シングルサインオン&キャプティブポータル認証 用のActive DirectoryとFirepowerアプライアンス の設定

内容
<u>はじめに</u>
<u>前提条件</u>
要件
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u> ステップ 1:シングルサインオン用のFirepowerユーザエージェントの設定</u>
<u>ステップ 2:firepower Management Center(FMC)とUser Agentの統合</u>
<u>ステップ3:FirepowerとActive Directoryの統合</u>
<u>手順 3.1 レルムの作成</u>
<u>手順 3.2 ディレクトリ サーバの追加</u>
<u>手順 3.3 レルム設定の変更</u>
<u>手順 3.4 ユーザ データベースのタウンロード</u>
<u>手順 4.1 キャフティフ ホータル(アクティフ認証)</u> モ順 4.2 シン・グリサイン・オン・ノ パッシュブ記証)
<u>士順42フノノルリイフオン(ハッフノ認証)</u> フテップ5・アクセスコントロールポリシーの設定
手順6:アクセスコントロールホリシーの導入
<u>手順7:ユーザイベントと接続イベントの監視</u>
<u>確認とトラフルシューティング</u>
<u>FMC とユーザ エージェントの間の接続の確認(パッシブ認証)</u>
<u>FMC と Active Directory の間の接続の確認</u>
<u>Firepower センサーとエンド システムの間の接続の確認(アクティブ認証)</u>
<u>ポリシー設定とポリシー展開の確認</u>
<u>イベント ログの分析</u>
<u>関連情報</u>

はじめに

このドキュメントでは、キャプティブ ポータル認証(アクティブ認証)とシングルサインオン (パッシブ認証)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Sourcefire Firepower デバイス
- ・ バーチャル デバイス モデル
- Light Weight Directory Service (LDAP)
- Firepower ユーザ エージェント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Center(FMC)バージョン6.0.0以降
- Firepowerセンサーバージョン6.0.0以降

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

背景説明

キャプティブ ポータル認証またはアクティブ認証では、ログイン ページが表示され、ホストがイ ンターネットにアクセスするためにユーザ クレデンシャルが必要になります。

シングルサインオンまたはパッシブ認証は、ネットワークリソースおよびインターネットアクセ スに関して、ユーザのクレデンシャルが複数回発生することなく、シームレスな認証をユーザに 提供します。シングルサインオン認証は、Firepower ユーザ エージェントまたは NTLM ブラウザ 認証のいずれかによって実現できます。

💊 注:キャプティブポータル認証の場合、アプライアンスはルーテッドモードである必要があります。

設定

ステップ1:シングルサインオン用のFirepowerユーザエージェントの設定

次の記事では Windows マシンで Firepower ユーザ エージェントを設定する方法について説明しています。

Sourcefire ユーザ エージェントのインストールとアンインストール

ステップ 2: firepower Management Center(FMC)とUser Agentの統合

Firepower Management Center にログインし、[System] > [Integration] > [Identity Sources] の順に 移動します。 [New Agent] オプションをクリックします。ユーザ エージェント システムの IP ア ドレスを設定して [Add] ボタンをクリックします。 [Save] ボタンをクリックして変更内容を保存します。

Overview	Analysis	Policies Devices	Objects AM	1P							Deplo	y 🗛 Sy	rstem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses v	Health •	Monitoring •	Tools •
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Softwa	are Satellite								
											You have unsave	d changes	Cancel	Save
Identity S	ources													
Service Type		None	Identity Services	Engine User Ag	lent	A New Acces								
Host Name	/IF User /	Agent			? ×	I New Agent								
	Host	Name/IP Address 192.1	68.10.11											
			(Add Ca	ncel									

ステップ3: FirepowerとActive Directoryの統合

手順 3.1 レルムの作成

FMC にログインして [System] > [Integration] > [Realm] の順に移動します。[Add New Realm] オ プションをクリックします。

名前と説明:レルムを一意に識別するための名前と説明を指定します。

タイプ:AD

ADプライマリドメイン: Active Directoryのドメイン名

ディレクトリユーザ名: <username>

ディレクトリパスワード: <password>

ベースDN:システムがLDAPデータベースでの検索を開始するドメインまたは特定のOU DN。

グループDN:グループDN

グループ属性:メンバー

					Configu	ration Users	Domains	Int	tegration Updates	Licenses •	H	ealth 🔻 🛛 M	onitoring	y ▼ Tools ▼
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Satellite									
					Add New Realm					?	×	Compare r	ealms	New realm
Name				Description	Name *	Servertest						e St	ate	
servertest-1					Description							G		5 / 🗅 🖥
					Type *	AD		~						
					AD Primary Domain *	servertest.com			ex: domain.com					
					Directory Username *	servertest\admir	n		ex: user@domain					
					Directory Password *	•••••								
					Base DN *	dc=servertest,de	c=com		ex: ou=user,dc=cisco,	dc=com				
					Group DN *	cn=TAC,ou=Sec	urity-Team,dc=	ser	ex: ou=group,dc=cisco	o,dc=com	. 1			
					Group Attribute	Member		*						
					* Required Field									
									ок	Cancel				

次の記事は、ベース DN およびグループ DN の値を決めるのに役立ちます。

<u>Active Directory LDAP オブジェクトの属性の特定</u>

手順 3.2 ディレクトリ サーバの追加

次の手順に進むために [Add] ボタンをクリックし、[Add directory] オプションをクリックします。

Hostname/IP Address:ADサーバのIPアドレス/ホスト名を設定します。

ポート: 389 (Active Directory LDAPポート番号)

暗号化/SSL証明書: (オプション)FMCとADサーバ間の接続を暗号化するには、

記事:<u>FireSIGHTシステムでのSSL/TLSを介したMicrosoft AD認証のための認証オブジェクトの検</u> 証

Overvie	ew Analysis Po	licies Devices Objects AM	1P						Deploy	A Sys	stem Help 🔻	admin 🔻
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
Serve Enter a de	ertest escription								Save (Cancel		
Director	y Realm Configur	ation User Download										
	Edit directory		? ×								0	Add directory
URL (Hos	Hostname / IP	192 168 10 11						Encryptic	on			
192.168.1	Address	172.100.10.11						none			6	8 8
	Port	389										
	Encryption	STARTTLS LDAPS None										
	SSL Certificate	▼ ○										
		ок	Test Cancel									

FMC が AD サーバに接続できるかどうかを確認するには、[Test] ボタンをクリックします。

手順 3.3 レルム設定の変更

AD サーバの統合設定を確認したり AD の設定を変更したりするには、[Realm Configuration] に移動します。

手順 3.4 ユーザ データベースのダウンロード

AD サーバからユーザ データベースを取得するために、[User Download] オプションに移動します。

[Download users and groups] チェックボックスをオンにしてダウンロードを有効にし、ユーザ デ ータベースをダウンロードするために FMC が AD に接続する頻度を時間間隔で定義します。

認証を設定するグループを選択し、[include] オプションに追加します。

Directory Realm Configuration User Download		
✓ Download users and groups		
Begin automatic download at 12 V AM V America/New York Repeat Every 24 V	Hours	
Available Groups 😋	Groups to Include (1)	Groups to Exclude (0)
Search by name	🛃 TAC	None
A TAC		
Add to Include		
	Enter User Inclusion Add	Enter User Exclusion Add

図に示すように、AD の状態を有効にします。

Overview Analysis P	olicies Devices (Objects AM	Р					Deploy	0 ₁ Sy	stem He	lp v admin v
Dashboards • Reporting	g Summary 🔻										
Cisco CSI Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Sa	tellite						
									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	member			ቲ 🥒 🛅 🖯

ステップ 4:

アイデンティティ ポリシーはユーザ認証を実行します。ユーザが認証されないと、ネットワーク リソースへのアクセスが拒否されます。ポリシーを設定すると、ロールベース アクセス コントロ ール(RBAC)が組織のネットワークとリソースに適用されます。

手順 4.1 キャプティブ ポータル(アクティブ認証)

アクティブ認証は、ブラウザでユーザ名とパスワードの入力を求め、ユーザIDを特定して接続を 許可します。 ブラウザは、認証ページを使用してユーザを認証するか、NTLM認証を使用してサ イレントモードで認証します。 NTLM は、Web ブラウザを使用して、認証情報を送受信します 。アクティブ認証は、さまざまな方式を使用してユーザのアイデンティティを確認します。認証 の方式は次のとおりです。

- 1. HTTP Basic:この方法では、ブラウザはユーザクレデンシャルの入力を求めます。
- NTLM:NTLMはWindowsワークステーションクレデンシャルを使用し、Webブラウザを介し てActive Directoryとネゴシエートします。ブラウザで NTLM 認証を有効にする必要があり ます。ユーザ認証は、クレデンシャルのプロンプトなしで透過的に行われます。ユーザにシ ングルサインオン環境を提供します。
- 3. HTTPネゴシエーション:このタイプでは、システムはNTLMによる認証を試行します。失 敗した場合、センサーはフォールバック方式としてHTTP Basic認証タイプを使用し、ユー ザクレデンシャルの入力を求めるダイアログボックスを表示します。
- 4. HTTP応答ページ:これはHTTP基本タイプに似ていますが、このページでは、カスタマイ

ズ可能なHTMLフォームに認証を入力するように求められます。

各ブラウザにはNTLM認証を有効にする固有の方法があるため、NTLM認証を有効にするにはブラ ウザのガイドラインに従います。

ルーテッド センサーとクレデンシャルを安全に共有するには、自己署名サーバ証明書または公開 署名サーバ証明書をアイデンティティ ポリシーにインストールする必要があります。

Generate a simple self-signed certificate using openSSL -

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

[Policies] > [Access Control] > [Identity] の順に移動します。[Add Policy] をクリックし、ポリシー に名前を付けて保存します。

Overview Analysis Policies Devices Obj	ects AMP			Deploy 🛕 System Help 🔻 admi	in 🔻
Access Control > Identity Network Discovery	Application Detectors Correlation	Actions •			
				Object Management Access Con	trol
				Compare Policies New Po	olicy
Identity Policy	Domain	Statu	•	Last Modified	
	New Iden Name Description	Identity_Policy ? ×	Add a new policy		
		Save Cancel			

Active Authenticationタブに移動し、Server Certificateオプションでアイコン(+)をクリックし、 openSSLで前の手順で生成した証明書と秘密キーをアップロードします。



[Add rule] ボタンをクリックしてルールの名前を指定し、アクションとして [Active Authentication] を選択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信元/宛先ネットワ [Realm] で前の手順で設定したレルムを選択し、環境に適した認証タイプを選択します。

Identity_Policy Ever a description Rules Active Authentication Inser Add Rule Inser Insert into Category Insert Rules Auth Type Action Active Authentication Insert into Category Insert Rules Auth Type Insert Rules Auth Type Insert Rules Realm & Secretest (AD) Insert Rules Realm & Secretest (AD) Insert Rules Insert Rules This category is empty Realm & Secretest (AD) Rule Authentication Type IntTP Regulate Identifies/Guest if authentication cannot identify user Application Filters Available Applications (B3) Insert Prove Page Realm Active Authentication Cancel Packaging Tool Interview Identifies Active Active Packaging Tool Interview Identified Active Identified Interview Identified Active Identified	Overview Analysis Polic Access Control + Identity	Cies Devices Objects AMP Network Discovery Application Detectors Correlation Actions -	Deploy 🛕 System Help 🕶 admin 🗸
Rules Add Rule ? × Name Add Rule ? × Name Regive_Portal Insert into Category * Standard Rules * This category is empty: Standard Rules ? × Auth Type Standard Rules ? × Realm & Servertest (AD) Authentication Type : HTTP Negotiate Exclude HTTP User-Agents: None This category is empty: Realm * Servertest (AD) * * * This category is empty: Realm * Servertest (AD) * * This category is empty: Realm * Servertest (AD) * * This category is empty: Realm * Servertest (AD) * * This category is empty: Realm * Servertest (AD) * * Authentication Type HTTP Negotiate * * * Application Filters * Available Applications (83) * Exclude HTTP User-Agents (0) * * * * Addebealing * # * Realm * Sected by name * # * * Realered Field * *	Identity_Policy Enter a description		Save Cancel
Add Rule ? × Addinistrator Rules Name Captive_Portal Action Active Authentication Realm © Enabled This category is empty Standard Rules Standard Rules Zones Networks VLAN Tags Ports Realm * Servertest (AD) Root Rules	Rules Active Authentication		a the and a second gules
Standard Rules Zones Networks VLAN Tags Ports Realm & Settings This category is empty Realm * Servertest (AD) V Image: Control of the co	# Name Administrator Rules This category is empty	Add Rule Name Captive_Portal Action Active Authentication Y Realm: Servertest (AD) Authentication Type: HTTP Negotiate Exclude F	? × Standard Rules × Auth Type ITTP User-Agents: None
	Standard Rules This category is empty Root Rules This category is empty	Zones Networks VLAN Tags Ports Realm * Servertest (AD) Servertest (AD) Identify as Special Identifies/Guest if authentication cannot identify user Authentication Type HTTP Negotiate Available Applications (83) ¢ Exclude HT Search by name Search by name ABC Advanced Packaging Tool Medium AirPlay Amazon Instant Video Required Field 	Realm & Settings TP User-Agents (0)

キャプティブ ポータル用の ASA の設定

ASA Firepower モジュールについて、キャプティブ ポータルを設定するために ASA で次のコマ ンドを設定します。

ASA(config)# captive-portal global port 1055

アイデンティティポリシーのアクティブ認証タブのportオプションで、サーバポートTCP 1055が 設定されていることを確認します。

アクティブなルールとそのヒットカウントを確認するには、次のコマンドを実行します。

ASA# show asp table classify domain captive-portal

💊 注:キャプティブポータルコマンドは、ASAバージョン9.5(2)以降で使用できます。

手順 4.2 シングルサインオン(パッシブ認証)

パッシブ認証では、ドメイン ユーザがログインして、AD の認証を行うことができる場合、 Firepower ユーザ エージェントは AD のセキュリティ ログからユーザと IP のマッピングの詳細 情報をポーリングし、この情報を Firepower Management Center(FMC)と共有します。FMC はアクセス制御を強化するために、その詳細情報をセンサーに送信します。 [Add rule] ボタンをクリックしてルールの名前を指定し、[Action] で [Passive Authentication] を選 択します。ユーザ認証を有効にする送信元/宛先ゾーンと送信元/宛先ネットワークを定義します。

次の図に示すように、[Realm] で前の手順で設定したレルムを選択し、環境に適した認証タイプ を選択します。

フォールバック方法として、[Active authentication if passive authentication cannot identify the user identity] を選択できます。

Overview Analysis Policies Devices Objects AMP	elp 🔻 admin 🔻
Access Control > Identity Network Discovery Application Detectors Correlation Actions ▼	
Identity Policy You have unsaved changes	e 🛛 🔀 Cancel
Enter a description	
Rules Active Authentication	
Editing Rule - Captive_Portal ? ×	×
# Name Single Sing On California	h Type
Administrator Ruli	
This category is em	
Standard Rules Zones Networks VLAN Tags Ports Realm & Settings	
1 Captive_Portal Realm * Servertest V	P Negotiate 🥔 📋
Root Rules Use active authentication if passive authentication cannot identify user	
This category is em	
* Required Field	
Save Cancel	

ステップ 5:

[Policies] > [Access Control] > [Create/Edit a Policy] の順に移動します。

[Identity Policy] (左上隅)をクリックして、前の手順で設定したアイデンティティ ポリシーを選択し、[OK] をクリックします(次の図を参照)。

Overview Analysis Polici	i es Devices Objects	AMP		Deploy 🔍 System Help 🔻 admin 🔻
Access Control + Access Cont	rol Network Discovery	Application Detectors	Correlation	ctions •
NGFW_Policy				🔝 Show Warnings
Enter a description				
Identity Policy: None	SSL Policy: None			
	Identity Policy		? ×	Theritance Settings E Policy Assignments (1)
Rules Security Intelligence				
General Settings	Identity_Policy		× 6/	insport/Network Layer Preprocessor Settings
Maximum URL characters to sta	Revert to Defaults	OK	Cancel	nore the VLAN boarder when tracking connections

Add ruleボタンをクリックして、新しいルールを追加します。次の図に示すように、Usersに移動 し、アクセスコントロールルールが適用されるユーザを選択します。OKをクリックし、次に Saveをクリックして変更を保存します。

Overview Anal	vsis Policies	Devices Objects	AMP					Deploy	🛕 System H	Help ▼ a	dmin 🔻
Access Control >	Access Control	Network Discovery	Application Detectors	Correlation	Actions T						
NGFW_Polic	:y									ave 🛛 🕄	Cancel
Enter a description											
Identity Policy: Ide	ntity_Policy	SSL Policy: None									
Rules Securit	Editing Rule -	Allow_LAN_User							? ×	y Assignm	ents (1)
# Filter by Devic	Name Allow_LA	N_User		🗹 Enabled	Move						×
# Name	Action	(✓ IPS: no po	licies Variables	: n/a Files: no inspe	ection Logging: co	onnections: Event V	/iewer			
👻 Mandatory - I	Zones Net	works VLAN Tags	Users Applications	Ports URLs	🔺 ISE Attributes		Inspection	Logging	Comments		
1 Allow LAN L	Available Realms	s Ċ	Available Users	Ċ		Sele	ected Users (2)			R 0	0 B
I ANOW_DANY_O	Search by nar	me or value	Search by nam	e or value		8	Servertest/sunil		8	- ·	ø U
🗢 Default - NGF	Special Identi	ities				*	Servertest/admin		6		
2 IPS_test	Servertest									0	08
Default Action										~	\$ 📕
								ок	Cancel		

手順 6:

[Deploy] オプションに移動し、[Device] を選択して [Deploy] オプションをクリックします。これ によって設定の変更がセンサーにプッシュされます。[Message Center] アイコン([Deploy] オプ ションと [System] オプションの間のアイコン)によってポリシーの展開をモニタし、ポリシーが 正常に適用されたことを確認します(次の図を参照)。

		Deploy 🛕 Sys	stem Help 🔻 admin 🔻
C Deploy Policies Version:201	5-12-10 09:29 PM		? ×
Device		Group	Current Version
NGFW			2015-12-10 09:14 PM
Settings: NGFW			
D Access Control Policy: No	GFW_Policy		
- Intrusion Policy: Ba	anced Security and Connectivity		
- Intrusion Policy: No	Rules Active		
- Identity Policy: Iden	ntity_Policy		
ONS Policy: Default	DNS Policy		
Network Discovery			
Device Configuration (De	<u>tails)</u>		
Selected devices: 0			Deploy Cancel

手順7:ユーザモニタするイベントと接続のイベント

現在アクティブなユーザ セッションは、[Analysis] > [Users] > [Users] セクションで確認できます。

ユーザ アクティビティのモニタリングは、ユーザに関連付けられている IP アドレスの確認や、 アクティブ認証とパッシブ認証のいずれによってユーザがシステムに検出されたかの確認に役立 ちます。 [Analysis] > [Users] > [User Activity]

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 × 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 > Connections > Eventsの順に移動し、ユーザが使用するトラフィックのタイプを監視します。

Overview Analysis Policies Devices Objects AMP Deploy 🔺 System Help + admin									admin 🔻		
Cor	text E	xplorer Connectio	ns • Events Intru	sions 🔻 Fil	es 🔹 Hosts 👻	Users • Vulnerabilities •	Correlation • Cus	stom v Search			
								Bookmark Thi	s Page Report Designer Da	shboard View Bookmarks	Search •
Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events Expanding											
Search Constraints (Edit Search Save Search) Disabled Columns											
J	ump to.	•									
		✓ First Packet ×	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	i <u>192.168.20.20</u>	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
4		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		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 Right-olick for menu								alada			

確認とトラブルシューティング

[Analysis] > [Users] に移動し、トラフィック フローに関連付けられているユーザ認証、認証の種類、ユーザ IP マッピング、アクセス ルールを確認します。

FMC とユーザ エージェントの間の接続の確認(パッシブ認証)

ユーザ エージェントからユーザ アクティビティ ログ データを受信するために、Firepower Management Center (FMC)は TCP ポート 3306 を使用します。

FMC のサービス ステータスを確認するには、FMC で次のコマンドを使用します。

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

ユーザエージェントとの接続を確認するには、FMC でパケット キャプチャを実行します。

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

FMCがユーザエージェントからユーザログインの詳細を受信するかどうかを確認するには、 Analysis > Users > User Activityの順に移動します。

FMC と Active Directory の間の接続の確認

FMCはTCPポート389を使用して、ユーザデータベースを Active Directory.

Active Directory との接続を確認するには、FMC でパケット キャプチャを実行します。

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

FMCレルムの設定で使用されているユーザクレデンシャルに、ADユーザデータベースを取得する ための十分な権限があることを確認します。

FMC レルムの設定を調べて、ユーザまたはグループがダウンロードされること、およびユーザ セッションのタイムアウトが正しく設定されていることを確認します。

[Message Center] > [Tasks] に移動して、次の図に示すように、ユーザまたはグループのダウンロ ードのタスクが正常に完了していることを確認します。

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

Firepower センサーとエンド システムの間の接続の確認(アクティブ認証)

アクティブ認証の場合は、証明書とポートがFMCアイデンティティポリシーで正しく設定されて いることを確認します。デフォルトでは、FirepowerセンサーはTCPポート885でアクティブ認証 をリッスンします。

ポリシー設定とポリシー展開の確認

[Identity Policy] で [Realm]、[Authentication type]、[User agent]、[Action] の各フィールドが正し く設定されていることを確認します。

アイデンティティ ポリシーがアクセス コントロール ポリシーと正しく関連付けられていること を確認します。

[Message Center] > [Tasks] に移動して、ポリシーの展開が正常に完了したことを確認します。

イベント ログの分析

接続イベントとユーザアクティビティイベントは、ユーザログインが成功したかどうかを診断す るために使用できます。これらのイベントは、

どのアクセスコントロールルールがフローに適用されているかも確認できます。

[Analysis] > [User] に移動して、ユーザ イベント ログをチェックします。

[Analysis] > [Connection Events] に移動して、接続イベントをチェックします。

関連情報

・ テクニカル サポートとドキュメント - Cisco Systems

翻訳について

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