Ansibleを使用してFMCを設定し、FTDハイアベ イラビリティを作成します。

はじめに

このドキュメントでは、Firepower Management Center(FMC)を自動化して、AnsibleでFirepower Threat Defense(FTD)の高可用性を実現する手順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。

- アンサブル
- Ubuntuサーバ
- Cisco Firepower Management Center(FMC)仮想
- Cisco Firepower Threat Defense(FTD)仮想

このラボ環境では、AnsibleはUbuntuに導入されています。

この記事で参照されているAnsibleコマンドを実行するために、Ansibleがサポートするすべてのプ ラットフォームにAnsibleが正常にインストールされていることを確認する必要があります。

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。

Ubuntuサーバ22.04

- Ansible 2.10.8
- Python 3.10
- Cisco Firepower Threat Defense(FTD)仮想7.4.1
- Cisco Firepower Management Center(FMC)仮想7.4.1

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

Ansibleは汎用性の高いツールで、ネットワークデバイスの管理において大きな効果を発揮します 。Ansibleを使用して自動化されたタスクを実行するには、さまざまな方法を使用できます。この 文書で使用されている方法は、テスト目的の参照用として使用できます。

この例では、プレイブックの例を正常に実行した後、FTDハイアベイラビリティとそのスタンバ イIPアドレスが作成されます。

設定

ネットワーク図





トポロジ

コンフィギュレーション

シスコはサンプルスクリプトまたはお客様が作成したスクリプトをサポートしていないため、お

客様のニーズに応じてテストできる例がいくつかあります。

予備検証が正常に完了したことを確認することが不可欠です。

- Ansibleサーバはインターネット接続を備えています。
- Ansibleサーバは、FMC GUIポート(FMC GUIのデフォルトポートは443)と正常に通信できます。
- 2台のFTDデバイスがFMCに正常に登録されました。
- プライマリFTDはインターフェイスIPアドレスで設定されます。

ステップ1:SSHまたはコンソールを使用してAnsibleサーバのCLIに接続します。

ステップ2:コマンドansible-galaxy collection install cisco.fmcansibleを実行して、AnsibleサーバにFMCのAnsibleコレクションをインストールします。

<#root>

cisco@inserthostname-here:~\$

ansible-galaxy collection install cisco.fmcansible

ステップ3:コマンドmkdir /home/cisco/fmc_ansibleを実行して、関連ファイルを保存する新しいフォルダを作成します。この例で は、ホームディレクトリは/home/cisco/で、新しいフォルダ名はfmc_ansibleです。

<#root>

cisco@inserthostname-here:~\$

mkdir /home/cisco/fmc_ansible

ステップ 4: /home/cisco/fmc_ansibleフォルダに移動し、インベントリファイルを作成します。この例では、インベントリファイルの名前はinventory.iniです。

<#root>

cisco@inserthostname-here:~\$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible\$

ls

inventory.ini

この内容を複製して貼り付け、利用できるようにすることで、正確なパラメータを使用して太字のセクションを変更できます。

<#root>

[fmc]

10.0.5.11

[fmc:vars] ansible_user=

cisco

ansible_password=

cisco

```
ansible_httpapi_port=443
ansible_httpapi_use_ssl=True
ansible_httpapi_validate_certs=False
network_type=HOST
ansible_network_os=cisco.fmcansible.fmc
```

ステップ 5: /home/cisco/fmc_ansibleフォルダに移動し、FTD HAを作成するための変数ファイルを作成します。この例では、変数のファイル名はfmc-create-ftd-ha-vars.ymlです。

<#root>

 $cisco@inserthostname-here:{\sim}\$$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible\$

ls

fmc-create-ftd-ha-vars.yml

inventory.ini

この内容を複製して貼り付け、利用できるようにすることで、正確なパラメータを使用して太字のセクションを変更できます。

<#root>

user: domain: 'Global' device_name: ftd1: '

FTDA

' ftd2: '

FTDB

```
' ftd_ha: name: '
FTD_HA
' active_ip: '
192.168.1.1
' standby_ip: '
192.168.1.2
' key:
cisco
mask24: '
255.255.255.0
'
```

手順 6: /home/cisco/fmc_ansibleフォルダに移動し、FTD HAを作成するためのプレイブックファイルを作成します。この例では、 プレイブックのファイル名はfmc-create-ftd-ha-playbook.yamlです。

<#root>

cisco@inserthostname-here:~\$

```
cd /home/cisco/fmc_ansible/
```

ccisco@inserthostname-here:~/fmc_ansible\$

ls

fmc-create-ftd-ha-playbook.yaml

fmc-create-ftd-ha-vars.yml inventory.ini

この内容を複製して貼り付け、利用できるようにすることで、正確なパラメータを使用して太字のセクションを変更できます。

<#root>

---- - name: FMC Create FTD HA hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configuration: operation: user.domain

}}" register_as: domain - name: Task02 - Get FTD1 cisco.fmcansible.fmc_configuration: operation: getAl
device_name.ftd1

}}" register_as: ftd1_list - name: Task03 - Get FTD2 cisco.fmcansible.fmc_configuration: operation: ge device_name.ftd2 }}" register_as: ftd2_list - name: Task04 - Get Physical Interfaces cisco.fmcansible.fmc_configuration
ftd.bs.meme

ftd_ha.name

}}" type: "DeviceHAPair" ftdHABootstrap: { 'isEncryptionEnabled': false, 'encKeyGenerationScheme': 'CU ftd_ha.key

}}", 'useSameLinkForFailovers': true, 'lanFailover': { 'useIPv6Address': false, 'subnetMask': "{{

ftd_ha.mask24

```
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'
```

ftd_ha.standby_ip

}}", 'logicalName': 'LAN-INTERFACE', 'activeIP': "{{

ftd_ha.active_ip

}}" }, 'statefulFailover': { 'useIPv6Address': false, 'subnetMask': "{{

ftd_ha.mask24

```
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'
```

ftd_ha.standby_ip

}}", 'logicalName': 'STATEFUL-INTERFACE', 'activeIP': "{{

ftd_ha.active_ip

}}" } path_params: domainUUID: "{{ domain[0].uuid }}" - name: Task06 - Wait for FTD HA Ready ansible



注:このプレイブック例で太字で示されている名前は変数として機能します。これらの変数に対応する値は、変数ファ イル内に保存されます。

手順7: /home/cisco/fmc_ansibleフォルダに移動し、ansibleタスクを再生するansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"ためにコマンドを実行します。

この例では、コマンドはansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yml"です。

<#root>

cisco@inserthostname-here:~\$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible\$

ls

ステップ8: /home/cisco/fmc_ansibleフォルダに移動し、FTD HAスタンバイIPアドレスを更新するための変数ファイルを作成しま す。この例では、変数のファイル名はfmc-create-ftd-ha-standby-ip-vars.ymlです。

<#root>

```
cisco@inserthostname-here:~$
```

cd /home/cisco/fmc_ansible/

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-create-ftd-ha-playbook.yaml
fmc-create-ftd-ha-standby-ip-vars.yml
fmc-create-ftd-ha-vars.yml inventory.ini
```

この内容を複製して貼り付け、利用できるようにし、正確なパラメータで太字のセクションを変更します。

<#root>

user: domain: 'Global' ftd_data: outside_name: '

Outside

```
' inside_name: '
```

Inside

```
'outside_ip: '10.1.1.1' inside_ip: '10.1.2.1' mask24: '255.255.255.0' ftd_ha: name: '
```

FTD_HA

```
' outside_standby: '
```

10.1.1.2

```
' inside_standby: '
```

10.1.2.2

1

ステップ9: /home/cisco/fmc_ansibleフォルダに移動し、FTD HAスタンバイIPアドレスを更新するためのプレイブックファイルを 作成します。この例では、プレイブックのファイル名はfmc-create-ftd-ha-standby-ip-playbook.yamlです。

<#root>

cisco@inserthostname-here:~\$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible\$

```
ls
```

fmc-create-ftd-ha-playbook.yaml

fmc-create-ftd-ha-standby-ip-playbook.yaml

fmc-create-ftd-ha-standby-ip-vars.yml fmc-create-ftd-ha-vars.yml inventory.ini

この内容を複製して貼り付け、利用できるようにすることで、正確なパラメータを使用して太字のセクションを変更できます。

<#root>

---- name: FMC Update FTD HA Interface Standby IP hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_con user.domain

}}" register_as: domain - name: Task02 - Get FTD HA Object cisco.fmcansible.fmc_configuration: operati
ftd_data.outside_name

}}" register_as: outside_interface - name: Task04 - Get Inside Interface cisco.fmcansible.fmc_configur
ftd_data.inside_name

}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c
ftd_ha.outside_standby

}}"} monitorForFailures: true path_params: objectId: "{{ outside_interface[0].id }}" containerUUID: "{
ftd_ha.inside_standby

}}"} monitorForFailures: true path_params: objectId: "{{ inside_interface[0].id }}" containerUUID: "{{



注:このプレイブック例で太字で示されている名前は変数として機能します。これらの変数に対応する値は、変数ファ イル内に保存されます。

ステップ10: /home/cisco/fmc_ansibleフォルダに移動し、ansibleタスクを再生するansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"ためにコマンドを実行します。

この例では、コマンドはansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml"です。

<#root>

cisco@inserthostname-here:~\$

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

ls

fmc-create-ftd-ha-playbook.yaml
fmc-create-ftd-ha-standby-ip-playbook.yaml

fmc-create-ftd-ha-standby-ip-vars.yml

fmc-create-ftd-ha-vars.yml

inventory.ini

```
cisco@inserthostname-here:~/fmc_ansible$
```

ansible-playbook -i inventory.ini	fmc-create-ft	d-ha-standby-ip-playbook.yaml	-e@"fmc-create-ftd-ha-stand
PLAY [FMC Update FTD HA Interface	e Standby IP]	*****	****

確認

応答タスクを実行する前に、FMC GUIにログインします。Devices > Device Management, 2 FTD registered successfully on FMC with configured access control policyの順に移動します。

Fir Dev	rewall Manag rices / Device Man	ement Center	Overview	v Analysis	Policie	es Devi	ces Objects	Integratio	'n	Deploy	۹
View By: All (2)	Group Error (0)	• Warning (0)	Offline (0)	 Normal (2) 	Depl	oyment Pend	ling (0) • Upgra	ade (0)	Snort 3 (2)		
Collapse All											
Na	me			Model		Version	Chassis		Licenses	Access (Contro
□ ~ u	Jngrouped (2)										
	FTDA Snort 3 10.0.5.12 - Route	ed		FTDv for KVM		7.4.1	N/A		Essentials	TEMPACE	Ρ
	FTDB Snort 3 10.0.5.13 - Route	ed		FTDv for KVM		7.4.1	N/A		Essentials	TEMPACE	Ρ

Ansibleタスクの実行前

割り当て可能なタスクの実行後、FMC GUIにログインします。**Devices > Device Management,** FTD HA is created successfullyの順に 移動します。

Firewall Management Center Devices / Device Management	verview Analysis	Policies Devices	o Objects Integ	ration Deploy Q
View By: Group All (2) Error (0) Warning (0) Offline	(0) Normal (2)	 Deployment Pending 	g (0) • Upgrade (0)	 Snort 3 (2)
Collapse All				
Name	Model	Version Chassis	Lic	enses Access Contr
Ungrouped (1)				
FTD_HA High Availability				
FTDA(Primary, Active) Snort 3 10.0.5.12 - Routed	FTDv for KVM	7.4.1 N/A	Esse	ntials TEMPACP
FTDB(Secondary, Standby) Snort 3 10.0.5.13 - Routed	FTDv for KVM	7.4.1 N/A	Esse	ntials TEMPACP

Ansibleタスクを正常に実行した後

FTD HAのEditをクリックすると、フェールオーバーIPアドレスとインターフェイスのスタンバイIPアドレスが正常に設定されます。

Firewall Management Center Overview	w Analysis Policies D	evices Objects	Integration Deplo	w q 🥝 🌣 🛛	admin v dual	SECURE
FTD_HA Cisco Firepower Threat Defense for KVM						Cancel
Summary High Availability Device Routing I	nterfaces Inline Sets DHCP	VTEP				
High Availability Link		State Link				
Interface	GigabitEthernet0/7	Interface			GigabitEthern	et0/7
Logical Name	LAN-INTERFACE	Logical Name			LAN-INTER	FACE
Primary IP	192.168.1.1	Primary IP			192.16	8.1.1
Secondary IP	192.168.1.2	Secondary IP			192.16	8.1.2
Subnet Mask	255.255.255.0	Subnet Mask			255.255.	255.0
IPsec Encryption	Disabled	Statistics				Q
Monitored Interfaces						
Interface Name Active IPv4 Standby IPv4	Active IPv6 - Standby IPv6		Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
management					٥	/
Inside 10.1.2.1 10.1.2.2					٥	/
Outside 10.1.1.1 10.1.1.2					٢	/

FTDハイアベイラビリティの詳細

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

Ansible Playbookのログをさらに表示するには、-vvvを使用してAnsible Playbookを実行します。

<#root>

cisco@inserthostname-here:~/fmc_ansible\$ ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-playbook.yaml

-vvv

関連情報

Cisco Devnet FMCアンサブル

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。