FXOS(firepower eXtensible Operating System) 2.2: RADIUS를 사용하는 ISE를 통한 원격 관리를 위한 섀시 인증/권한 부여

P	ᆕ	
ᆃ		ľ

 소····

 사·····

 요·····

 요·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ·····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

 ····

소개

이 문서에서는 ISE(Identity Services Engine)를 통해 Firepower FXOS(eXtensible Operating System) 섀시에 대한 RADIUS 인증 및 권한 부여를 구성하는 방법에 대해 설명합니다.

FXOS 섀시에는 다음 사용자 역할이 포함됩니다.

- 관리자 전체 시스템에 대한 완전한 읽기 및 쓰기 액세스. 기본 관리자 계정은 기본적으로 이 역할에 할당되며 변경할 수 없습니다.
- 읽기 전용 시스템 상태를 수정할 권한이 없는 시스템 컨피그레이션에 대한 읽기 전용 액세스
- 운영 NTP 컨피그레이션, Smart Licensing용 Smart Call Home 컨피그레이션, 시스템 로그 (syslog 서버 및 결함 포함)에 대한 읽기 및 쓰기 액세스 시스템의 나머지 부분에 대한 읽기 액 세스.
- AAA 사용자, 역할 및 AAA 구성에 대한 읽기 및 쓰기 액세스. 시스템의 나머지 부분에 대한 읽기 액세스.

CLI를 통해 다음과 같이 확인할 수 있습니다.

fpr4120-TAC-A /security* # 역할 표시

역할:

역할 이름 권한

----- ----

aaa

관리자

운영 작업

읽기 전용 읽기 전용

기고자: Tony Remirez, Jose Soto, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower eXtensible 운영 체제(FXOS)에 대한 지식
- ISE 구성에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 4120 Security Appliance 버전 2.2
- 가상 Cisco Identity Services Engine 2.2.0.470

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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

컨피그레이션의 목표는 다음과 같습니다.

- ISE를 통해 FXOS의 웹 기반 GUI 및 SSH에 로그인하는 사용자 인증
- ISE를 통해 각 사용자 역할에 따라 FXOS의 웹 기반 GUI 및 SSH에 로그인하는 사용자에게 권 한을 부여합니다.
- ISE를 통해 FXOS에서 인증 및 권한 부여가 제대로 작동하는지 확인합니다.

네트워크 다이어그램



설정

FXOS 섀시 구성

Chassis Manager를 사용하여 RADIUS 제공자 생성

1단계. Platform Settings(플랫폼 설정) > AAA로 이동합니다.

2단계. RADIUS 탭을 클릭합니다.



3단계. 추가할 각 RADIUS 제공자에 대해(최대 16개 제공자).

3.1. RADIUS Providers(RADIUS 제공자) 영역에서 Add(추가)를 클릭합니다.

3.2. Add RADIUS Provider(RADIUS 제공자 추가) 대화 상자가 열리면 필요한 값을 입력합 니다.

3.3. OK(확인)를 클릭하여 Add RADIUS Provider(RADIUS 제공자 추가) 대화 상자를 닫습 니다.

Edit 10.88.244.50	?×
Hostname/FQDN(or IP Address):*	10.88.244.50
Order:*	1
Key:	•••••• Set:Yes
Confirm Key:	•••••
Authorization Port:*	1812
Timeout:*	5 Secs
Retries:*	1
	OK Cancel

4단계. 저장을 클릭합니다.

Overview Interfaces Logic	cal Devices Security Engine	Platform Settings			
NTP	LDAP RADIUS TACACS				
SSH SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
Syslog	Retries:* 1				
DNS EIRS and Common Criteria	RADIUS Providers				
Access List					Add
	Hostname	Order	Service	Auth Port	
	10.88.244.50	1	authorization	1812	J 🗍
	Save				

5단계. System(시스템) > User Management(사용자 관리) > Settings(설정)로 이동합니다.

6단계. Default Authentication(기본 인증)에서 RADIUS를 선택합니다.

Overview Interfaces Logic	al Devices Security Engine Platform Settings		-	System Too	is Help fxosadmin
		Configuration	Licensing	Updates	User Management
Local Users Settings					
Default Authentication	RADIUS v *Local is failback authentication method				
Console Authentication	Local v				
Remote User Settings Remote User Role Policy	Q Assign Default Role ○ No-Login				

CLI를 사용하여 RADIUS 제공자 생성

1단계. RADIUS 인증을 활성화 하려면 다음 명령을 실행 합니다.

fpr4120-TAC-A# 범위 보안

fpr4120-TAC-A /보안 # 범위 기본 인증

fpr4120-TAC-A /security/default-auth # 영역 반경 설정

2단계. show detail 명령을 사용하여 결과를 표시합니다.

fpr4120-TAC-A /security/default-auth # 세부 정보 표시

기본 인증:

관리 영역: Radius

작동 영역: Radius

웹 세션 새로 고침 기간(초): 600

웹, ssh, 텔넷 세션에 대한 세션 시간 초과(초): 600

웹, ssh, 텔넷 세션에 대한 절대 세션 시간 초과(초): 3600

직렬 콘솔 세션 시간 초과(초): 600

Serial Console Absolute Session 시간 초과(초): 3600

관리자 인증 서버 그룹:

운영 인증 서버 그룹:

두 번째 요소의 사용: 아니요

3단계. RADIUS 서버 매개변수를 구성하려면 다음 명령을 실행합니다.

fpr4120-TAC-A# 범위 보안

fpr4120-TAC-A /security # 범위 반경

fpr4120-TAC-A /security/radius # enter server 10.88.244.50

fpr4120-TAC-A /security/radius/server # set descr "ISE 서버"

fpr4120-TAC-A /security/radius/server* # set key

키 입력: ******

키 확인: *****

4단계. show detail 명령을 사용하여 결과를 표시합니다.

fpr4120-TAC-A /security/radius/server* # 세부 정보 표시

RADIUS 서버:

호스트 이름, FQDN 또는 IP 주소: 10.88.244.50

설명:

주문: 1

인증 포트: 1812

키: ****

시간 초과: 5

ISE 서버 구성

FXOS를 네트워크 리소스로 추가

1단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.

2단계. Add(추가)를 클릭합니다.

dentity Services Engine	Home + Context	Visibility	► Policy - Administr	tion Vork Centers		
System Identity Management	 Network Resources 	Device Portal Manageme	ent pxGrid Services + F	eed Service + Threat Centric N	IAC	
Network Devices Network Device Gi	roups Network Devi	ce Profiles External RADIL	JS Servers RADIUS Serve	r Sequences NAC Managers	External MDM	
0						
Network devices	Network Devic	es				
Default Device						
Device Security Settings	/ Edit 🕂 Add [Duplicate	Export Generate PAC	XDelete		
	Name	▲ IP/Mask Profile	e Name	Location	Туре	Description
					No da	a available

3단계. 필수 값(이름, IP 주소, 디바이스 유형 및 RADIUS 활성화, 키 추가)을 입력하고 Submit(제출)을 클릭합니다.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Network Devices Network Device G	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
0		
Network devices	Network Devices List > New Network Device	
Default Device	Nome EVOC	
Device Security Settings	Description	
	* IP Address: 10.83.180.6 / 32	
	Device Profile Box Cisco T	
	Model Name	
	Software Version	
	1 Network Davies Course	
	* Network Device Group	
	Device Type FXOS Set To Default	
	IPSEC Is IPSEC Device 📀 Set To Default	
	Location All Locations Set To Default	
	RADIUS Authentication Settings	
	RADIUS UDP Settings	
	Protocol RADIUS	
	* Shared Secret Show	
	CoA Port 1700 Set To Default	
	RADIUS DTLS Settings ()	
	DTLS Required 🔲 🕧	
	Shared Secret radius/dtls (1)	
	CoA Port 2083 Set To Default	
	Issuer CA of ISE Certificates for CoA Select if required (optional)	

ID 그룹 및 사용자 생성

1단계. Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)로 이동합니다.

2단계. Add(추가)를 클릭합니다.

denti	ty Services E	ingine	Home	▸ Context V	/isibility	 Operations 	▶ Policy	→ Admini	istration	▸ Work Centers	
System	- Identity Man	agement	Network	Resources	Device	Portal Managemen	t pxGrid S	Services	Feed Ser	vice	AC
Identities	Groups Ex	xternal Iden	tity Sources	Identity So	urce Sequ	ences	s				

Identity Groups	User Identity Groups	
⟨= • E • [⊕] •		
Endpoint Identity Groups	Name 🔺	Description
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	Default Employee User Group
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
	GuestType_Contractor (default)	Identity group mirroring the guest type
	GuestType_Daily (default)	Identity group mirroring the guest type
	GuestType_Weekly (default)	Identity group mirroring the guest type
	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

3단계. Name(이름) 값을 입력하고 Submit(제출)을 클릭합니다.

dentity Services Engine	Home	Operations Policy	Administration Work Centers	
► System - Identity Management	Network Resources Devi	ice Portal Management pxGrid	Services + Feed Service + Threat Centr	ic NAC
Identities Groups External Iden	ntity Sources Identity Source Se	equences > Settings		
Identity Groups Identity Groups Image: Ima	User Identity G Identity G * Name Description Submit	Groups > New User Identity Grov Oup FXOS ADMIN Cancel	4r	

4단계. 필요한 모든 사용자 역할에 대해 3단계를 반복합니다.

tisco Identity Services Engine Home	Context Visibility Operations Policy Adn	ninistration Work Centers
System Identity Management Network Re	sources	Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
<	✓ Edit ♣Add X Delete ▼ ♣Import ♣ Export	•
Endpoint Identity Groups	Name	Description
User Identity Groups	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Rame: Currently Sorted	Default Employee User Group
	EXOS AAA	
	FXOS ADMIN	
	EXOS OPER	
	FXOS Read Only	
		BLE-IL CROUR LOCOURTS (J.E. IN U.S. C

5단계. Administration(관리) > Identity Management(ID 관리) > Identity(ID) > Users(사용자)로 이동 합니다.

6단계. Add(추가)를 클릭합니다.

-indu Identity Services Engine	Home ► Context Visibility ► Op	perations Policy Administration	► Work Centers
System Identity Management	Network Resources	Management pxGrid Services + Feed Se	ervice
◄ Identities Groups External Identity	Sources Identity Source Sequences	 Settings 	
0			
Users	Network Access Users		
Latest Manual Network Scan Results	/ Edit + Add SChange Status	Timport Export X Delete	Duplicate
	Status Name	Description First	rst Name Last Name Email Address User Identity Groups Admin
			No data available

7단계. 필수 값(이름, 사용자 그룹, 비밀번호)을 입력합니다.

dentity Services Engine Ho	me Context Visibility Operations Policy Administration Work Centers
System ✓ Identity Management Ne	etwork Resources
✓ Identities Groups External Identity So	surces Identity Source Sequences + Settings
0	
Users	etwork Access Users List > New Network Access User
Latest Manual Network Scan Results	
	* Name fxosadmin
	Status 🗹 Enabled 👻
	Email
	▼ Passwords
	Password Type: Internal Users
	Password Re-Enter Password
	* Login Password Generate Password
	Enable Password
	▼ User Information
	First Name
	Last Name
	✓ Account Options
	Description
	Change password on next login
	Account Disable Policy
	Diable account if date exceede 2018-02-01 (www.mm-dd)
	— Disprie genorium agte evenenge T070.02.07 (1)11
	▼ User Groups
	Submit

8단계. 모든 필수 사용자에 대해 6단계를 반복합니다.

Identity Services Engine	Home + Conte	xt Visibility	Policy Administra	tion 🔹 Work Ce	onters			
System - Identity Management	Network Resources	 Device Portal Manageme 	nt pxGrid Services + Fe	eed Service + Th	reat Centric NAC			
Identities Groups External Identity	Sources Identity	Source Sequences Settin	gs					
0								
Users	Network Acce	ss Users						
Latest Manual Network Scan Results	/ Edit 🕂 Add	🔀 Change Status 👻 🎲 Impo	t 🔀 Export 👻 🗙 Delete 🕶	Duplicate				
	Status	Name	 Description 	First Name	Last Name	Email Address	User Identity Groups	Admin
	🗌 🛃 Enabled	👤 fxosaaa					FXOS AAA	
	Enabled	👤 fxosadmin					FXOS ADMIN	
	🗌 🗹 Enabled	2 fxosoper					FXOS OPER	
	🗌 🛃 Enabled	👤 fxosro					FXOS Read Only	

각 사용자 역할에 대한 권한 부여 프로파일 생성

1단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다.

dentity Services Engine	Home	ons - Policy - Administration	Work Centers ■	
Authentication Authorization Profili	ng Posture Client Provisioning - Pol	y Elements		
Dictionaries + Conditions - Results	3			
0				
Authentication	Standard Authorization Profil	s		
Authorization	For Policy Export go to Administration	System > Backup & Restore > Policy Expo	ort Page	
Authorization Dealling	/ Edit 🕂 Add 🕞 Duplicate 🗙 D	ete		
Authorization Prohies	Name	Profile	•	Description
Downloadable ACLs	Blackhole_Wireless_Access	sta Cisco	Ð	Default profile used to blacklist wireless devices. Ens
▶ Profiling	Cisco_IP_Phones	deta Cisco	Ð	Default profile used for Cisco Phones.
▶ Posture	ture Cisco_WebAuth		Ð	Default Profile used to redirect users to the CWA por
			Ð	Onboard the device with Native Supplicant Provisioni
Client Provisioning	Non_Cisco_IP_Phones	deta Cisco	Ð	Default Profile used for Non Cisco Phones.
	DenyAccess			Default Profile with access type as Access-Reject
	PermitAccess			Default Profile with access type as Access-Accept

2단계. 권한 부여 프로파일에 대한 모든 특성을 채웁니다.

2.1. 프로파일 이름을 구성합니다.

Authentication Authorization Prof	ing Posture Client Provisioning - Policy Elements
Dictionaries Conditions Result	ts
6	
Authentication	Authorization Profiles > FXOS-ADMIN-PROFILE
	Authorization Profile
- Authorization	* Name FXOS-ADMIN-PROFILE
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT T
▶ Profiling	Network Device Profile dt Cisco 👻 🕀

2.2. Advanced Attributes Settings(고급 특성 설정)에서 다음 CISCO-AV-PAIR를 구성합니다

cisco-av-pair=shell:roles="admin"

Advanced Attributes Settings		
Cisco:cisco-av-pair 📀	= shell:roles="admin"	⊘ — ф

2.3. 저장을 클릭합니다.



3단계. 다음 Cisco-AV 쌍을 사용하여 나머지 사용자 역할에 대해 2단계를 반복합니다

cisco-av-pair=shell:roles="aaa"

Cisco:cisco-av-pair

cisco-av-pair=shell:roles="operations"

|--|

 Advanced Attributes Settings 	
Cisco:cisco-av-pair	🔰 = shell:roles="aaa" 📀 — 🕂
 Advanced Attributes Settings 	

= shell:roles="operations"

 \bigcirc

⊘ — +

인증 정책 생성

1단계. Policy(정책) > Authentication(인증) >으로 이동하고 규칙을 생성할 수정 위치 옆의 화살표를 클릭합니다.



2단계. 설정은 간단합니다. 좀 더 세부적으로 설정할 수 있지만 이 예에서는 디바이스 유형을 사용 합니다.

이름: FXOS 인증 규칙

IF Select new attribute/value(새 특성/값 선택): Device:Device Type Equals All Devices Types #FXOS(디바이스:디바이스 유형이 모든 디바이스 유형과 같음)

프로토콜 허용: 기본 네트워크 액세스

용도: 내부 사용자

e 🖉 🖉	F	EXOS AUTHENTICATION RULE : If	DEVICE:Device Type EQUALS All Device Types#FXOSAllow Protocols : Default Network Access	and
	~	Default	:use Internal Users	

권한 부여 정책 생성

1단계. Policy(정책) > Authorization(권한 부여) >으로 이동하고 화살표 네트를 클릭하여 규칙을 생성할 위치를 수정합니다.

cisco Identity S	Services Engine	Home + Context Visibility + Operations	Centers	🕒 🤉 🔍 🖉 🖉
Authentication	Authorization	Profiling Posture Client Provisioning + Policy Elements		Click here to do wireless set in and visibility set in Do not show this again
				Citick have to do writeress setup and hadning setup do not anow the again.
Authorization	Policy			
Define the Authorit For Policy Export	zation Policy by c go to Administrati	onfiguring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. on > System > Backup & Restore > Policy Export Page		
First Matched Rul	le Applies	v		
Exceptions	(0)			
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Default	If no matches, then DenyAccess		Insert New Rule Above
Save Dese	•			

2단계. 필수 매개변수를 사용하여 Authorization 규칙의 값을 입력합니다.

2.1. 규칙 이름: Fxos <사용자 역할> 규칙



2.2. 경우: User Identity Groups(사용자 ID 그룹) > Select <USER ROLE>.

Conditions (identity groups and other condition	ions) Permissions
if FX Condition(s)	ය then AuthZ Pr ද
í no ma	
FXOS ADMIN	○ - +
	User Identity Groups
	⟨= •
	FXOS AAA
	GuestType_Weekly (default)
	OWN_ACCOUNTS (default)
	GROUP_ACCOUNTS (default)
	FXOS ADMIN
	FXOS OPER
	Employee
	GuestType_Daily (default)
	GuestType_Contractor (default)
	FXOS Read Only
	ALL_ACCOUNTS (default)

2.3. AND: Create New Condition(새 조건 생성) > Device(디바이스):Device Type Equals All Devices Types #FXOS(디바이스 유형이 모든 디바이스 유형과 같음).

Conditions (identity groups and other	er conditions)	Permissions			
if FX 💠 and DEVIC	E:Device Type EQUALS All 🗢	then Select an item 🔶			
if no matches, then DenyAc 💾 🗚	Add All Conditions Below to Library				
	Condition Name Description DEVICE:Device	Ty 🚫 Equals 🔻	All Device Types# 📀	ŵ .	
			C	<u>م</u> العالم العام العالم العالم الم)
				All Device Types	
				All Device Types#FXOS	
				AD >	
				Airespace >	<u></u>
				Alcatel-Lucent >	·
				Aruba >	·
				Brocade >	·
				CERTIFICATE >	,
				Cisco >	•
				Cisco-BBSM >	,
				Cisco-VPN3000 >	,
				CWA >	,

2.4. 권한: 표준 > 사용자 역할 프로필 선택

Permissions		
then FXOS-A 🗢		
FXOS-ADMIN-PROFILE		
	Standard	
	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	
	General Blackhole_Wireless_Access	
	Cisco_IP_Phones	
	G Cisco_WebAuth	
	G DenyAccess	
	😪 FXOS-AAA-PROFILE	
	S FXOS-ADMIN-PROFILE	
	S FXOS-OPER-PROFILE	
	Generation FXOS-ReadOnly-PROFILE	
	😪 NSP_Onboard	
	😪 Non_Cisco_IP_Phones	
	SermitAccess	
l.		

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Fxos Admin Rule if	FXOS ADMIN AND DEVICE: Device Type EQUALS All Device Types#FXOS	FXOS-ADMIN-PROFILE

3단계. 모든 사용자 역할에 대해 2단계를 반복합니다.

Status	Rule Name	nditions (identity groups and o	ther conditions)	Permissions
~	Fxos Admin Rule	DS ADMIN AND DEVICE:Dev es#FXOS	vice Type EQUALS All Device the	n FXOS-ADMIN-PROFILE
	Fxos AAA Rule	DS AAA AND DEVICE:Devic es#FXOS	e Type EQUALS All Device the	n FXOS-AAA-PROFILE
	Fxos Oper Rule	DS OPER AND DEVICE:Devi es#FXOS	ce Type EQUALS All Device the	n FXOS-OPER-PROFILE
	Fxos Read only Rule	OS Read Only AND DEVICE es#FXOS	Device Type EQUALS All Device the	n FXOS-ReadOnly-PROFILE
~	Default	atches, then DenyAccess		

4단계. 페이지 하단에서 Save(저장)를 클릭합니다.



다음을 확인합니다.

이제 각 사용자를 테스트하고 할당된 사용자 역할을 확인할 수 있습니다.

FXOS 섀시 확인

1. 텔넷 또는 SSH를 FXOS 섀시에 연결하고 ISE에서 생성된 사용자 중 하나를 사용하여 로그인 합니다.

사용자 이름: fxosadmin

암호:

fpr4120-TAC-A# 범위 보안

fpr4120-TAC-A /security # 원격 사용자 세부 정보 표시

원격 사용자 fxosaaa:

설명:

사용자 역할:

이름: aaa

이름: 읽기 전용

원격 사용자 fxosadmin:

설명:

사용자 역할:

이름: admin

이름: 읽기 전용

원격 사용자 FXOSOPER:

설명:

사용자 역할:

Name(이름): operations(작업)

이름: 읽기 전용

원격 사용자 fxosro:

설명:

사용자 역할:

이름: 읽기 전용

입력한 사용자 이름에 따라 FXOS 섀시 cli는 할당된 사용자 역할에 대해 권한이 부여된 명령만 표시 합니다.

관리자 사용자 역할

fpr4120-TAC-A /security # ?

승인

사용자 세션 지우기 사용자 세션 지우기

작성 관리 객체 작성

삭제 관리 객체 삭제

disable 서비스 비활성화

enable 서비스 활성화

enter 관리되는 개체를 입력합니다.

범위 현재 모드를 변경합니다.

set Set 속성 값

show 시스템 정보 표시

활성 cimc 세션 종료

fpr4120-TAC-A# fxos 연결

fpr4120-TAC-A (fxos) # debug aaa-requests

fpr4120-TAC-A(fxos)#

읽기 전용 사용자 역할

fpr4120-TAC-A /security # ?

범위 현재 모드를 변경합니다.

set Set 속성 값

show 시스템 정보 표시

fpr4120-TAC-A# fxos 연결

fpr4120-TAC-A (fxos) # debug aaa-requests

% 역할에 대해 거부된 권한

2. FXOS 섀시 IP 주소로 이동하고 ISE에서 생성된 사용자 중 하나를 사용하여 로그인합니다.

관리자 사용자 역할

Overview Interfaces Logica	al Devices Security Engine Platform S	ettings						s	ystem Tools	Help fxosadmin
NTP SSH SNMP	LDAP RADIUS TACACS Properties									
NTTPs AAA Syslog DNS FIPS and Common Criteria	Timeout:* 5 Secs Retries:* 1 RADIUS Providers		Add RADIUS Provider							
Access List	Hostname	Order	Key:	Concert and name	Set:No	-				
	10.88.244.16 1 Confirm Key: Authorization Port:* Timesuti* Retries:*	Confirm Key: Authorization Port:" Timeout:" Retries:"	1812 5 Secs 1 OK Carc	el	- 5					

읽기 전용 사용자 역할

Ove	rview Interfaces	Logical Devices Security Engine	Platform Settings			ļ
N	TP	LDAP RADIUS TACKS				
5	SH NMP	Properties				
н	TTPS	Timeout:* 5 Secs				
5	yslog	Retries:* 1				
0	NS IPS and Common Criteria	RADIUS Previders				0
~	coess List	Hostname	Order	Service	Auth Port	
		10.88.244.16	1	authorization	1812	۹.9

참고: ADD(추가) 버튼이 회색으로 표시됩니다.

ISE 2.0 확인

1. Operations(운영) > RADIUS > Live logs(라이브 로그)로 이동합니다. 성공 및 실패한 시도를 볼 수 있어야 합니다.

dent	tity Services Engir	e Home	Context Visi	bility • Operat	tions Pr	olicy	Administration	Work Centers						 	0 0	1
→ RADIUS	Threat-Centric NA	C Live Logs + 1	TACACS • Tr	oubleshoot + A	daptive Networ	rk Contro	ol Reports					Click here to do w	ireless setup and visibili	ty setup Do not	show this again.	
Live Logs	Live Sessions															
	Misconfigured Supplicants ()			Miscon	Misconfigured Network Devices O			RADIUS Drops 🕲		Client Stopped Re	sponding O		Repeat Counter 1			
	0			0		0	0				0					
										Refresh	Never	• Show	Latest 20 records	• Within La	st 3 hours	•
C Refresh O Reset Repeat Counts 🔮 Export To -											Y Filter - O	•				
Time	•	Status	Details	Repeat C	Identity	1	Authentication Pol	icy	Authoriz	zation Policy	Au	thorization Profiles	Network Dev.	. Identity C	Broup	
×		-			Identity		Authentication Policy	y .	Authoriz	zation Policy	A	uthorization Profiles	Network Device	Identity G	roup	
Jan 2	20, 2018 10:14:09	2	<u>o</u>		fxosadmin	C	Default >> FXOS AU	THENTICATION RULE >> Defau	It Default >	Fxos Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:13:59	۰	0		fxosadmin	0	Default >> FXOS AU	THENTIGATION RULE >> Defau	lt				FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:09:01	~	0		fxosro	0	Default >> FXOS AU	THENTIGATION RULE >> Defau	It Default >	Fxos Read only F	tule FX	OS-ReadOnly-PROFI	LE FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:08:50	۲	Q		fxosro	0	Default >> FXOS AU	THENTICATION RULE >> Defau	ít.				FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:06:17	۲	0		fxosro	0	Default >> FXOS AU	THENTIGATION RULE >> Defaul	it				FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:05:15	۲	0		fxosro	0	Default >> FXOS AU	THENTIGATION RULE >> Defau	it				FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:04:23	~	0		fxosadmin	0	Default >> FXOS AU	THENTICATION RULE >> Defau	It Default >	Fxos Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Ident	ity Groups:FXOS	
Jan 2	20, 2018 10:02:59		à +		fxosadmin	÷ (Default >> FXOS AU	THENTICATION RULE >> Defau	it Default >	Pros Admin Rule	FX	OS-ADMIN-PROFILE	FXOS	User Ident	ity Groups:FXOS	1

문제 해결

AAA 인증 및 권한 부여를 디버깅하려면 FXOS cli에서 다음 명령을 실행합니다.

fpr4120-TAC-A# fxos 연결

fpr4120-TAC-A (fxos) # debug aaa-requests

fpr4120-TAC-A (fxos) # debug aaa event

fpr4120-TAC-A (fxos) # debug aaa 오류

fpr4120-TAC-A(fxos)# 기간 mon

성공적인 인증 시도 후 다음 출력이 표시됩니다.

2018 Jan 20 17:18:02.410275 aaa: aaa_req_process for authentication. session no 0

2018 Jan 20 17:18:02.410297 aaa: aaa_req_process: appln의 일반 AAA 요청: login appln_subtype: default

2018년 1월 20일 17:18:02.410310 aaa: try_next_aaa_method

2018 Jan 20 17:18:02.410330 aaa: 구성된 총 메서드는 1이고, 시도할 현재 인덱스는 0입니다.

2018 Jan 20 17:18:02.410344 aaa: handle_req_using_method

2018년 1월 20일 17:18:02.410356 aaa: AAA_METHOD_SERVER_GROUP

2018 Jan 20 17:18:02.410367 aaa: aaa_sg_method_handler group = radius

2018 Jan 20 17:18:02.410379 aaa: 이 함수에 전달되는 sg_protocol 사용

2018 Jan 20 17:18:02.410393 aaa: RADIUS 서비스로 요청 전송

2018년 1월 20일 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon: 페이로드 길이 = 374

2018 Jan 20 17:18:02.412973 aaa: session: 0x8dfd68c added to the session table 1

2018 Jan 20 17:18:02.412987 aaa: 구성된 메서드 그룹 성공

2018년 1월 20일 17:18:02.656425 aaa: aaa_process_fd_set

2018 Jan 20 17:18:02.656447 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018 Jan 20 17:18:02.656470 aaa: mts_message_response_handler: mts 응답

2018 Jan 20 17:18:02.656483 aaa: prot_daemon_response_handler

2018년 1월 20일 17:18:02.656497 aaa: 세션: 0x8dfd68c가 세션 테이블 0에서 제거되었습니다.

2018년 1월 20일 17:18:02.656512 aaa: is_aaa_resp_status_success status = 1

2018년 1월 20일 17:18:02.656525 aaa: is_aaa_resp_status_success is TRUE

2018년 1월 20일 17:18:02.656538 aaa: aaa_send_client_response for authentication. session->flags=21. aaa_resp->flags=0.

2018 1월 20 17:18:02.656550 aaa: AAA_REQ_FLAG_NORMAL

2018년 1월 20일 17:18:02.656577 aaa: mts_send_response 성공

2018 Jan 20 17:18:02.700520 aaa: aaa_process_fd_set: aaa_accounting_q의 mtscallback

2018 1월 20 17:18:02.700688 aaa: 이전 OPCODE: accounting_interim_update

2018 Jan 20 17:18:02.700702 aaa: aaa_create_local_acct_req: user=, session_id=, log=added user fxosro

2018 Jan 20 17:18:02.700725 aaa: accounting을 위한 aaa_req_process. session no 0

2018 Jan 20 17:18:02.700738 aaa: MTS 요청 참조가 NULL입니다. 로컬 요청

2018 Jan 20 17:18:02.700749 aaa: AAA_REQ_RESPONSE_NOT_NEEDED 설정

2018 Jan 20 17:18:02.700762 aaa: aaa_req_process: appln의 일반 AAA 요청: default appln_subtype: default

2018년 1월 20일 17:18:02.700774 aaa: try_next_aaa_method

2018 Jan 20 17:18:02.700798 aaa: 기본 설정에 대해 구성된 메서드 없음

2018 Jan 20 17:18:02.700810 aaa: 이 요청에 사용할 수 있는 구성이 없습니다.

2018 Jan 20 17:18:02.700997 aaa: aaa_send_client_response for accounting. session->flags=254. aaa_resp->flags=0.

2018 Jan 20 17:18:02.701010 aaa: 구 도서관의 회계 요청에 대한 응답이 SUCCESS로 전송됩니다

2018 Jan 20 17:18:02.701021 aaa: 이 요청에 대한 응답이 필요하지 않습니다.

2018년 1월 20일 17:18:02.701033 aaa: AAA_REQ_FLAG_LOCAL_RESP

2018년 1월 20일 17:18:02.701044 aaa: aaa_cleanup_session

2018년 1월 20일 17:18:02.701055 aaa: aaa_req는 비워져야 합니다.

2018년 1월 20일 17:18:02.701067 aaa: 추락 방법 로컬 성공

2018년 1월 20일 17:18:02.706922 aaa: aaa_process_fd_set

2018 Jan 20 17:18:02.706937 aaa: aaa_process_fd_set: aaa_accounting_q의 mtscallback

2018 1월 20 17:18:02.706959 aaa: 이전 OPCODE: accounting_interim_update

2018 Jan 20 17:18:02.706972 aaa: aaa_create_local_acct_req: user=, session_id=, log=역할에 추 가된 user:fxosro:read-only

실패한 인증 시도 후 다음 출력이 표시됩니다.

2018년 1월 20일 17:15:18.102130 aaa: aaa_process_fd_set

2018 Jan 20 17:15:18.102149 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018년 1월 20일 17:15:18.102267 aaa: aaa_process_fd_set

2018 Jan 20 17:15:18.102281 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018년 1월 20일 17:15:18.102363 aaa: aaa_process_fd_set

2018 Jan 20 17:15:18.102377 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018년 1월 20일 17:15:18.102456 aaa: aaa_process_fd_set

2018 Jan 20 17:15:18.102468 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018년 1월 20일 17:15:18.102489 aaa: mts_aaa_req_process

2018 Jan 20 17:15:18.102503 aaa: aaa_req_process for authentication. session no 0

2018 Jan 20 17:15:18.102526 aaa: aaa_req_process: appln의 일반 AAA 요청: login appln_subtype: default

2018년 1월 20일 17:15:18.102540 aaa: try_next_aaa_method

2018 Jan 20 17:15:18.102562 aaa: 구성된 총 메서드는 1이고, 시도할 현재 인덱스는 0입니다.

2018년 1월 20일 17:15:18.102575 aaa: handle_req_using_method

2018년 1월 20일 17:15:18.102586 aaa: AAA_METHOD_SERVER_GROUP

2018 Jan 20 17:15:18.102598 aaa: aaa_sg_method_handler group = radius 2018 Jan 20 17:15:18.102610 aaa: 이 함수에 전달되는 sg_protocol 사용 2018 Jan 20 17:15:18.102625 aaa: RADIUS 서비스에 요청 전송 2018년 1월 20일 17:15:18.102658 aaa: mts_send_msg_to_prot_daemon: 페이로드 길이 = 371 2018 Jan 20 17:15:18.102684 aaa: session: 0x8dfd68c added to the session table 1 2018 Jan 20 17:15:18.102698 aaa: 구성된 메서드 그룹 성공 2018년 1월 20일 17:15:18.273682 aaa: aaa_process_fd_set 2018 Jan 20 17:15:18.273724 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018 Jan 20 17:15:18.273753 aaa: mts_message_response_handler: mts 응답

2018년 1월 20일 17:15:18.273768 aaa: prot_daemon_response_handler

2018년 1월 20일 17:15:18.273783 aaa: 세션: 0x8dfd68c가 세션 테이블 0에서 제거되었습니다.

2018년 1월 20일 17:15:18.273801 aaa: is_aaa_resp_status_success status = 2

2018년 1월 20일 17:15:18.273815 aaa: is_aaa_resp_status_success is TRUE

2018년 1월 20일 17:15:18.273829 aaa: aaa_send_client_response for authentication. session->flags=21. aaa_resp->flags=0.

2018 1월 20 17:15:18.273843 aaa: AAA_REQ_FLAG_NORMAL

2018년 1월 20일 17:15:18.273877 aaa: mts_send_response 성공

2018년 1월 20일 17:15:18.273902 aaa: aaa_cleanup_session

2018 1월 20 17:15:18.273916 aaa: mts_drop of request msg

2018년 1월 20일 17:15:18.273935 aaa: aaa_req는 비워져야 합니다.

2018년 1월 20일 17:15:18.280416 aaa: aaa_process_fd_set

2018 Jan 20 17:15:18.280443 aaa: aaa_process_fd_set: aaa_q의 mtscallback

2018 Jan 20 17:15:18.280454 aaa: aaa_enable_info_config: aaa 로그인 오류 메시지에 대한 GET_REQ

2018 Jan 20 17:15:18.280460 aaa: 구성 작업의 반환 값을 다시 가져왔습니다. 알 수 없는 보안 항 목

관련 정보

TACACS/RADIUS 인증이 활성화된 경우 FX-OS cli의 Ethanalyzer 명령에서 비밀번호를 묻습니다. 이 동작은 버그로 인해 발생합니다.

버그 ID: <u>CSCvg87518</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.