Déployer un contrôleur FMC fourni dans le cloud (cdFMC) dans Cisco Defense Orchestrator (CDO)

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Configurer Déployez un centre de gestion Firepower fourni dans le cloud sur CDO, Intégration d'un FTD sur un FMC fourni dans le cloud Informations connexes

Introduction

Ce document décrit le processus de déploiement et d'intégration de FMC fourni dans le cloud sur la plate-forme CDO.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Centre de gestion Firepower (cdFMC) fourni dans le cloud
- Cisco Defense Orchestrator (CDO)
- Protection virtuelle contre les menaces Firepower (FTDv)

Version FTD minimale 7.0.3

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CdFMC
- FTDv 7.2.0

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Defense Orchestrator (CDO) est la plate-forme du centre de gestion des pare-feu (CdFMC) fourni dans le cloud. Le Centre de gestion des pare-feu, fourni dans le cloud, est un produit SaaS (Software-as-a-Service) qui gère les périphériques Secure Firewall Threat Defense. Il offre un grand nombre des mêmes fonctions qu'un pare-feu sécurisé sur site, Secure Firewall Threat Defense. Il a le même aspect et le même comportement qu'un centre de gestion de pare-feu sécurisé sur site et utilise la même interface de programmation d'application (API) FMC.

Ce produit est conçu pour la migration des centres de gestion de pare-feu sécurisés sur site vers la version SaaS du centre de gestion de pare-feu sécurisé.

Configurer

Déployez un centre de gestion Firepower fourni dans le cloud sur CDO.

Ces images montrent le processus de configuration initiale nécessaire pour déployer un FMC fourni dans le cloud sur CDO.

Dans le menu CDO, accédez à Tools & Services > Firewall Management Center > Onboard.

= Hide Menu	Welcome to Cisco Defense Orchestrator	Quick Action
📥 Dashboard		
C Multicloud New	Inventory & Objects	+ Onboard
inventory		
Configuration		
Policies		
Objects		
₀å₀ VPN		
Events & Monitoring		
√ Analytics		Onboard a Device or Service Onboard ASAs, FTDs or other devices or services to begin your CDO Experience
(Change Log		
(+) Jobs		
🛞 Tools & Services		
袋 Settings	Version a611b0d748c7628568984b831cfd7f8856390e80 CDO Status	© 2024 Cisco Systems, Inc

Sélectionner Enable Cloud-Delivered FMC.

CDO met en service une instance de Firewall Management Center dans le cloud en arrière-plan ; cela prend généralement 15 à 30 minutes. Vous pouvez suivre la progression du provisionnement dans la colonne État de Cloud-Delivered FMC.

Hide Menu		Onc FTD	e your cdFMC becomes active s.	e, you will need to log	out and log back in to st	art using your	cdFMC to	add		
Dashboard										
C Multicloud Defense	New	0	Constitution Devices Marries 10 Adde							
Inventory		Q	search by Device Name, IP Add	ress, or Serial Number						
Configuration		FMC	Secure Connectors							
Policies	>		Name	Ve	ersion		Devices	Туре	Status	Last Heartbeat
Objects			Cloud-Delivered FMC	N/	A		⊕0	Cloud-Delivered FMC	$\ddot{\mathbf{Q}}$ Provisioning (This process will take 15	
₀ð₀ VPN	>									_
Events & Monitoring										
-√- Analytics	>									
(Change Log										
📥 Jobs										
😤 Tools & Servi	ces >									
Settings	>									

Une fois la mise en service terminée, l'état passe à Actif. En outre, vous recevez une notification « Firewall Management Center is Ready » dans le panneau de notifications CDO.



-ili-ili cisco	Defense Orchestr	ator	Ser	vices				Q Sea	rch
≡	Hide Menu								
	Dashboard		Q	Search by Device Name, IP Address, or Serial Nu	imber				e +
\bigcirc	Multicloud Defense	ew	FMC	Secure Connectors					
	Inventory			Name	Version	Devices	Туре	Status	Last Heartbeat
Con	figuration			Cloud-Delivered FMC	20240412	⊜ 0	Cloud-Delivered FMC	 Active 	05/07/2024, 16:24:43
3	Policies	>							
\otimes	Objects	>							
ംറ്റം	VPN	>							
Ever	nts & Monitoring								
	Analytics	>							
٩	Change Log								
<u>(*</u>)	Jobs								
R	Tools & Services	>							
ŝ	Settings	>							

Vous pouvez ensuite intégrer vos appareils de protection contre les menaces au centre de gestion des pare-feu fourni dans le cloud et les gérer.

Accédez à Menu > Tools & Services > Firewall Management Center.



Sélectionnez votre cdFMC pour afficher les informations de cdFMC et, afin d'accéder à l'interface graphique utilisateur (GUI) du cdFMC, sélectionnez l'une des options disponibles sur le côté droit.

cisco Defense Orchestrator	Services				Q Search		₽.	۵۰ 📥 ۲۰
Hide Menu	Q Search by Device Name, IP / FMC Secure Connectors	Address, or Serial Number				c •	•	Cloud-Delivered FN Hostname cdo-cisco-mul tac.app.us.cdo Version 20240412
Multicloud Defense New Inventory	Name	Version	Devices	Туре	Status	Last Heartbeat	ſ	Actions
Configuration Policies	Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	C Active	05/07/2024, 16:24:43		O Check For Changes
Objects → *Ô* VPN →								Workflows API Explorer
Events & Monitoring								Devices Policies
Change Log (+) Jobs								 ⊕ Objects +⊂ NAT -> Site to Site VPN
Image: Services > Image: Im								ふ Remote Access VPN ④ Platform Settings
								System Configuration Smart Licenses AMP Management -> Device Health Audit Cisco Cloud Events

Vous pouvez maintenant voir l'interface graphique utilisateur de cdFMC.

Defense Orchesti FMC / System / Health /	rator Analysis	Policies	Devices Objects	Integration	🕤 Return Home Deploy Q 🐠 🔅	Imatuscl@cisco.com Imatuscl@cisco.com
Monitoring	Health Status 1 total 0 critical Devices ••••••••••••••••••••••••••••••••••••	0 warnings 1	1 normal 0 disabled	Q. Filter using device name		
	Device			Version	Model	
	> © FTDv			7.2.0	Cisco Firepower Threat Defense for Azure	

Intégration d'un FTD sur un FMC fourni dans le cloud

Ces images montrent comment intégrer un FTD afin d'être enregistré sur un cdFMC avec une clé d'enregistrement de l'interface de ligne de commande (CLI).

Tout d'abord, sélectionnez Onboard an FTD sur la page d'accueil de CDO.



Sélectionnez ensuite l'Use CLI Registration Key option.

dute Defense Orchestrator	Onboard FTD Device					Q	٥.	4	• •	cmonterr_cdo cmonterr@cisco.com
		Follow the steps below					Cancel			
Configuration										
Policies >		FTD 0000	A Important: After onboarding you manager will not be available after	r FTD, it will be managed by Firewa onboarding, and all existing policy	all Management Center in CDO. Note that use of configurations will be reset. You will need to rec	the firew onfigure	all device polices from	1		
Objects >		Firepower Threat Defense	CDO after onboarding. Learn more	C.						
-& VPN >		90-day Evaluation License: 89 days left Manage Smart License	Use CLI Registration Key Onboard a device using a registration	Use Serial Number Use this method for low-touch						
Events & Monitoring			key generated from CDO and applied on the device using the Command Line	provisioning or for onboarding configured devices using their serial						
\sqrt{r} Analytics \rightarrow			Interface. (FTD 7.0.3+ & 7.2+)	number. (FTD 7.2+)						
Change Log										

Saisissez les informations FTDv requises et souhaitées.

1 Device Name	FTDv				Edit
2 Policy Assignment	Access Control Policy: Defau	It Access Control Policy			Edit
3 Subscription License	Please indicate if this FTD is ph Physical FTD Device Virtual FTD Device Performance Tier (FTDv 7.0 FTDv100 - Tiered (16 ca License Type Base License Threat Malware URL License RA VPN VPNOnly +	and above only) ore / 32 GB) Includes Base Firewall Capabilities C File Policy URL Reputation RA VPN	En: the CD Le: No Ma the acc FT	able subscription licenses. CDO will attempt to enable e selected licenses when the device is connected to DO and registered with the supplied Smart License. arn more about Cisco Smart Accounts. the: All virtual FTDs require performance tier license. ake sure your subscription licensing account contains a available licenses you need. Its important to choose a tier that matches the license you have in your count. Until you choose a tier, your FTDv defaults to Dv50 selection.	e ,

Enfin, le cdFMC crée une configuration spécifique CLI Keypour votre périphérique.

4 CLI Registration Key	 Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more Copy the CLI Key below and paste it into the CLI of the FTD 	C
	configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdKqsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr- cdo.app.us.cdo.cisco.com	A

Copiez le CLI Key dans l'interface de ligne de commande de votre périphérique géré.

> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK qsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com File HA_STATE is not found. Manager cmonterr-cdo.app.us.cdo.cisco.com successfully configured. Please make note of reg_key as this will be required while adding Device in FMC. show managers > Туре : Manager Host : cmonterr-cdo.app.us.cdo.cisco.com : cmonterr-cdo.app.us.cdo.cisco.com Display name Identifier : 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd Registration : Pending

Le cdFMC lance une tâche d'enregistrement.

cisco Defense Orchestrator	Inventory			Q	∴ · · · · · · · · · · · · · · · · · · ·	_cdo _
	T Devices Templates Q Search by Device Name, IP Address, or Serial Number	Displaying 1 of 1 results C ③ +	> F	TDv @		
E Inventory	All FTD			E	Jevice Details	~
Configuration Policies Configuration Configurati	Name 0 FTDv FTD	Configuration Status 9	Connectivity #		Location n/a Model n/a Serial n/a Version n/a Onboarding Registration Key Method	
⊷č⊷ VPN >						
Events & Monitoring				6	Registration Pending Waiting for Device Registration to start. Please comp	plete the
√r Analytics >					onboarding process by executing the following regis command on the device (ignore if already done). My	stration ake sure
Change Log					your FTD can connect to cmonterr-cdo.app.us.cdo.c	zisco.com.
🟥 Jobs					configure manager add cmonterr-cdo.a	0- (3)
				C	Jevice Actions	~
X Tools & Services					Workflows	
ô Settings >				ħ	Monitoring	÷
				c	Jevice Management	v
				F	Policies	~
				c	Objects	~
				1	abel Groups and Labels	÷
					Add Labels 🛛	
					Add label groups and labels	+

Remarque : assurez-vous que votre périphérique FTD communique avec le locataire CDO via les ports 8305 (sftunnel) et 443 afin de terminer le processus d'enregistrement. Consultez la configuration réseau requise complète.

Remarque : si vous ne pouvez pas vous connecter à l'hôte, vous pouvez rectifier la configuration DNS dans l'interface de ligne de commande FTD à l'aide de la commande suivante : **configure network dns <addresss**>.

Pour surveiller le processus d'enregistrement, accédez à **Device Actions > Workflows.**

Workflows				Q 4-	Cmonterr_cdo
 Return to Inventory 					
FTDv (FTD)					C 🖲
Name	Priority	Condition	Current State	Last Active	Time
fmceRegisterFtdStateMachine	On Demand	Done	Done	8/30/2022, 3:35:50 PM	8/30/2022, 3:33:11 PM / 8/30/2022, 3:35:50 PM
ftdcOnboardingStateMachine	On Demand	Done	Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

Développez l'Active état pour avoir des informations supplémentaires, ces images montrent comment le FTDv a été enregistré avec succès.

/orkflows					٩ ٥.	÷ ?) • cmonte Imatusci@c
eturn to Inventory ETDy (ETD)							
(FID)							
Name	Priority	Condition	Current State	Last Active		Time	
ACTION	TIME	START STATE	END STATE		RESULT		
PollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_RED	ISTER_FTD @INITIATE_GET_TASK_	STATUS	SUCCESS		
FmcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TAS	K_STATUS	SUCCESS		
FmcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_executeFm	cRequests POLLING_WAIT_BEFO	DRE_CHECK_REGISTER_FTD	JOB_IN_PROG	RESS	
PollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_REG	ISTER_FTD @ INITIATE_GET_TASK_	STATUS	SUCCESS		
FmcRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	WAIT_FOR_GET_TAS	K_STATUS	SUCCESS		
FmcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_executeFrr	cRequests INITIATE_GET_DEVIC	E_RECORDS_REGISTER_FTD	JOB_SUCCEE	DED	
FmcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_REC	WAIT_FOR_DEVICE_F	RECORDS_REGISTER_FTD	SUCCESS		
FmceFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_executeFm	cRequests OONE		SUCCESS		
ноок	TYPE	TIME	RESULT				
SaveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connecti	ivity State to context			
UpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersio	onInSMContext			
DeviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred	d			
FmceRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre ho	ook successfully for FTD device: FTD	v		
FmceRegisterFtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook :	successfully			
NotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skip	ped for this event			
UpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice				
AddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device n	ame to debug record			
DeviceStateMachineSetErrorAfterHock	After	15:35:50.528 / 15:35:50.530	noErrorOccurred	đ			
						0.000.0000	
Devices Templates Q Search by Dev	vice Name, IP Address, or Serial N	umber	Displaying 1 of 1 results	c 🕘 🕇	→ FTDv @		Imatusci@cisc
ETD.					FTD		
Name ¢		Configuration Status \$	Connectivity \$		Device Detai	5	
FTDv		© Synced	Online		Model	nra Cisco Firepo Azure	ower Threat Defens
					Serial Version	9AGTAFW2 7.2.0	406
					Onboardin	g Registration	i Key
					Snort Versi	ion 3.1.21.1-12	26
							_
					Vour device	's configuration is up	-to-date.
					Device Action	15	
					C Check f	or Changes	
					E Workflo	ws	
					Remove	·	
					Monitoring		
					🔶 Health		
					Device Mana	gement	
						Overview	
					B Routing		
					 Interfac Inline S 	es ets	
					E VTEP	nitability	

Enfin, accédez à **Device Management > Device Overview** afin d'accéder à cdFMC et consultez l'état de la vue d'ensemble FTDv.

Defense Orchestrator Analysis Police FMC / Devices / Secure Firewall Device Summary Analysis	ies D	vices Objects Integration		😁 Return Home Deploy Q 🔮 🕻	Imatuscl@cisco.com • SECUR
Device Routing Interfaces Inline Sets DHCP VTEP					
General	+ +	License	/	System	0 G
Name: F	TDv	Performance Tier :	FTDv100 - Tiered (Core 16 / 32 GB)	Model:	Cisco Firepower Threat Defense for Azure
Transfer Packets:	No	Base:	Yes	Serial:	9AGTAFW24C6
Mode: Ro	uted	Export-Controlled Features:	No	Time:	2022-08-30 21:04:27
Compliance Mode: N	lone	Malware:	No	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration: Disa	bled	Threat:	No	Version:	7.2.0
		URL Filtering:	No	Time Zone setting for Time based Rules:	UTC (UTC+0:00)
Device Configuration: Import Export Down	beo	AnyConnect Apex:	No		
		AnyConnect Plus:	No		
		AnyConnect VPN Only:	No		
	_				
Inspection Engine		Health		Management	/ 🔍
Inspection Engine: Sn	ort 3	Status:	•	Host:	NO-IP
Revert to Snort 2		Policy:	Initial_Health_Policy 2022-06-04 01:25:03	Status:	•
		Excluded:	None	Manager Access Interface:	Management Interface

Informations connexes

- <u>Assistance et documentation techniques Cisco Systems</u>
- <u>Gestion des périphériques Cisco Secure Firewall Threat Defense grâce au centre de gestion des pare-feu fourni dans le cloud</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.