신청자 액세스에 대한 시스템 2단계 인증 구성

목차 <u>소개</u> <u>사전 요구 사항</u> 요구 사항 <u>사용되는 구성 요소</u> 네트워크 다이어그램 배경 정보 설정 <u>C1000의 컨피그레이션</u> <u>Windows PC의 구성</u> <u>1단계. AD 도메인에 PC 추가</u> <u>2단계. 사용자 인증 구성</u> Windows Server의 구성 1단계. 도메인 컴퓨터 확인 <u>2단계. 도메인 사용자 추가</u> ISE의 컨피그레이션 <u>1단계. 장치 추가</u> <u>2단계. Active Directory 추가</u> 3단계. 머신 인증 설정 확인 <u>4단계. ID 소스 시퀀스 추가</u> <u>5단계. DACL 및 권한 부여 프로파일 추가</u> 6단계. 정책 집합 추가 7단계. 인증 정책 추가 8단계. 권한 부여 정책 추가 다음을 확인합니다. 패턴 1. 머신 인증 및 사용자 인증 <u>1단계. Windows PC 로그아웃</u> <u>2단계. 인증 세션 확인</u> <u>3단계. Windows PC 로그인</u> 4단계. 인증 세션 확인 <u>5단계. Radius 라이브 로그 확인</u> <u>패턴 2. 사용자 인증만</u> <u>1단계. Windows PC의 NIC 비활성화 및 활성화</u> <u>2단계. 인증 세션 확인</u> <u>3단계. Radius 라이브 로그 확인</u> <u>문제 해결</u> 관련 정보

소개

이 문서에서는 머신 및 dot1x 인증을 사용하여 2단계 인증을 구성하는 데 필요한 단계를 설명합니 다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Services Engine 구성
- Cisco Catalyst 구성
- IEEE802.1X

사용되는 구성 요소

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 그림에서는 이 문서의 예에 사용된 토폴로지를 보여줍니다.

Windows Server 2019에 구성된 도메인 이름은 ad.rem-xxx.com이며 이 문서의 예제로 사용됩니다.



배경 정보

머신 인증은 네트워크 또는 시스템에 액세스하려는 디바이스의 ID를 확인하는 보안 프로세스입니 다. 사용자 이름 및 비밀번호와 같은 자격 증명을 기반으로 사람의 ID를 확인하는 사용자 인증과 달 리 머신 인증은 디바이스 자체의 유효성을 검사하는 데 중점을 둡니다. 이는 종종 디바이스에 고유 한 디지털 인증서 또는 보안 키를 사용하여 수행됩니다.

조직은 머신 및 사용자 인증을 함께 사용하여 승인된 디바이스와 사용자만 네트워크에 액세스할 수 있도록 함으로써 보다 안전한 환경을 제공할 수 있습니다. 이 2단계 인증 방식은 민감한 정보를 보 호하고 엄격한 규제 표준을 준수하는 데 특히 유용합니다.

설정

C1000의 컨피그레이션

이는 C1000 CLI의 최소 컨피그레이션입니다.

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 PC의 구성

1단계. AD 도메인에 PC 추가

Control Panel(제어판) > System and Security(시스템 및 보안)로 이동하고 System(시스템)을 클릭 한 다음 Advanced system settings(고급 시스템 설정)를 클릭합니다. System Properties(시스템 속 성) 창에서 Change(변경)를 클릭하고 Domain(도메인)을 선택한 다음 도메인 이름을 입력합니다.



```
AD 도메인에 PC 추가
```

Windows 보안 창에서 도메인 서버의 사용자 이름과 암호를 입력합니다.



사용자 이름 및 비밀번호 입력

2단계. 사용자 인증 구성

Authentication(인증)으로 이동하고 Enable IEEE 802.1X authentication(IEEE 802.1X 인증 활성화)을 선택합니다. Protected EAP Properties(보호된 EAP 속성) 창에서 Settings(설정)를 클릭하고 Verify the server's identity by validating the certificate(인증서를 검증하여 서버 ID 확인)의 선택을 취소한 다음 Configure(구성)를 클릭합니다. EAP MSCHAPv2 Properties(EAP MSCHAPv2 속성) 창에서 Automatically use my Windows logon name and password (and if any if any)(내 Windows 로그온 이름 및 암호(있는 경우 도메인)를 선택하여 사용자 인증을 위해 Windows 머신 로그인 중에 입력한 사용자 이름을 사용합니다.

pciPassthru0 Properties X	Protected EAP Properties ×	EAP MSCHAPv2 Properties X
Networking Authentication	When connecting:	When connecting:
this Ethernet adapter.	Connect to these servers (examples:srv1;srv2;.**,srv3),com):	OK Cancel
Choose a network authentication method: Microsoft: Protected EAP (PEAP) V Settings	AAA Certificate Services ad-WDKSERVER-CA Baltmore CyberTrust Root	
Permember my credentials for this connection each time I'm logged on Fallback to unauthorized network access	Class 3 Public Primary Certification Authority DigCert Assured ID Root CA DigICert Global Root CA DigICert Global Root G2 v	
Additional Settings	Notifications before connecting: Tell user if the server's identity can't be verified	
	Select Authentication Method: Secured password (EAP-MSCHAP v2) V Configure	
0K Canoel	Enable Fast Reconnect Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
	OK Cancel	

사용자 인증 활성화

Authentication(인증)으로 이동하고 Additional Settings(추가 설정)를 선택합니다. 드롭다운 목록에 서 사용자 또는 컴퓨터 인증을 선택합니다.

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

Windows Server의 구성

1단계. 도메인 컴퓨터 확인

Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터)로 이동하고 Computers(컴퓨터)를 클릭합니다. Win10 PC1이 도메인에 나열되는지 확인합니다.



```
도메인 컴퓨터 확인
```

2단계. 도메인 사용자 추가

Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터)로 이동하고 Users(사용 자)를 클릭합니다. testuser를 도메인 사용자로 추가합니다.

Active Directory Users and Computers						
File Action View Help						
++ 2 📷 4 🖬 🗙 🖬 2 🕞 🖬 🖏 🖏	🐱 la 🐨 🚨 🐱					
Active Directory Users and Computers [winserver.ad.rem-z	Name	Туре	Description			
Computers Computers Computers Domain Controllers Managed Service Accounts Users	Administrator Allowed RODC Password Replication Group Cert Publishers Cloneable Domain Controllers DefaultAccount Denied RODC Password Replication Group DesAdmins Domain Admins Domain Admins Domain Computers Domain Controllers Domain Guests Demain Users D	User Security Group - Domain Local Security Group - Domain Local Security Group - Global User Security Group - Domain Local Security Group - Domain Local Security Group - Domain Local Security Group - Domain Local Security Group - Global Security Group - Universal Security Group - Universal	Built-in acc al Members in A user acco al Members of A user acco al Members in DNS clients st user Properties Member Of Remote control General Address St user user	ount for administering in this group can have til f this group are permitt f this group that are do unt managed by the sy is this group cannot hav istrators Group who are permitted to s Dalen Env Remote Desktop Se Account Profile	the computer reir passwords ted to publish main controlle stern. e their passwo perform duman connect noces Profile Telephones	Idomain replicated to certificates to rs may be cl rds replicate ric sodates o ? X Sessione COM+ Organization
	Enterprise Read-only Domain Controllers Enterprise Read-only Domain Controllers Goup Policy Creator Owners Key Admins Notected Users Read-only Domain Controllers Read-only Domain Controllers Schema Admins Schema Admins	Security Group - Universal Security Group - Global User Security Group - Global User Security Group - Global Security Group - Global Security Group - Olobal Security Group - Universal User	Bist name: Last name: Digplay name: Decouption: Office:	Liter Liter] (réaix: [

```
도메인 사용자 추가
```

도메인 사용자를 Domain Admins 및 Domain Users의 구성원에 추가합니다.

				. ^	test user Properties				1	
Member Of	Dial-in	Envir	ronment	Sessions	Remote control	Remote	Desktop Se	ervices Profile	CO	M+
Remote control Re		esktop Ser	rvices Profile	COM+	General Address	Account Profile Telephones		Telephones	Organization	
Seneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Env	ironment	Sessio	ns
(ser logon name:					Member of:					
estuser		@ad.ren	n-6, 1. 3m.com	~	Name	Active Direct	tory Domain	Services Folder	r	
lser logon name (pre	Windows 200	0):			Domain Admins	ad rem-syllin	m.com/Use	ins 🛛		
AD\		testuser			Domain Users	ad.rem-sy"t.s	m.com/Use	975		
Uplock account										
Uglock account Uglock account User must chan User cannot ch Password neve Store password Account expires	ge password a ange password r expires using reversibl	t next logor I le encryption	n	*	Add E Primary group: Do	emove		ebanna Déarra		
Uglock account ccount gotions: User must chan User cannot ch Password neve Store password Account expires Never Sind of:	ge password a ange password r expires using reversibl Thursday ,	t next logor I e encryption June	n 6, 2024	×	Add E Primary group: Do Set Primary Group	emove omain Users There is r you have applicatio	no need to Macintosh ms.	change Primary (clients or POSD	group unit	ess

도메인 관리자 및 도메인 사용자

ISE의 컨피그레이션

1단계. 장치 추가

Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가) 버튼을 클릭하 여 C1000 디바이스를 추가합니다.

≡	dentity Services	Engine		Administration / Network Resources							
Щ	Bookmarks	Network Devices	Network Devic	ce Groups	Network Device Profiles	External RADIUS	Servers	RADIUS Server Sequences	NAC Managers		
11	Dashboard	Network Devices		Network Devices L	ist > C1000						
0	Context Visibility	Default Device	05	Network Devi	ices						
*	Operations	or any or an		Name	C1000						
U	Policy			Deservation	0.000						
20	Administration			Description							
nii.	Work Centers					(
				IP Address	✓ ⁺ IP ⁺ : 1.5100,101	/ 32 💿					
?	Interactive Help			Davias Profile	de Cieco	~ ~					
				Device Profile	55 USCO	· · · · ·					
				Model Name		~					
				Software Versi	on	~					
				Network Device	e Group						
				Location	All Locations	~	Set To Defau	ult			
				IPSEC	No	~	Set To Defau	ult			
				Device Type	All Device Types	~	Set To Defau	ult			
				🗹 🗸 RAE	DIUS Authentication Settin	igs					
				RADIUS	S UDP Settings						
				Protoco	RADIUS						
				Shared	Secret cisco123		Hide				

장치 추가

2단계. Active Directory 추가

Administration(관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동하여 Connection(연결) 탭을 클릭하고 Active Directory를 ISE에 추가합니다.

- 조인 지점 이름: AD_Join_Point
- Active Directory 도메인: ad.rem-xxx.com

≡	duals Identity Services	jine Administration / identity Manag	ement
Щ	Bookmarks	entities Groups External Identity Sources Identity Source Sequences Settings	
51	Dashboard		
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Adva	unced Settings
*	Operations	Certificate Authenticat Join Point Name AD_Join_Point	
0	Policy	Active Directory ad.rem-s; i	
20	Administration	AD_Join_Point	

Active Directory 추가

Groups(그룹) 탭으로 이동하고 드롭다운 목록에서 Select Groups From Directory(디렉토리에서 그 룹 선택)를 선택합니다.

	dentity Services E	Engine Administration / Identity Management
Л	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
-	Dashboard	
0 ¹	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Corrificate Authenticat
.0	Policy	Select Groups From Directory Select Groups From Directory SiD
å 0	Administration	Add Group Control Assist ad.rem-sy 2m.com/S-1-5-32-579

디렉터리에서 그룹 선택

Retrieve Groups from 드롭다운 목록을 클릭합니다. ad.rem-xxx.com/Users/Domain Computers and ad.rem-xxx.com/Users/Domain Users를 선택하고 OK를 클릭합니다.

	then the services	Engine						×	A 1
		Identifies Groups F	Sel	ect Directory	Groups				
	Bookmarks) U serences el	This di	ialog is used to select grou	ps from the Directo	ry.			
	Dashboard	Active Director	Do	main adven-s, r m.com					
	Context Visibility	AD_Join_Poin	1	lame . Filter	SID . Filter	Type ALL Filter			
~	Operations	C (549		Retrieve Groups	9 Groups Retrieved				
0	Policy	RADIUS Token	-						
10	Administration	C RSA SecuriD	0	Name advances - in condition/	C.	Group 580 5-1-5-21-4193742415-4139520026-20462398	Group Type DOMAN LOCAL		
12	Work Centers	SAML IS Provide	0	adven-ay ten.com/theraft	Instandante Provy	5-1-5-21-4133742415-4133520528-20442399	GLOBAL	-	
		C Social Login	0	ad rem-ay "em.com/Users/E	Iomain Admina	5-1-5-21-4193742415-4133520824-20492399	GLOBAL		
	Interactive Help			adven-sy.1.m.com/Gara/	Iomain Computers	5-1-5-21-4193742415-4133920126-20462399	610845		
			0	adven-c.st.m.con/Users/C	Iomain Controllers	5-1-5-21-4193742415-4133520526-20492399	010846		
			0	adven-a, instanciaend	Iomain Guesta	5-1-5-21-41103742415-4130520126-20482399	GLOBAL		
			•	advenia, uniteritation	Iomain Users	5-1-5-21-4193742415-4133920128-20492399.	6L084L		
			0	adven-aj / m.con/Geo/d	Interprise Admins	5-1-5-21-4193742415-4133920028-20492399	UNIVERSAL		
			0	adrem-aj v m.com/Users/E	Interprise Key Admins	5+1-5-21-4110742415-4130520124-20482398	UNIVERSAL		
			0	adremia, stim.com/Users/E	interprise Read-only	5-1-5-21-4193742415-4133920026-20492399.	UNIVERSAL	-	
			0	ad.rem-ay.am.com/Users/C	Droug Policy Creator	5-1-5-21-4110742415-4100120028-20442098	CLOBAL		
			1					,	
							Cancel	ox	

도메인 컴퓨터 및 사용자 추가

3단계. 머신 인증 설정 확인

Advanced Settings(고급 설정) 탭으로 이동하여 머신 인증 설정을 확인합니다.

- Enable Machine Authentication(머신 인증 활성화): 머신 인증을 활성화하려면
- Enable Machine Access Restriction(머신 액세스 제한 활성화): 권한 부여 전에 사용자 인증과 머신 인증을 결합합니다.



참고: 유효한 에이징 시간 범위는 1~8760입니다.



머신 인증 설정

4단계. ID 소스 시퀀스 추가

Administration(관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동하여 ID 소스 시퀀스를 추가합니다.

- 이름: Identity_AD
- 인증 검색 목록: AD_Join_Point

≡	dentity Services I	ngine Administration / Identity Management
Ц	Bookmarks	dentities Groups External Identity Sources Identity Source Sequences Settings
-	Dashboard	Identity Source Sequences List > Identity AD
15	Context Visibility	Identity Source Sequence
×	Operations	
.0	Policy	Identity Source Sequence Name
80	Administration	Identity_AD
đ	Work Centers	Description
٢	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
	시 미리 시 국 기	

ID 소스 시퀀스 추가

5단계. DACL 및 권한 부여 프로파일 추가

Policy(정책) > Results(결과) > Authorization(권한 부여) > Downloadable ACLs(다운로드 가능한 ACL)로 이동하여 DACL을 추가합니다.

- 이름: MAR_Passed
- DACL 콘텐츠: 허용 ip any host 1.x.x.101 및 허용 ip any host 1.x.x.105

≡	dentity Services E	ingine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions Results		
53	Dashboard	Authentication > Download	dable ACL List > MAR_Passed	
망	Context Visibility	Authorization	loadable ACL	
*	Operations	Authorization Profiles	* Name MAR_Passed	
0	Policy	Downloadable ACLs	escription	
a.	Administration	Profiling >	IP version @ IPv4	
n li	Work Centers	Posture > * DACI	2L Content 1224567 permit ip any host 1.(1),0.101	
		Client Provisioning >	2010111 permit ip any host 1.13 (2.151) 2131415 1617181	

```
DACL 추가
```

Policy(정책) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파 일)로 이동하여 권한 부여 프로파일을 추가합니다.

- 이름: MAR_Passed
- DACL 이름: MAR_Passed

≡	dentity Services I	Ingine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	R	esults	
	Dashboard	Authentication	>	Authorization Profiles > MAR_P	Passed
15	Context Visibility	Authorization	, ,	Authorization Profile	
*	Operations	Authorization Profiles		* Name	MAR Passed
U.	Policy	Downloadable ACLs		Description	murit 634.8
80	Administration	Profiling	>		
nii:	Work Centers	Posture	>	* Access Type	ACCESS_ACCEPT V
		Client Provisioning	>	Network Device Profile	± Cisco ∨⊕
?	Interactive Help			Service Template	8
				Track Movement	
				Agentless Posture	
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed ~
권한	! 부여 프로파일	추가			

6단계. 정책 집합 추가

Policy(정책) > Policy Sets(정책 세트)로 이동하고 +를 클릭하여 정책 세트를 추가합니다.

- 정책 집합 이름: MAR_Test
- 조건: Wired_802.1X
- 허용되는 프로토콜/서버 시퀀스: 기본 네트워크 액세스

=	dentity Services Er	ngine		Policy / Policy Sets		A Evaluation	on Mode El	9 0 aya C	۵ ۵	0	0	۹
н	Bookmarks	Policy Sets				Click he	re to do v	isibility set	tup Do n	ot show th	his again.	×
11	Dashboard	 Status Policy Set Name 	Description	Conditions	Allowe	d Protocols	/ Server	Sequence	Hits	Actions	View	
15	Context Visibility	Q Search										
*	Operations	MAR_Test		Www.s.802.1X	Defau	it Network A	ccess	×+	15	٢	•	
8.	Administration	Oefault	Default policy set		Defau	it Network A	ccess	/+	٥	ø	•	
-1	Work Centers											
									Reset		Save	

정책 집합 추가

7단계. 인증 정책 추가

인증 정책을 추가하려면 Policy Sets(정책 집합)로 이동하고 MAR_Test(MAR_테스트)를 클릭합니 다.

- 규칙 이름: MAR_dot1x
- 조건: Wired_802.1X
- 사용: Identity_AD

~Authentication Policy(2)									
	⊙	Status	Rule Name	Use	Hits	Actions			
	Q	Search	h						
		0	MAR_dot1x	E Wired_802.1X	Identity_AD //	n	ŵ		
		0	Default		All_User_ID_Stores /	0	¢		

인증 정책 추가

8단계. 권한 부여 정책 추가

Policy Sets(정책 집합)로 이동하고 MAR_Test를 클릭하여 권한 부여 정책을 추가합니다.

- 규칙 이름: MAR_Passed
- 조건: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- 결과: MAR_Pass
- 규칙 이름: User_MAR_Passed
- 조건: 네트워크 액세스·WasMachineAuthenticated EQUALS True AND AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Users
- 결과: Permit Access

✓Authorization Policy(3)										
🕣 Status Rule Name	Conditions	Results Profiles	Security Groups							
Q Search MAR_Passed	AND R AD_Join_Point ExternalDroups EQUALS ad.rem-sp im.com/Users/Domain Computers Wetwork_Access_Authentication_Passed	MAR_Passed	/ + Select from list /	+ 1	\$					
User_MAR_Passed	AND AD AD AD AD AD AD AD	PermitAccess	A + Select from list A	+ 1	¢					
Oefault		DenyAccess	/ + Select from list /	• +	ŵ					

다음을 확인합니다.

패턴 1. 머신 인증 및 사용자 인증

1단계. Windows PC 로그아웃

Win10 PC1에서 로그아웃 단추를 클릭하여 머신 인증을 트리거합니다.



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

3단계. Windows PC 로그인

Win10 PC1에 로그인하여 사용자 인증을 트리거하려면 사용자 이름 및 비밀번호를 입력합니다.



Windows PC 로그인

4단계. 인증 세션 확인

C1000에서 사용자 인증 세션을 확인하려면 명령을 실행하십시오show authentication sessions interface GigabitEthernet1/0/2 details.

<#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

5단계. Radius 라이브 로그 확인

ISE GUI에서 Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동하여 머신 인증 및 사용자 인증을 위한 라이브 로그를 확 인합니다.

	dentity Services	Engine					Operations / F	ADIUS				A Evaluation Mode -Days	۵ ۵	
н	Bookmarks	Live Lo	gs Live Sessions											
51	Dashboard		-											
명	Context Visibility	м	isconfigured Supplicants 🕕			Mis	configured Network Devices 🕕		RADIUS Drops		Client Stopped Responding	0		Repeat Counter 🕕
*	Operations		0				0		0		0			0
0	Policy										Refresh Never	Show Latest 20 reco	ards 🗸	Within Last 3 hours 🗸 🗸
-1	Work Centers	0	🖆 Reset Repeat Counts	\oplus Export To \vee										Filter $\vee = 0$
			Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P IP Addr	ress	Network De
(?)	Interactive Help		×	~			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi IP Addr	ess 🗸	Network Devic
			May 07, 2024 04:36:14	•	0	0	ADitestuser	84.96.91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto User_MAR_Pessed$	PermitAccess 1.1) 2	9	
			May 07, 2024 04:36:13	8	à		ADitestuser	84.96.91.15.84	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess 1.1 - 0.	9	C1000
			May 07, 2024 04:35:12	8	ò		#ACSACL#-IP-MAR_Passed-6639ba20							C1000
			May 07, 2024 04:35:12	8	ò		host/DESKTOP-L2IL9I6.ad.rem-s_ithm	84:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \gg MAR_Passed$	MAR_Passed 169.254	.90.1	C1000

Radius 라이브 로그

시스템 인증의 자세한 라이브 로그를 확인합니다.

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 mm.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 Queried PIP - Normalised Radius.RadiusFlowType 15048 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 Returned RADIUS Access-Challenge 1 11006 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

RADIUS is re-using an existing session

0

Steps

11018

머신 인증 세부 정보

사용자 인증의 자세한 라이브 로그를 확인합니다.

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
			11001	Received RADIUS Access-Request	8
			11018	RADIUS is re-using an existing session	0
Authentication Details	S		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	1.77 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
Identify Course	Deefferd		12810	Prepared TLS ServerDone message	0
Identity Group	Profiled		12305	Prepared EAP-Request with another PEAP challenge	1
Audit Session Id	01C2006500000049AA780D80		11006	Returned RADIUS Access-Challenge	0
Authentication Method	dot1x		11001	Received RADIUS Access-Request	30
Authention Drotocol	DEAD (EAD-MSCHAD-2)		11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPVZ)		12304	Extracted EAP-Response containing PEAP challenge-	0

사용자 인증 세부 정보

패턴 2. 사용자 인증만

1단계. Windows PC의 NIC 비활성화 및 활성화

사용자 인증을 트리거하려면 Win10 PC1의 NIC를 비활성화하고 활성화합니다.

2단계. 인증 세션 확인

C1000에서 사용자 인증 세션을 확인하려면 명령을 실행하십시오show authentication sessions interface GigabitEthernet1/0/2 details.

<#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

```
3단계. Radius 라이브 로그 확인
```

ISE GUI에서 Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동하여 사용자 인증을 위한 라이브 로그를 확인합니다.



참고: MAR 캐시는 ISE에 저장되므로 사용자 인증만 필요합니다.

$\equiv \frac{1}{1000}$ 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 Malo	×	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	04:96:91:15:84: In	ntel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1	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

사용자 인증의 자세한 라이브 로그를 확인합니다.

Cisco ISE

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (m
		11001	Received RADIUS Access-Request - AD_Join_Point	
Username	AD\testuser	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
		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	Extracted EAP-Resonase/NAK requestion to use PEAP	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 EAP-Key-Name attribute received	0
		11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01	11001	Received RADIUS Access-Request	25
Event	5200 Authentication succeeded	11018	Extracted EAP-Researce containing PEAP challenge	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	B4-96-91-15-84-CB	12318	Successfully negotiated PEAP version 0	0
		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	AD tale Dates	12807	Prepared TLS Certificate message	26
Store	AD_Join_Point	12810	Propared TLS ServerDone message	0
Identity Group	Profiled	12305	Prepared EAP-Request with another PEAP challenge	0
Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	14
Authentication Method	dot1x	11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge- response	1
Service Type	Framed	12305	Prepared EAP-Request with another PEAP challenge	0
Network Device	C1000		ISE has confirmed previous successful machine	
	service-type=Framed,	24422	authentication for user in Active Directory	0
	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
	362cec4b413d#testuser@ad.rem-sy_tc_1.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef92	24211	Found Endpoint in Internal Endpoints IDStore	3
	17/9	24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad.rem-sy: em.com/Builtin/Users	24355	LDAP fetch succeeded	
AD Croups Names	ad rom and a com/Duiltie (Administration	24416	User's Groups retrieval from Active Directory succeeded	
AD-Groups-Names	au.rem-sim.com/builun/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
AD-Groups-Names	ad.rem-sy** n.com/Users/Denied RODC Password Replication Group	15016	Selected Authorization Profile - PermitAccess	5
	common data strange	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-syffm.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

사용자 인증 세부 정보

문제 해결

이러한 디버그 로그(prrt-server.log)는 ISE에서 인증의 자세한 동작을 확인하는 데 도움이 됩니다.

• 런타임 구성

- 런타임 로깅
- 런타임 AAA

패턴 1의 디버그 로그 예입니다. 이 문서의 시스템 인증 및 사용자 인증

<#root>

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

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,CPMSessionII
```

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

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

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

// 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,CPMSessionII

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

관련 정보

<u>머신 액세스 제한 장점 및 단점</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.