking: Het geldige bereik van de verouderingstijd is 1 tot 8760.



Stap 4. Identity Source Sequences toevoegen

Ga naar Beheer > Identity Source Sequences en voeg een Identity Source Sequence toe.

- Naam: Identity_AD
- Verificatie Zoeklijst: AD_Join_Point

≡	diada Identity Services I	Engine		Administration / Io	dentity Management
Щ	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
- 55	Dashboard	Identity Source Sequence	es List > Identity_AD		
15	Context Visibility	Identity Source S	equence		
*	Operations				
-0	Policy	 Identity Source Name 	e Sequence		
80	Administration	Description	dentity_AD		
-fli	Work Centers	Description			
?	Interactive Help	✓ Certificate B □ Select Certifi	ased Authentication	~	
		 Authentication A set of ide 	on Search List ntity sources that will be accessed i	n sequence until first authentication s	Rucceeds
		Available	3	Selected	
		Internal	Endpoints	AD_Join_Point	
		Internal	Users		
		All_AD	Join_Points		
			》 《		∑ ∑
Iden	tity Source Sequence	es toevoegen			

Stap 5. DACL-profiel en autorisatieprofiel toevoegen

Navigeer naar Beleid > Resultaten > Autorisatie > Downloadbare ACL's, voeg een DACL toe.

- Naam: MAR_Passed
- DACL-inhoud: laat ip elke host 1.x.x.101 toe en laat ip elke host 1.x.x.105 toe

≡	dentity Services E	Engine	Policy / Policy Elements	
Ш.	Bookmarks	Dictionaries Conditions	Results	
	Dashboard	Authentication	Downloadable ACL List > MAR_Passed	
15	Context Visibility	Authorization	Downloadable ACL	
- %	Operations	Authorization Profiles	* Namo MAR Decent	
0	Policy	Downloadable ACLs	Description	
80	Administration	Profiling		
ส้น	Work Centers	Posture	* DACL Content 1234567 permit ip any host 1.[1].0.101	
		Client Provisioning	233415 1417181	

DACL toevoegen

Navigeer naar Beleid > Resultaten > Autorisatie > Autorisatieprofielen en voeg een autorisatieprofiel toe.

- Naam: MAR_Passed
- DACL-naam: MAR_Passed

≡	abala Identity Services E	ingine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	R	sults	
	Dashboard	Authentication	>	Authorization Profiles > MAR_Pase	sed
18	Context Visibility Operations	Authorization Authorization Profiles	~	Authorization Profile	
0	Policy	Downloadable ACLs		Description	AR_Passed
80	Administration	Profiling	>		
-file	Work Centers	Posture	>	Access Type	ACCESS_ACCEPT V
(?)	Interactive Help	Client Provisioning	>	Network Device Profile the format in the fo	
				✓ Common Tasks	
				DACL Name	MAR_Passed ~
Verg	gunningsprofiel t	oevoegen			

Stap 6. Beleidsset toevoegen

Navigeer naar Policy > Policy Sets, klik op + om een policy set toe te voegen.

- Naam van de beleidsreeks: MAR_Test
- Voorwaarden: Wired_802.1x
- Toegestane protocollen/serverreeks: standaard netwerktoegang

=	dentity Services En	gine Policy / Policy Sets		A type	ion Mode 8	9 Days (۵ ۵	0	0	۹
Л	Bookmarks	Policy Sets		R Click h	ere to do v	isibility se	tup Do r	ot show t	his agair	×
	Dashboard	 Status Policy Set Name Description Conditions 	Allow	ed Protocol	s / Server	Sequence	Hits	Actions	View	
N	Context Visibility	Q, Search								
*	Operations	MAR_Text Wined_802.1X	Defa	it Network J	lecess	× +	15	٢	•	
8.	Administration	Default Default policy set	Detai	it Network i	locess	<u>×</u> +	۰	ø	>	
ก็	Work Centers									
							Reset		Save	

Beleidsset toevoegen

Stap 7. Verificatiebeleid toevoegen

Navigeer naar Policy Sets, klik op MAR_Test om een verificatiebeleid toe te voegen.

- Regel Naam: MAR_dot1x
- Voorwaarden: Wired_802.1x
- Gebruik: Identity_AD

~	Authe	entication	n Policy(2)				
	⊙	Status	Rule Name	Conditions	Use	Hits	Actions
	Q	Search	h				
		0	MAR_dot1x	E Wind_802.1X	Identity_AD /		¢
		0	Default		All_User_ID_Stores / > Options	0	@

Verificatiebeleid toevoegen

Stap 8. Toepassingsbeleid toevoegen

Navigeren naar Policy Sets, klik op MAR_Test om een autorisatiebeleid toe te voegen.

- Regel Naam: MAR_Passed
- Voorwaarden: AD_Join_Point·ExterneGroepen EQUALS ad.rem-xxx.com/Users/Domain Computers EN Network_Access_Verification_Passed
- Resultaten: MAR_Passed
- Regel Naam: Gebruiker_MAR_Passed
- Voorwaarden: Network Access·WasMachineAuthenticated EQUALS True en AD_Join_Point·ExterneGroepen GELIJKT ad.rem-xxx.com/Users/Domain Gebruikers
- Resultaten: PermitAccess

VAuthorization Policy(3)					
🕣 Status Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
Q Search MAR_Passed	AND R AD_Join_Point ExternalGroups EQUALS ad.rem-sp : im.com/Users/Domain Computers Workinds_Access_Authentication_Passed	MAR_Passed	+ Select from list	1	\$
User_MAR_Passed	AND L Network Access WasMachineAuthenticated EQUALS True R AD_Join_PointExternalGroups EQUALS ad.rem-sy _m.com/Users/Domain Users	PermitAccess	+ Śelect from list 🥒 +	1	ø
O Default		DenyAccess /	+ Select from list 🥒 +	9	٨

Toepassingsbeleid toevoegen

Verifiëren

Patroon 1. Machine-verificatie en gebruikersverificatie

Stap 1. Uitloggen op Windows-pc

Klik op de knop Uitloggen vanaf Win10 PC1 om de machine-verificatie te activeren.



Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:

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

Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 5s Common Session ID: 01C2006500000049AA780D80 Acct Session ID: 0x000003C Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2

Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies: ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list: Method State

dot1x Authc Success

Stap 3. Aanmelden bij Windows-pc

Login Win10 PC1, voer gebruikersnaam en wachtwoord in om gebruikersverificatie te activeren.



Aanmelden bij Windows-pc

Stap 4. Verificatiesessie bevestigen

show authentication sessions interface GigabitEthernet1/0/2 details Voer de opdracht uit om de gebruikersverificatiesessie in C1000 te bevestigen.

<#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: 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 status list:
Method State
dot1x Authc Success
```

Stap 5. Radius live log bevestigen

Navigeer naar **Operations** > **RADIUS** > **Live logs** in ISE GUI, bevestig het bewegende logbestand voor machine-verificatie en gebruikersverificatie.

=	dentity Services	Engine					Operations /	RADIUS				A Evaluation Mode	Q 6	00	A
Щ	Bookmarks	Live Log	s Live Sessions												
51	Dashboard														
15	Context Visibility	Mise	onfigured Supplicants 📀			Mis	configured Network Devices 🕕		RADIUS Drops	0	Client Stopped Responding	10		Repeat Count	ter 🕜
*	Operations		0				0		0		0			0	
U	Policy										Refresh	Show	20 records	Within	
2.0 Ali	Administration Work Centers	ø	1 Reset Repeat Counts	් Export To 🗸										Filter V	•
			Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network D	e
(?)	Interactive Help	×		~			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	Network De	vic
			May 07, 2024 04:36:14	٠	0	0	ADitestuser	84:96:91:15:84:	Intel-Devi	$MAR_Test \Rightarrow MAR_dot1x$	$MAR_Test \mapsto User_MAR_Pessed$	PermitAccess	1.1 2.9		
			May 07, 2024 04:36:13		0		ADitestuser	84.96.91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 2.9	C1000	
			May 07, 2024 04:35:12	2	à		#ACSACL#-IP-MAR_Passed-6639ba20							C1000	
			May 07, 2024 04:35:12	2	ò		host/DESKTOP-L2IL9I6.ad.rem-s_rhm	B4:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \Rightarrow MAR_Passed$	MAR_Passed	169.254.90.1	C1000	

Radius live log

Bevestig het gedetailleerde bewegende logbestand voor machinale authenticatie.

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_finm.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

Gedetailleerde beschrijving van de machineverificatie

Bevestig het gedetailleerde live logbestand van gebruikersverificatie.

Cisco ISE

	Overview		Steps		
	Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
ł	Lion	SZOV Addicition Successo	11001	Received RADIUS Access-Request - AD_Join_Point	
	Username	AD\testuser	11017	RADIUS created a new session - ad.rem-sy .em.com	0
	Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	0
	Endpoint Profile	Intel-Device	15008	Evaluating Service Selection Policy	1
ł	Endpoint Frome		11507	Extracted EAP-Response/Identity	7
	Authentication Policy	MAR_Test >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
	Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
	Authorization Result	PermitAccess	11006	Returned RADIUS Access-Challenge	0
ļ	Autorization Resourc	1 011110100000	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
	Source milestamp	2024-05-07 10.50.15.746	12625	Valid EAP-Key-Name attribute received	0
	Received Timestamp	2024-05-07 16:36:13.748	11006	Returned RADIUS Access-Challenge	0
	Policy Server	ise33-01	11001	Received RADIUS Access-Request	11
	Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
	Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	0
	Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
	Lindpoint id	54100101110104100	12318	Successfully negotiated PEAP version 0	1
	Calling Station Id	B4-96-91-15-84-CB	12800	Extracted first TLS record; TLS handshake started	0
	Endpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
	IPv4 Address	1.11.2.9	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

Details van gebruikersverificatie

Patroon 2. Alleen gebruikersverificatie

Stap 1. NIC van Windows-pc uitschakelen en inschakelen

Om gebruikersverificatie te activeren, schakelt u de NIC van Win10 PC1 uit en schakelt u deze in.

Stap 2. Verificatiesessie bevestigen

show authentication sessions interface GigabitEthernet1/0/2 details Voer de opdracht uit om de gebruikersverificatiesessie in C1000 te bevestigen.

<#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

Stap 3. Radius live log bevestigen

Navigeer naar Operations > RADIUS > Live logs in ISE GUI en bevestig het live log voor gebruikersverificatie.



Opmerking: omdat de MAR cache is opgeslagen in ISE, is alleen gebruikersverificatie nodig.

≡ dealer Identity Service	rs Engine	or of the second s	perations / RADIUS	La Evaluation Mode	Q & O P
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 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

Radius live log

Bevestig het gedetailleerde live logbestand van gebruikersverificatie.

Cisco ISE				
Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (r
		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
Authentication Delicu	MAD Tool on MAD doubs	11507	Extracted EAP-Response/Identity	16
Authentication Policy	MAR_TOST >> MAR_OUTX	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 Timestamo	2024-05-07 16:42:04 467	12625	Valid EAP-Key-Name attribute received	0
nossing initiating	NAME AND A DESCRIPTION	11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01	11001	Received RADIUS Access-Request	25
Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
Calling Station Id	D4-06-01-15-04-CD	12318	Successfully negotiated PEAP version 0	0
Gailing Station id	D4-30-31-12-04-0D	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
		12305	Prepared EAP-Request with another PEAP challenge	0
Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
Authentication Method	dot1x	11001	Received RADIUS Access-Request	14
Authentication Protocol	PEAP (EAP-MSCHAPv2)	11018	RADIUS is re-using an existing session	0
		12304	response	1
Service Type	Framed	 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, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2af92	24211	Found Endpoint in Internal Endpoints IDStore	3
	17/9	24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad.rem-sy: m.com/Builtin/Users	24355	LDAP fetch succeeded	
and a post of the second s		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
	Replication Group	22081	Max sessions policy passed	0
AD-Groups-Names	ad.rem-synte.n.com/Users/Domain Admins	22080	New accounting session created in Session cache	0
AD-Groups-Names	ad.rem-symm.com/Users/Domain Users	12306	PEAP authentication succeeded	0
		61026	Shutdown secure connection with TLS peer	0
		11503	Prepared EAP-Success	1
		11002	Returned RADIUS Access-Accept	2

Details van gebruikersverificatie

Problemen oplossen

Deze debug logbestanden (poortserver.log) helpen u het gedetailleerde gedrag van verificatie in ISE te bevestigen.

• tijdens uitvoering configureren

- runtime-vastlegging
- runtime-AAA

Dit is een voorbeeld van het debug log voor Patroon 1. Machine-verificatie en gebruikersverificatie in dit document.

<#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

Gerelateerde informatie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.