Single-Sign-On & 종속 포털 인증을 위해 Active Directory와 Firepower 어플라이언스 통합 구성

목차
<u> </u>
사전 요구 사항
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
배경정보
<u>구성</u>
<u>1단계. Single-Sign-On용 Firepower 사용자 에이전트 구성</u>
<u>2단계. FMC(Firepower 관리 센터)를 사용자 에이전트와 통합</u>
<u>3단계. Firepower를 Active Directory와 통합</u>
<u>3.1단계 영역 생성</u>
<u>3.2단계 디렉토리 서버 추가</u>
<u>3.3단계 영역 컨피그레이션 수정</u>
<u>3.4단계 사용자 데이터베이스 다운로드</u>
<u>4단계. ID 정책 구성</u>
<u>4.1단계 종속 포털(활성 인증)</u>
<u>4.2단계 Single-Sign-On(수동 인증)</u>
<u>5단계. 액세스 제어 정책 구성</u>
<u>6단계. 액세스 제어 정책 구축</u>
<u>7단계, 사용자 이벤트 및 연결 이벤트 모니터링</u>
<u>확인 및 문제 해결</u>
<u>FMC와 사용자 에이전트 간의 연결 확인(수동 인증)</u>
FMC와 Active Directory 간의 연결 확인
<u>firepower 센서와 엔드 시스템 간의 연결 확인(활성 인증)</u>
<u>정책 구성 및 정책 배포 확인</u>
<u>이벤트 로그 분석</u>
<u>관련 정보</u>

소개

이 문서에서는 종속 포털 인증(액티브 인증) 및 단일 로그인(패시브 인증)의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Sourcefire Firepower 디바이스
- 가상 디바이스 모델
- LDAP(Light Weight Directory Service)
- Firepower 사용자 에이전트

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC(firepower Management Center) 버전 6.0.0 이상
- Firepower 센서 버전 6.0.0 이상

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.

배경 정보

종속 포털 인증 또는 활성 인증은 로그인 페이지를 표시하고 인터넷 액세스를 얻기 위해 호스트에 대한 사용자 자격 증명이 필요합니다.

Single-Sign-On 또는 Passive Authentication은 여러 사용자 자격 증명 발생 없이 네트워크 리소스 및 인터넷 액세스에 대해 사용자에게 원활한 인증을 제공합니다. Single-Sign-on 인증은 Firepower 사용자 에이전트 또는 NTLM 브라우저 인증을 통해 수행할 수 있습니다.

💊 참고: 종속 포털 인증의 경우 어플라이언스는 라우팅 모드여야 합니다.

구성

1단계. Single-Sign-On용 Firepower 사용자 에이전트 구성

이 문서에서는 Windows 시스템에서 Firepower 사용자 에이전트를 구성하는 방법에 대해 설명합니다.

Sourcefire 사용자 에이전트 설치 및 제거

2단계. FMC(Firepower 관리 센터)를 사용자 에이전트와 통합

Firepower Management Center에 로그인하고 System > Integration > Identity Sources로 이동합니 다. New Agent(새 에이전트) 옵션을 클릭합니다. User Agent 시스템의 IP 주소를 구성하고 Add(추 가) 버튼을 클릭합니다.

변경 사항을 저장하려면 Save(저장) 버튼을 클릭합니다.

Overview /	Analysis	Policies Devices	Objects AN	1P							Deploy	A Sy	rstem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses v	Health v	Monitoring •	Tools •
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Softwar	e Satellite								
											You have unsave	d changes	Cancel	Save
Identity Se	ources													
Service Type		None	Identity Services	Engine User Ager	nt									
						New Agent								
Host Name	User /	Agent			? ×									
	Host	Name/IP Address 192.1	168.10.11											
			(Add Cano	el									

3단계. Active Directory와 Firepower 통합

3.1단계 영역 생성

FMC에 로그인하고 System > Integration > Realm으로 이동합니다. Add New Realm(새 영역 추가) 옵션을 클릭합니다.

이름 및 설명: 영역을 고유하게 식별하는 이름/설명을 지정합니다.

유형: AD

AD 주 도메인: Active Directory의 도메인 이름

디렉토리 사용자 이름: <username>

디렉터리 암호: <password>

Base DN: 시스템이 LDAP 데이터베이스에서 검색을 시작하는 도메인 또는 특정 OU DN입니다.

그룹 DN: 그룹 DN

그룹 특성: 멤버

		_			C	Configurat	tion Users	Domains	Integr	ration Updates	Licenses 🔻	He	alth 🔻	Monitorin	g ▼ Tools ▼
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Sa	tellite									
					Add New Realm						?	×	Company	e realms	O New realm
Name				Description	Name *		Servertest					•	e	State	
servertest-1					Description							11			± 🥒 🛅 🗊
					Type *		AD		*						
					AD Primary Domain	•	servertest.com		ex:	: domain.com		11			
					Directory Usernam	e *	servertest\admin		ex:	<: user@domain		11			
					Directory Password	••	•••••					11			
					Base DN *		dc=servertest,dc	=com	exc	c: ou=user,dc=cisco,dc=	com	11			
					Group DN *		cn=TAC,ou=Secu	irity-Team,dc=:	en ex:	c: ou=group,dc=cisco,do	=com	11			
					Group Attribute		Member		~						
					• Required Field										
										ОК	Cancel				

이 문서는 기본 DN 및 그룹 DN 값을 확인하는 데 도움이 됩니다.

<u>Active Directory LDAP 개체 특성 식별</u>

3.2단계 디렉토리 서버 추가

다음 단계로 이동하려면 Add(추가) 버튼을 클릭한 다음 Add directory(디렉토리 추가) 옵션을 클릭 합니다.

호스트 이름/IP 주소: AD 서버의 IP 주소/호스트 이름을 구성합니다.

포트: 389 (Active Directory LDAP 포트 번호)

암호화/SSL 인증서: (선택 사항) FMC와 AD 서버 간의 연결을 암호화하려면 다음을 참조하십시오.

문서: <u>FireSIGHT System에서 Microsoft AD Authentication Over SSL/TLS의 인증 객체 확인</u>

Overvie	ew Analysis Po	licies Devices Objects A	мр						Deploy	A Sys	stem Help v	admin 🔻
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
Serve	ertest										Save (🔀 Cancel
Enter a de	escription											
Director	y Realm Configur	ation User Download										
	Edit directory		? ×								0	Add directory
URL (Hos	Hostname / IP	102 168 10 11						Encryptio	on			
192.168.1	Address	192.100.10.11						none			6	28
	Port	389										
	Encryption	STARTTLS LDAPS None										
	SSL Certificate	· 0										
		ок	Test Cancel									

FMC가 AD 서버에 연결할 수 있는지 확인하려면 Test(테스트) 버튼을 클릭합니다.

3.3단계 영역 컨피그레이션 수정

AD 서버의 통합 컨피그레이션을 확인하려면 Realm Configuration(영역 컨피그레이션)으로 이동하고 AD 컨피그레이션을 수정할 수 있습니다.

3.4단계 사용자 데이터베이스 다운로드

AD 서버에서 사용자 데이터베이스를 가져오려면 User Download(사용자 다운로드) 옵션으로 이동 합니다.

사용자 및 그룹 다운로드를 다운로드하고 FMC가 AD에 연결하여 사용자 데이터베이스를 다운로드 하는 빈도에 대한 시간 간격을 정의하려면 이 확인란을 활성화합니다.

그룹을 선택하고 인증을 구성하려는 Include 옵션에 추가합니다.

Directory Realm Configuration User Download			
Download users and groups Begin automatic download at 12 AM America/New York Repeat Every 24 Lag Download Now	Hours		
Available Groups 😋	Groups to Include (1)	Groups to Exclude (0)	
Search by name Ad Inc Ad Exc	d to uude	None	
	Enter User Inclusion	Add Enter User Exclusion	Add

이미지에 표시된 대로 AD 상태를 활성화합니다.

Overview Analysis Po	olicies Devices C	bjects AM	Р					Deploy	₽ ₁ Sy	stem He	p∓ admin∓
Dashboards Reporting	Summary •										
Cisco CSI Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Satellit	te						
									Comp	are realms	New realm
Name			Description	Domain	Туре	Base DN	Group DN	Group Attribu	te	State	
servertest-1				Global	AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tea	n member			ቲ 🥒 🛅 🖯

4단계. ID 정책 구성

ID 정책은 사용자 인증을 수행합니다. 사용자가 인증하지 않으면 네트워크 리소스에 대한 액세스가 거부됩니다. 이렇게 하면 조직의 네트워크 및 리소스에 RBAC(Role-Based Access Control)가 적용 됩니다.

4.1단계 종속 포털(활성 인증)

활성 인증에서는 브라우저에서 사용자 이름/비밀번호를 요청하여 모든 연결을 허용할 사용자 ID를 식별합니다. 브라우저에서 인증 페이지로 사용자를 인증하거나 NTLM 인증으로 자동으로 인증합 니다. NTLM은 웹 브라우저를 사용하여 인증 정보를 보내고 받습니다. Active Authentication(액티 브 인증)에서는 다양한 유형을 사용하여 사용자의 ID를 확인합니다. 다양한 인증 유형은 다음과 같 습니다.

- 1. HTTP Basic: 이 방법에서는 브라우저가 사용자 자격 증명을 묻는 메시지를 표시합니다.
- 2. NTLM: NTLM은 Windows 워크스테이션 자격 증명을 사용하여 웹 브라우저를 통해 Active Directory와 협상합니다. 브라우저에서 NTLM 인증을 활성화해야 합니다. 사용자 인증은 자격 증명에 대한 프롬프트 없이 투명하게 수행됩니다. 사용자에게 단일 로그인 경험을 제공합니다
- 3. HTTP Negotiate:이 유형에서는 시스템이 NTLM으로 인증을 시도합니다. 실패하면 센서는 HTTP 기본 인증 유형을 대체 방법으로 사용하고 사용자 자격 증명에 대한 대화 상자를 표시 합니다.
- 4. HTTP Response(HTTP 응답) 페이지: 이 페이지는 HTTP 기본 유형과 유사하지만 사용자 정

의할 수 있는 HTML 형식으로 인증을 입력하라는 메시지가 사용자에게 표시됩니다.

각 브라우저에는 NTLM 인증을 활성화하는 특정 방법이 있으므로 NTLM 인증을 활성화하기 위해 브라우저 지침을 준수합니다.

라우티드 센서와 자격 증명을 안전하게 공유하려면 ID 정책에 자체 서명 서버 인증서 또는 공개 서 명 서버 인증서를 설치해야 합니다.

Generate a simple self-signed certificate using openSSL -

- Step 1. Generate the Private key openssl genrsa -des3 -out server.key 2048

Policies(정책) > Access Control(액세스 제어) > Identity(ID)로 이동합니다. Add Policy(정책 추가)를 클릭하고 정책에 이름을 지정한 다음 저장합니다.

Overview Analysis Policies Devices Obj	ects AMP			Deploy 🛕 System Help 🔻 admin 🔻
Access Control > Identity Network Discovery	Application Detectors Correl	elation Actions 🔻		
				Object Management Access Control
				Compare Policies New Policy
Identity Policy	Domain	Statu	s Las	Modified
	New Io	Identity policy ? ×	Add a new policy	
	Name	e Identity_Policy	nud a new poney	
	Descrip	ription		
		Save Cancel		

Active Authentication(활성 인증) 탭으로 이동하고 Server Certificate(서버 인증서) 옵션에서 아이콘 (+)을 클릭하고 openSSL을 사용하여 이전 단계에서 생성한 인증서 및 개인 키를 업로드합니다.



이제 Add rule(규칙 추가) 버튼을 클릭하고 규칙에 이름을 지정한 다음 작업을 Active Authentication(활성 인증)으로 선택합니다. 사용자 인증을 활성화하려는 소스/대상 영역, 소스/대상

네트워크를 정의합니다.

이전 단계에서 구성한 Realm(영역)과 사용자 환경에 가장 적합한 인증 유형을 선택합니다.

Overview Analysis Polic Access Control > Identity	Devices Objects AMP Devices Objects Correlation Actions • Devices Devices	ployASystem Help v admin v
Identity_Policy		Save Cancel
Rules Active Authentication		Count Balan
	Add Rule	? ×
# Name	Name Captive_Portal 🗹 Enabled Insert into Category 🌱 Standard Rules	✓ Auth Type
Administrator Rules	Action Active Authentication V Realm: Servertest (AD) Authentication Type: HTTP Negotiate Exclude HTTP User-Agents: None	
This category is empty	Zanas Naturalis 18 AN Zana Danta	
Standard Rules This category is empty Root Rules This category is empty	Zones Networks VLAN lags Ports Realm * Servertest (AD) V Image: Constraint of the servertest (AD) Identify as Special Identities/Guest if authentication cannot identify user Authentication Type HTTP Negotiate Audication Filters c Available Applications (83) c Exclude HTTP User-Agents (0)	
	Search by name Search by name	

종속 포털에 대한 ASA 컨피그레이션

ASA Firepower 모듈의 경우, 종속 포털을 구성하기 위해 ASA에서 이러한 명령을 구성합니다.

ASA(config)# captive-portal global port 1055

서버 포트, TCP 1055가 ID 정책 활성 인증 탭의 포트 옵션에서 구성되었는지 확인합니다.

활성 규칙 및 적중 횟수를 확인하려면 다음 명령을 실행합니다.

ASA# show asp table classify domain captive-portal

♥ 참고: 종속 포털 명령은 ASA 버전 9.5(2) 이상에서 사용할 수 있습니다.

4.2단계 Single-Sign-On(수동 인증)

수동 인증에서는 Firepower 사용자가 로그인하고 AD를 인증할 수 있는 경우 도메인 사용자 에이전 트가 AD의 보안 로그에서 사용자-IP 매핑 세부사항을 폴링하고 이 정보를 FMC(Firepower 관리 센 터)와 공유합니다. FMC는 액세스 제어를 시행하기 위해 이러한 세부 정보를 센서로 전송합니다.

Add rule(규칙 추가) 버튼을 클릭하고 규칙에 이름을 지정한 다음 Action as Passive Authentication(수동 인증으로 작업)을 선택합니다. 사용자 인증을 활성화하려는 소스/대상 영역, 소 스/대상 네트워크를 정의합니다. 이전 단계에서 구성한 Realm(영역)과 이 이미지에 표시된 대로 환경에 가장 적합한 인증 유형을 선택합니다.

패시브 인증이 사용자 ID를 식별할 수 없는 경우 여기서 Active 인증으로 폴백 방법을 선택할 수 있 습니다.



5단계. 액세스 제어 정책 구성

Policies(정책) > Access Control(액세스 제어) > Create/Edit a Policy(정책 생성/수정)로 이동합니다

ID 정책(왼쪽 상단 모서리)을 클릭하고 이전 단계에서 구성한 ID 정책을 선택한 다음 이 이미지에 표 시된 대로 OK(확인) 버튼을 클릭합니다.

Overview Analysis Policie	es Devices Objects	AMP		Deploy	🌒 🖣 System Help 🔻 admin 🔻
Access Control > Access Contr	ol Network Discovery	Application Detectors	Correlation	Actions 🔻	
NGFW_Policy				Show 1	Warnings 📄 Save 🛛 🔀 Cancel
Identity Policy: None	SSL Policy: None				
	Identity Policy		? ×	Tankeritano	ce Settings 🗒 Policy Assignments (1)
Rules Security Intelligence General Settings	Identity_Policy		• @	insport/Network Layer Preprocessor Settings	0
Maximum URL characters to sto	Revert to Defaults	ок	Cancel	nore the VLAN header when tracking connections	No

새 규칙을 추가하려면 Add rule(규칙 추가) 버튼을 클릭합니다. Users(사용자)로 이동하고 이 이미 지에 표시된 대로 액세스 제어 규칙이 적용되는 사용자를 선택합니다. 변경 사항을 저장하려면 OK(확인)를 클릭하고 Save(저장)를 클릭합니다.

Overview Anal	ysis Policies	Devices Objects	AMP					Deploy	🛕 System	Help 🔻 adı	nin 🔻
Access Control >	Access Control	Network Discovery	Application Detectors	Correlation	Actions 🔻						
NGFW Polic	CV									ave 🛛 🔀 C	ancel
Enter a description	<i>'</i>										
Identity Policy: Ide	ntity_Policy	SSL Policy: None									
Rules Securit	Editing Rule -	Allow_LAN_User							? ×	y Assignmen	ts (1)
# Filter by Devic	Name Allow_LA	AN_User		Enabled	Move	1					×
# Name	Action	v	▼ IPS: no po	licies Variables	: n/a Files: no inspe	ection Logging	: connections: Event	/iewer			
👻 Mandatory - I	Zones Net	works VLAN Tags	Users Applications	Ports URLs	🛕 ISE Attributes		Inspection	Logging	Comments		
	Available Realms	s Ċ	Available Users	Ċ		S	Selected Users (2)				0 0
1 Allow_LAN_U	Search by nar	me or value	Search by nam	e or value			Servertest/sunil			U	<i>v</i> 0
🗢 Default - NGF	f Special Identi	ities					Servertest/admin		8		
2 IPS_test	Servertest									0	08
Default Action						Add to Dute				~	5 🔳
								ок	Cancel		

6단계. 액세스 제어 정책 구축

Deploy(구축) 옵션으로 이동하여 Device(디바이스)를 선택하고 Deploy(구축) 옵션을 클릭하여 컨피 그레이션 변경 사항을 센서로 푸시합니다. 메시지 센터 아이콘(구축 및 시스템 옵션 사이의 아이콘) 옵션에서 정책의 구축을 모니터링하고 이 이미지에 표시된 대로 정책이 성공적으로 적용되어야 하 는지 확인합니다.

		Deploy 🔒 A3 Syste	em Help v admin v
C Dep	DIOY Policies Version: 2015-12-10 09:29 PM		? ×
	Device	Group	Current Version
	NGFW		2015-12-10 09:14 PM
5	 NGFW Settings: NGFW Access Control Policy: NGFW_Policy -Intrusion Policy: Balanced Security and Connectivity -Intrusion Policy: No Rules Active -Identity Policy: Identity_Policy DNS Policy: Default DNS Policy Network Discovery Device Configuration (Details) 		
	Selected devices: 0		Deploy Cancel

7단계. 사용자 이벤트 및 연결 이벤트 모니터링

현재 활성화된 사용자 세션은 Analysis(분석) > Users(사용자) > Users(사용자) 섹션에서 사용할 수 있습니다.

User Activity Monitoring(사용자 활동 모니터링)은 어떤 사용자가 어떤 IP 주소와 연결되었는지, 그 리고 사용자가 액티브 또는 패시브 인증에 의해 시스템에 의해 어떻게 탐지되었는지를 파악하는 데 도움이 됩니다. Analysis(분석) > Users(사용자) > User Activity(사용자 활동)

User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

	<u>▼ Time</u> ×	Event ×	<u>Realm</u> ×	<u>Username</u> ×	<u>Type</u> ×	Authentication X Type	<u>IP Address</u> ×
4	2015-12-10 11:15:34	<u>User Login</u>	<u>Servertest</u>	📑 <u>sunil</u>	LDAP	Active Authentication	192.168.20.20
4	2015-12-10 10:47:31	<u>User Login</u>	<u>Servertest</u>	📇 <u>admin</u>	LDAP	Passive Authentication	<u>192.168.0.6</u>

Analysis(분석) > Connections(연결) > Events(이벤트)로 이동하여 사용자가 사용하는 트래픽 유형 을 모니터링합니다.

Overview Analysis Policies Devices Objects AMP Deploy 👍 System Help + admin											admin 🔻	
Co	ntext E	xplorer Connectio	ns F Events Intr	usions 🔻 🛛 Fi	les 🕶 Hosts 💌	Users • Vulnerabilities •	Correlation • Cus	tom • Search				
								Bookmark	This Page Report Designer Da	shboard View Bookmarks	Search 🔻	
	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events Expanding Example Contractions (Edit Search Save Search)											
1	ump to.	•	ave search)							Chain	indu columna	
			Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder IP ×	Access Control Rule	× Ingress Interface ×	Egress Interface ×	Count	
4		2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1	
4		2015-12-11 10:31:59		Allow	192.168.20.20	📙 sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1	
- 4		2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1	
-8		2015-12-11 09:46:28		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1	
4		2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1	
4		2015-12-11 09:46:07		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1	
4	0	2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1	
Last login on Thursday, 2015-12-10 at 11:17:25 AM from 10.65.39.165 R]pht-click for menu											allada	

확인 및 문제 해결

트래픽 흐름과 관련된 사용자 인증/인증 유형/사용자-IP 매핑/액세스 규칙을 확인하려면 Analysis > Users로 이동합니다.

FMC와 사용자 에이전트 간의 연결 확인(수동 인증)

FMC(firepower 관리 센터)는 TCP 포트 3306을 사용하여 사용자 에이전트로부터 사용자 활동 로그 데이터를 수신합니다.

FMC 서비스 상태를 확인하려면 FMC에서 이 명령을 사용합니다.

admin@firepower:~\$ netstat -tan | grep 3306

FMC에서 패킷 캡처를 실행하여 User Agent와의 연결을 확인합니다.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 3306

FMC가 User Agent로부터 사용자 로그인 세부 정보를 수신하는지 여부를 확인하려면 Analysis > Users > User Activity로 이동합니다.

FMC와 Active Directory 간의 연결 확인

FMC는 TCP 포트 389를 사용하여 Active Directory입니다.

FMC에서 패킷 캡처를 실행하여 Active Directory와의 연결을 확인합니다.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 389

FMC 영역 컨피그레이션에 사용된 사용자 자격 증명에 AD 사용자 데이터베이스를 가져올 수 있는 충분한 권한이 있는지 확인하십시오.

FMC 영역 컨피그레이션을 확인하고 사용자/그룹이 다운로드되고 사용자 세션 시간 초과가 올바르 게 구성되었는지 확인합니다.

Message Center(메시지 센터) > Tasks(작업)로 이동하여 이 이미지에 표시된 대로 작업 사용자/그 룹 다운로드가 성공적으로 완료되었는지 확인합니다.

	Deploy 🖲 System Help admin
Deployments 🔥 Health 🕕 Tasks	Ø ?
20+ total 0 waiting 0 running 0 ret	rying 20+ success 1 failure
 LDAP Download - Global Download users/groups from servert successful: 1 groups, 0 users downloaded 	2s ×
 LDAP Download - Global Download users/groups from servert successful: 1 groups, 5 users downloaded 	4m 52s ×

firepower 센서와 엔드 시스템 간의 연결 확인(활성 인증)

활성 인증의 경우 인증서 및 포트가 FMC ID 정책에서 올바르게 구성되었는지 확인합니다. 기본적 으로 Firepower 센서는 활성 인증을 위해 TCP 포트 885에서 수신 대기합니다.

정책 구성 및 정책 배포 확인

Realm(영역), Authentication type(인증 유형), User agent(사용자 에이전트) 및 Action(작업) 필드가 ID 정책에서 올바르게 구성되었는지 확인합니다.

ID 정책이 액세스 제어 정책과 올바르게 연결되었는지 확인합니다.

Message Center(메시지 센터) > Tasks(작업)로 이동하여 정책 구축이 성공적으로 완료되었는지 확 인합니다.

이벤트 로그 분석

연결 및 사용자 활동 이벤트를 사용하여 사용자 로그인의 성공 여부를 진단할 수 있습니다.이러한 이벤트

플로우에 어떤 액세스 제어 규칙이 적용되는지 확인할 수도 있습니다.

Analysis(분석) > User(사용자)로 이동하여 사용자 이벤트 로그를 확인합니다.

Analysis(분석) > Connection Events(연결 이벤트)로 이동하여 연결 이벤트를 확인합니다.

관련 정보 · 기술 지원 및 문서 - Cisco Systems 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.