



Migration d'une ASA vers un dispositif géré par FDM à l'aide de Cisco Defense Orchestrator

Première publication : 2019-06-17

Dernière modification : 2020-05-06

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

CHAPITRE 1

Pour commencer 1

- Choisissez le bon processus de migration 1
- À propos du processus de migration de Cisco Defense Orchestrator 1
- Licence pour le processus de migration 3
- Lignes directrices et limites relatives à la licence 3
- Protocoles IP pris en charge SUR CDO 7
- Pratiques exemplaires 9

CHAPITRE 2

Migration d'ASA vers un flux de travail de périphérique géré par FDM 11

- Comment mettre en œuvre le processus de migration 11
 - Préparation à la migration 11
 - Préparation d'un appareil ASA 12
 - Optimisez vos politiques ASA avant de migrer 12
 - Ajoutez des configurations EtherChannel au périphérique géré par FDM avant la migration 13
 - Exécuter la migration 14
 - Sélectionner le périphérique à migrer 14
 - (Facultatif) Mettre à jour le nom de la migration 15
 - (Facultatif) Préserver la configuration en cours d'exécution 15
 - Analyse de la configuration d'ASA en cours 16
 - Appliquer la migration 17
 - Affichez les actions de migration 21
 - Déployer la configuration 23

ANNEXE A

Télémetrie 25

- Cisco Success Network (Réseau de succès Cisco) 25

ANNEXE B

Foire aux questions 27

FAQ sur la résolution de problèmes 27



CHAPITRE 1

Pour commencer

- Choisissez le bon processus de migration, à la page 1
- À propos du processus de migration de Cisco Defense Orchestrator, à la page 1
- Licence pour le processus de migration, à la page 3
- Lignes directrices et limites relatives à la licence, à la page 3
- Protocoles IP pris en charge SUR CDO, à la page 7
- Pratiques exemplaires, à la page 9

Choisissez le bon processus de migration

Il existe deux méthodes pour migrer les configurations de l'appareil de sécurité adaptable (ASA) vers les appareils Gérés par FDM à l'aide de Cisco Defense Orchestrator (CDO) :

- Solution CDO : si vous avez l'intention de migrer vos configurations ASA vers des appareils Gérés par FDM et de les gérer avec CDO et Gestionnaire d'appareil Firepower, utilisez le processus en nuage dans CDO pour migrer vos configurations ASA.
- Solution sur site (Gestionnaire d'appareil Firepower) : si vous avez l'intention de migrer vos configurations ASA vers des appareils Gérés par FDM, utilisez le processus en nuage dans CDO pour migrer vos configurations ASA. Vous pouvez ensuite utiliser le gestionnaire d'appareil Firepower pour gérer votre configuration.

Ce guide suppose que vous avez une compréhension de base des opérations de CDO. Pour en savoir plus, consultez la [fiche technique de CDO](#).

À propos du processus de migration de Cisco Defense Orchestrator

CDO peut vous aider à migrer votre Appareil de sécurité adaptable (ASA) vers un Appareil Géré par FDM. CDO fournit l'assistant de **migration ASA vers FDM** pour vous aider à migrer la configuration en cours d'exécution de votre ASA vers un modèle FDM.



Remarque Les indicateurs de fonctionnalité *show-fdm* et *enable-asa-to-ftd-migration* doivent être activés pour afficher l'option de **migration ASA vers FDM** sous **Outils et Services**. Communiquez avec le TAC pour activer l'option de **migration ASA vers FDM** si elle n'est pas disponible sous **Outils et services**.

Vous pouvez migrer les éléments suivants de la configuration en cours d'exécution d'ASA vers un modèle FDM à l'aide de l'assistant de **migration ASA vers FDM** :

- Interfaces
- Routs
- Règles de contrôle d'accès (ACL)
- Règles de traduction d'adresses réseau (NAT)
- Objets réseau et objets de groupe de réseaux



Remarque CDO ne prend pas en charge les noms d'objet avec des mots clés réservés. Renommez les noms des objets en leur ajoutant le suffixe « ftdmig ».

- Objets de service et objets de groupe de services
- VPN de site à site

CDO migre uniquement les objets référencés. Les objets d'une liste de contrôle d'accès, qui sont définis, mais non référencés à un groupe d'accès, ne sont pas migrés. Certaines des raisons courantes d'échec de la migration de certains éléments peuvent être l'une ou plusieurs des raisons suivantes :

- Listes d'accès ICMP sans code ICMP
- Listes d'accès TCP/UDP sans configuration de groupe d'accès
- Listes d'accès IP non mappées aux profils VPN de site à site
- Tout objet réseau ou groupe faisant référence à des listes d'accès qui ne fait pas l'objet d'une migration
- Interfaces appelées arrêt



Remarque Tout objet ou groupe d'objets non référencé dans la configuration sera également abandonné et marqué comme inutilisé lors de la migration. Consultez le **Rapport de migration** pour plus d'informations sur les éléments qui n'ont pas été migrés.

Une fois que ces éléments de la configuration en cours d'exécution ASA ont été migrés vers le modèle FDM, vous pouvez appliquer le modèle FDM à un nouveau Géré par FDM Appareil qui est géré par CDO. Le périphérique Géré par FDM adopte les configurations définies dans le modèle et Géré par FDM est donc maintenant configuré avec certains aspects de la configuration en cours d'exécution de l'ASA.

Les autres éléments de la configuration en cours d'exécution de l'ASA ne sont pas migrés à l'aide de ce processus. Ces autres éléments sont représentés dans le modèle FDM par des valeurs vides. Lorsque le modèle

est appliqué au Géré par FDM périphérique, nous appliquons les valeurs que nous avons migrées vers le nouveau périphérique et ignorons les valeurs vides. Quelles que soient les autres valeurs par défaut du nouveau appareil, il les conserve. Les autres éléments de la configuration d'exécution ASA que nous n'avons pas migrés devront être recréés sur le périphérique Géré par FDM en dehors du processus de migration.

Licence pour le processus de migration

Le processus de migration du périphérique Géré par FDM fait partie de CDO et ne nécessite aucune licence spécifique autre que la licence CDO.

Lignes directrices et limites relatives à la licence



Remarque Les configurations qui ne sont pas prises en charge dans CDO seront abandonnées pendant la migration comme **Non prises en charge** et seront signalées dans le **Rapport de migration**.

Nom de la fonctionnalité ou de la fonction	Que peut-on faire migrer?	Restrictions ou limitations de la migration
Mode de pare-feu	Mode de pare-feu routé	Les configurations en mode transparent ne peuvent pas être migrées.
Configuration de l'interface	<ul style="list-style-type: none"> • Interfaces physiques • Sous-interfaces 	<ul style="list-style-type: none"> • Le Géré par FDMpériphérique doit avoir autant d'interfaces physiques ou plus que les configurations d'interface ASA faisant l'objet de la migration. • Sous-interfaces (l'ID de sous-interface sera toujours défini sur le même numéro que l'ID de VLAN lors de la migration) • Les configurations d'interface suivantes ne seront pas migrées vers Géré par FDMle périphérique : <ul style="list-style-type: none"> • VLAN secondaires sur les interfaces ASA • Interface redondante • interface de groupe de pont • Virtual Tunnel Interface

Nom de la fonctionnalité ou de la fonction	Que peut-on faire migrer?	Restrictions ou limitations de la migration
EtherChannels	<p>EtherChannels configurés sur les interfaces physiques.</p> <p>Les interfaces membres mappées aux EtherChannels sont conservées pendant la migration.</p>	<ul style="list-style-type: none"> • Avant de migrer les configurations, vous devez créer le nombre équivalent d’EtherChannels sur Géré par FDM le périphérique à l’aide de CDO. Voir Ajouter une interface EtherChannel pour un périphérique géré par FDM. • Peut uniquement être migré vers des configurations de périphériques Firepower de série 1000 ou 2100 : 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140. • Vous pouvez migrer les configurations EtherChannel d’ASA 8.4+ vers Géré par FDM un périphérique exécutant la version logicielle 6.5+. • Les EtherChannels créés sur le Géré par FDMpériphérique avant la migration doivent être du même type que l’EtherChannel faisant l’objet de la migration. CDO fera uniquement migrer EtherChannel vers EtherChannel et interface physique vers interface physique. • Les interfaces membres mappées aux EtherChannels dans le modèle FDM ne seront pas disponibles pour les utilisateurs lors de l’étape de mappage d’interface de l’assistant de migration. Cependant, ils sont conservés et migrés vers leurs EtherChannels attribués.
Routage	du routage statique;	<ul style="list-style-type: none"> • Lorsqu’il existe plusieurs routes statiques avec le même réseau comme destination, une seule route avec une valeur de mesure minimale est migrée et les autres sont abandonnées. • Les fonctionnalités de routage suivantes ne seront pas migrées vers Géré par FDMle périphérique : <ul style="list-style-type: none"> • Routes en tunnel • Routes d’interface nulles 0 • Routes statiques avec suivi SLA

Nom de la fonctionnalité ou de la fonction	Que peut-on faire migrer?	Restrictions ou limitations de la migration
Règles de contrôle d'accès (ACL)	<ul style="list-style-type: none"> • Règles de contrôle d'accès activées • Objets source et destination • CDO prend en charge des actions telles que Autoriser, Faire confiance et Bloquer pour Géré par FDMle périphérique. Pendant la migration, les actions d'autorisation et de refus dans la configuration ASA source sont gérées et mappées à l'action prise en charge pour Géré par FDMle périphérique sur CDO. • CDO prend en charge la migration des listes de contrôle d'accès associées à une politique, à une interface ou à un groupe d'accès sans protocole IP. • ACE avec protocoles de tunnel L3 non chiffrés 	<p>Les fonctionnalités d'ACL suivantes ne seront pas migrées vers Géré par FDMle périphérique :</p> <ul style="list-style-type: none"> • CDO et le gestionnaire d'appareil Firepower ne prennent pas en charge les ACL avec les protocoles IPv4 et IPv6 mixtes • Journalisation des informations sur le niveau de gravité • Règles inactives ou désactivées • ACE avec objet de service ou groupe de services ayant des protocoles non TCP, UDP ou ICMP • ACE avec objets de service non TCP ou UDP • Protocole non TCP ou UDP dans ACE avec objets en ligne • ACE avec l'intervalle de temps • Liste d'accès non mappée avec le groupe d'accès
Règles de traduction d'adresses réseau (NAT)	<ul style="list-style-type: none"> • Object réseau (Auto) et deux fois (Manuel) NAT ou PAT • NAT statique • NAT ou PAT dynamique • NAT d'identité • Traduction de Port source (service) 	<p>Les fonctionnalités de règles NAT suivantes ne seront pas migrées vers Géré par FDMle périphérique :</p> <ul style="list-style-type: none"> • Réserve PAT • Unidirectionnelle • Inactif • Avec Twice NAT, l'utilisation d'objets de service de destination pour la traduction de port de destination (service) (y compris les objets de service qui ont à la fois la source et la destination) • Traduction du port de destination • NAT46, NAT64 <p>Remarque CDO ne prend pas en charge les objets réseau avec 0.0.0.0/32.</p>

Nom de la fonctionnalité ou de la fonction	Que peut-on faire migrer?	Restrictions ou limitations de la migration
Objets de service et objets de groupe de services	Objets de service et groupes imbriqués Consultez la section Protocoles IP pris en charge SUR CDO pour obtenir la liste des protocoles utilisés dans les objets de service pris en charge par CDO.	<ul style="list-style-type: none"> • Les protocoles BCC-RCC-MON et BBN-RCC-MON ne sont pas pris en charge. • Les opérateurs comme inférieur à, supérieur à pas égal à, ne sont pas pris en charge. • Imbrication de groupes d'objets
Objets réseau et objets de groupe de réseaux	Objets réseau et objets de groupe de réseaux	<p>Les objets réseau ou groupes de réseaux suivants ne sont pas pris en charge :</p> <ul style="list-style-type: none"> • Basé sur un masque discontinu • Adresse IP commençant par le premier octet « 0 » dans l'adresse IPv4
Types ICMP	Types ICMP	<p>Les types ICMP suivants ne sont pas pris en charge :</p> <ul style="list-style-type: none"> • Entrées d'objets de service basées sur ICMP avec un type ou un code ICMP INVALIDE • Objet de type service ou ICMP sans code pour le type ICMPv4 ou ICMPv6 • Tout type d'ICMP non affecté (selon IANA) ou type d'ICMP non valide
Objets divers non pris en charge	-	<p>Les objets divers suivants ne sont pas pris en charge :</p> <ul style="list-style-type: none"> • Groupe d'objets réseau basé sur SGT • Groupe d'objets réseau basé sur l'utilisateur

Nom de la fonctionnalité ou de la fonction	Que peut-on faire migrer?	Restrictions ou limitations de la migration
VPN de site à site	<ul style="list-style-type: none"> • Propositions de phases 1 et 2 pour IKEv1 et IKEv2 • Perfect Forward Secrecy (Confidentialité de transmission parfaite) (PFS) pour IKEv1 et IKEv2 • Liste d'accès de chiffrement avec groupe d'objets imbriqués • Carte de chiffrement avec plusieurs adresses IP homologues • IKEv1 et IKEv2 utilisés pour un tunnel dans Crypto Map 	<p>Les fonctionnalités VPN de site à site suivantes ne sont pas prises en charge :</p> <ul style="list-style-type: none"> • VPN-Filtre • vpn-délai-d'inactivité • isakmp keepalive seuil 10 réessayer 10 • Crypto Map VPNMAP 200 définir la durée de vie de l'association de sécurité en 360 secondes • définir la durée de vie de l'association de sécurité en kilo-octets illimités • définir la durée de vie de l'association de sécurité en 3600 secondes • Authentification du certificat • Carte de chiffrement dynamique • Virtual Tunnel Interface (VPN) basé sur la route

Pour plus de renseignements sur les directives et les limitations, consultez les [Directives et limitations pour les configurations ASA](#) et les [directives et limitations pour les AppareilsGéré par FDM](#).

Protocoles IP pris en charge SUR CDO

Les protocoles IP pris en charge par CDO dans les objets de service sont les suivants :

Protocoles IP dans les objets de service			
1 = ICMP	34 = TROISPC	73 = CPHB	106 = QNX
2 = protocole IGMP	35 = IDPR	74 = WSN	107 = AN
3 = GGP	36 = XTP	75 = PVP	108 = IPCOMP
5 = ST2	37 = DDP	76 = BRSATMON	109 = SNP
6 = TCP	38 = IDPRCMTTP	78 = WBMON	110 = COMPAQPEER
7 = CBT	39 = TPPLUSPLUS	77 = SUNND	111 = IPXINIP
8 = EGP	40 = IL	79 = WBEXPAK	112 = VRRP
9 = IGP	42 = SDRP	80 = ISOIP	113 = PGM
10 = BBNRCCMON	45 = IDRP	81 = VMTP	115 = L2TP
11 = NVP2	46 = RSVP	82 = SECUREVMTP	116 = DDX
12 = PUP	48 = MHRP	83 = VIGNES	117 = IATP
13 = ARGUS	49 = BNA	84 = TTP	118 = ST
14 = EMCON	50 = ESP	85 = NSFNETIGP	119 = SRP
15=XNET	51 = AH	86 = DGP	120 = UTI
16 = CHAOS	52 = INLSP	87 = TCF	121 = SMP
17 = UDP	53 = SWIPE	88 = EIGRP	122 = SM
18 = MUX	54 = NARP	89 = OSPFIGP	123 = PTP
19 = DCNMEAS	55 = MOBILE	90 = SPRITERPC	124 = ISIS
20 = HMP	56 = TLSP	91 = LARP	125 = FIRE
21 = PRM	57 = SKIP	92 = MTP	126 = CRTP
22 = XNSIDP	58= IPv6-ICMP	93 = AX25	127 = CRUDP
23 = TRUNK1	59 = IPv6NONXT	94 = IPIP	128 = SSCOPMCE
24 = TRUNK2	62 = CFTP	95 = MICP	129 = IPLT
25 = LEAF1	64 = SATEXPAK	96 = SCCSP	130 = SPS
26 = LEAF2	65 = KRYPTOLAN	97 = ETHERIP	131= PIPE
27 = RDP	66 = RVD	98 = ENCAP	132 = SCTP
28 = IRTP	67 = IPPC	100 = GMTP	133 = FC
29 = ISOTP4	69 = SATMON	101 = IFMPP	254 = DIVERT
30 = NETBLT	70 = VISA	102 = PNNI	
31 = MFENSP	71 = IPCV	103 = PIM	
32 = MERITINP	72 = CPNX	104 = ARIS	
33 = SEP		105 = SCPS	

Pratiques exemplaires

Suivez ces meilleures pratiques lorsque vous utilisez CDO pour migrer une configuration ASA vers un modèle FDM :

- Assurez-vous de récupérer la configuration en cours d'exécution à partir d'un **show run** appareil ASA à l'aide de la commande dans une migration d'appareil de modèle.
- Examinez les rapports de migration pour les configurations ignorées, non prises en charge et partiellement prises en charge.
- Après la migration, vérifiez les règles et les objets migrés dans le modèle FDM avant de le déployer sur un Géré par FDM appareil.
- Optimisez vos politiques ASA avant de les migrer vers le modèle FDM.
- Nous vous recommandons de déployer la configuration ASA migrée sur Géré par FDM le périphérique qui n'a pas de configuration existante.



CHAPITRE 2

Migration d'ASA vers un flux de travail de périphérique géré par FDM

- [Comment mettre en œuvre le processus de migration, à la page 11](#)

Comment mettre en œuvre le processus de migration

	Faire ceci
Étape 1	Préparation à la migration, à la page 11 <ul style="list-style-type: none">• Préparation d'un appareil ASA• Optimisez vos politiques ASA avant de migrer• Ajoutez des configurations EtherChannel au périphérique géré par FDM avant la migration, à la page 13
Étape 2	Exécuter la migration, à la page 14 <ul style="list-style-type: none">• Sélectionner le périphérique à migrer• (Facultatif) Mettre à jour le nom de la migration• Analyse de la configuration d'ASA en cours• Appliquer la migration<ul style="list-style-type: none">• Appliquer la migration maintenant• Appliquer la migration ultérieurement
Étape 3	Affichez les actions de migration
Étape 4	Déployer la configuration, à la page 23

Préparation à la migration

Pour préparer vos périphériques à la migration, assurez-vous que :

- Vous avez un détenteur CDO et vous pouvez vous y connecter. Consultez la section [Connexion initiale](#) pour plus de renseignements.
- Vous avez intégré à votre détenteur le périphérique ASA ou le fichier de configuration ASA que vous souhaitez faire migrer vers un périphérique Géré par FDM

Le fichier de configuration en cours d'exécution de votre ASA doit faire moins de 4,5 Mo et compter 22 000 lignes. Reportez-vous à la section [Confirmation de la taille de la configuration d'exécution ASA](#).

- Vous avez intégré un périphérique Géré par FDM vers CDO si vous souhaitez migrer la configuration ASA vers le périphérique directement après le processus de migration, ou si vous souhaitez migrer les configurations EtherChannel vers le périphérique Géré par FDM. Consultez la section [Intégrer un périphérique FTD](#) pour obtenir de plus amples renseignements sur le sujet.
- Les périphériques doivent être **synchronisés**.
Cela garantit que la configuration en cours d'exécution sur le périphérique et la configuration en cours d'exécution qui est stockée dans CDO sont les mêmes.
- Votre ASA exécute la version logicielle 8.4 ou plus récente.

Pour en savoir plus sur le récapitulatif de la prise en charge des périphériques, les périphériques non pris en charge, le matériel et les logiciels, consultez la section [Logiciels et matériel pris en charge par CDO](#).

Préparation d'un appareil ASA

Cliquez sur (+) dans la page **Inventaire**.

La page **Intégration** s'affiche où vous pouvez intégrer l'appareil.

Comment intégrer un appareil ASA

Procédez comme suit pour intégrer un appareil ASA avec l'une de ces options :

- Intégrer un appareil ASA en direct.
- Importer la configuration pour la gestion hors ligne :
 - Saisissez le **nom du périphérique** et choisissez le **type d'appareil** comme ASA.
 - Cliquez sur **Parcourir** pour choisir le fichier de configuration ASA qui est un fichier *.TXT* ou un *.CFG*.
 - Cliquez sur **Upload** (Téléverser).

Optimisez vos politiques ASA avant de migrer

Maintenant que vous avez intégré tous vos ASA, commencez à utiliser CDO pour identifier et corriger les problèmes avec les objets réseau, optimiser vos politiques existantes, passer en revue vos connexions VPN et mettre à niveau vos ASA vers les versions les plus récentes.

Résoudre les problèmes d'objets réseau

Commencez à optimiser les politiques de sécurité de vos ASA en résolvant les problèmes liés aux [objets](#) de politique réseau.

- **Objets inutilisés** : CDO identifie les objets de politique réseau qui existent dans une configuration d'appareil, mais qui ne sont pas référencés par un autre objet, une liste d'accès ou une règle NAT. Trouvez ces objets inutilisés et supprimez-les.
- **Objets en double** : les objets en double sont deux objets ou plus sur le même appareil avec des noms différents, mais les mêmes valeurs. Ces objets sont généralement créés accidentellement, ont des objectifs similaires et sont utilisés par des politiques différentes. Recherchez des occasions de normaliser les noms tout en reconnaissant que certains doublons peuvent exister pour des raisons légitimes.
- **Objets incohérents** : les objets incohérents sont des objets sur deux appareils ou plus, portant le même nom, mais avec des valeurs différentes. Parfois, les utilisateurs créent des objets dans différentes configurations avec le même nom et le même contenu, mais avec le temps, les valeurs de ces objets divergent, ce qui crée une incohérence. Envisagez de normaliser les valeurs de ces objets ou de renommer un objet pour l'identifier comme un objet différent.

Réparez les règles d'ombre

Maintenant que vous avez résolu vos problèmes d'objets réseau, passez en revue les politiques de réseau pour les [règles d'ombre](#) et corrigez-les. Une règle d'ombre est marquée par un badge en demi-lune sur la page des politiques de réseau. Il s'agit d'une règle dans une politique qui ne se déclenchera jamais, car une règle avec une priorité plus élevée dans la politique agit sur tous les paquets avant qu'ils n'atteignent la règle dupliquée. S'il existe une règle occultée qui ne sera jamais touchée, supprimez-la ou [modifiez la politique](#) pour « afficher cette règle ».

Ajoutez des configurations EtherChannel au périphérique géré par FDM avant la migration

Avant de commencer

Passez en revue ces renseignements :

- [Préparation à la migration, à la page 11](#)
- [Le Lignes directrices et limites relatives à la licence, à la page 3](#) pour la migration des EtherChannels.

Procédure

Étape 1

Avant de migrer les configurations EtherChannel, vous devez créer le nombre équivalent d'EtherChannels sur Géré par FDM le périphérique que vous faites migrer à partir d'ASA. Vous pouvez utiliser CDO pour créer les EtherChannels. Consultez la section [Ajouter une interface EtherChannel pour un appareil géré par FDM](#) pour obtenir des instructions.

La configuration minimale pour un EtherChannel est un ID EtherChannel et au moins un membre EtherChannel.

Étape 2

Déployez les modifications sur votre Géré par FDM appareil.

Prochaine étape

Continuez vers [Exécuter la migration, à la page 14](#).

Exécuter la migration

Sélectionner le périphérique à migrer

Vous pouvez sélectionner le périphérique ASA pour la migration à l'aide de l'une des méthodes suivantes :

- [Lancez l'assistant de migration FDM et sélectionnez le périphérique](#)
- [Sélectionnez le périphérique et lancez l'assistant de migration FDM.](#)

Lancez l'assistant de migration FDM et sélectionnez le périphérique

Procédure

-
- Étape 1** Connectez-vous à votre détenteur CDO.
- Étape 2** Dans la barre de navigation, cliquez sur **Outils et Services**.
- Étape 3** Sous **Outils et Services**, sélectionnez **ASA vers la migration FDM**.
- Remarque** Les indicateurs de fonctionnalité *show-fdm* et *enable-asa-to-ftd-migration* doivent être activés pour afficher l'option de **migration ASA vers FDM** sous **Outils et Services**. Communiquez avec le TAC pour activer l'option de **migration ASA vers FDM** si elle n'est pas disponible sous **Outils et services**.
- Étape 4** Dans la page Migration FDM, cliquez sur (+) pour ajouter un périphérique ASA ou pour charger le fichier de configuration que vous souhaitez migrer vers le périphérique géré par FDM.
- Étape 5** Chargez le fichier de configuration ASA ou sélectionnez le périphérique dans la liste déroulante.
- S'il y a eu des migrations antérieures de ce périphérique, vous verrez les migrations résultantes du périphérique sélectionné.
- Pour plus de renseignements sur le filtrage, consultez [À propos des filtres de migration](#).
- S'il s'agit d'une nouvelle migration, cliquez sur **Démarrer une nouvelle migration pour (nom du périphérique)**.
-

Sélectionnez le périphérique et lancez l'assistant de migration FDM.

Procédure

-
- Étape 1** Connectez-vous à votre détenteur CDO.
- Étape 2** Dans la barre de navigation, cliquez sur **Inventaire**.
- Étape 3** Cliquez sur l'onglet **Devices (Appareils)** pour localiser votre appareil.
- Étape 4** Cliquez sur l'onglet **ASA** et sélectionnez le périphérique ASA ou le modèle que vous souhaitez migrer vers le périphérique géré par FDM.
- Les détails du périphérique ASA sélectionné, comme l'emplacement, le modèle, le numéro de série, etc., s'affichent dans le panneau **Détails du périphérique**.

- Étape 5** Dans le panneau **Actions du périphérique**, cliquez sur **Migrer vers FDM**.
- S'il y a eu des migrations antérieures de ce périphérique, vous verrez les migrations résultantes du périphérique sélectionné.
- Pour plus de renseignements sur le filtrage, consultez [À propos des filtres de migration](#).
- S'il s'agit d'une nouvelle migration, cliquez sur **Démarrer une nouvelle migration pour (nom du périphérique)**.
- Étape 6** (Facultatif) Si vous souhaitez sélectionner un autre appareil ASA ou un modèle à migrer vers le modèle FDM, consultez [À propos des filtres de migration](#).

(Facultatif) Mettre à jour le nom de la migration

Le nom de la migration est généré automatiquement en fonction du nom du périphérique et de l'horodatage.

Procédure

- Étape 1** Dans l'écran **Migration FDM**, vous pouvez également mettre à jour le nom de la migration ou conserver le nom par défaut. CDO vous permet de rechercher dans la liste de migration avec le nom de la migration.
- Remarque** Le nom du modèle FDM sera le même que le nom de la migration par défaut.
- Étape 2** Cliquez sur **Next (Suivant)** pour déclencher la migration.

(Facultatif) Préserver la configuration en cours d'exécution



Remarque Cela s'applique uniquement lorsque vous avez choisi l'ASA en direct dans la page **Inventaire**.

Dans **Conserver la configuration en cours d'exécution**, l'outil de migration vous permet d'enregistrer la copie de CDO de la configuration en cours d'exécution de l'ASA en tant que fichier de configuration. Ce modèle de configuration de périphérique est utilisé pour la migration et n'affecte donc pas l'ASA actif.

Les options suivantes sont disponibles pour la migration d'une copie de CDO de la configuration en cours d'exécution de l'ASA vers Géré par FDM le périphérique :

- Créer un fichier de configuration à partir de la copie du CDO du périphérique en cours d'exécution de l'ASA



Remarque Vous permet de conserver un instantané (périphérique modèle) de la configuration ASA au moment du lancement de la migration. Lorsque vous devez modifier la configuration à des fins de migration, vous pouvez utiliser le fichier de configuration sans affecter/interrompre la copie du CDO de la configuration en cours d'exécution de l'ASA.

- Migrez la configuration directement à partir du périphérique



Remarque La configuration source pour la migration est une copie de CDO de la configuration en cours d'exécution de l'ASA. L'outil de migration ne prend en compte que la configuration à partir du début de la migration. Toutes les modifications apportées ultérieurement à la copie de la configuration en cours d'exécution de l'ASA ne seront pas reflétées dans la migration résultante. Les tentatives de migration supplémentaires à partir de la copie modifiée de CDO de la configuration en cours d'exécution de l'ASA peuvent entraîner des Géré par FDM configurations de périphériques différentes.

Procédure

- Étape 1** Saisissez le nom du périphérique dans le champ **Model Device Name** (Nom du périphérique modèle).
- Étape 2** Effectuez l'une des actions suivantes :
- Cliquez sur **Next** (suivant).
Le périphérique modèle est créé et déclenche la migration pour ce périphérique.
 - Cliquez sur **Ignorer** pour déclencher la migration sur l'ASA actif.

Analyse de la configuration d'ASA en cours



Remarque Selon la taille des fichiers de configuration et le nombre d'autres appareils ou services, l'analyse de la configuration peut prendre un certain temps. Pour plus de renseignements, consultez [Confirmation de la taille de la configuration d'exécution ASA](#).

L'analyse de la migration se poursuit jusqu'à ce qu'elle réussisse ou échoue. Le processus de migration collecte les informations ASA, les analyse, crée un modèle FDM et permet à ce modèle FDM d'être appliqué à un appareil dans CDO. Pour plus de renseignements sur les modèles FDM, consultez [Modèles](#). Pendant la phase d'analyse, le processus de migration génère un **Rapport de migration** et un **Journal de migration** qui identifient :

- Les éléments de configuration ASA qui sont entièrement migrés, partiellement migrés, non pris en charge pour la migration et ignorés pour la migration.
- Les lignes de configuration ASA avec des erreurs, répertoriant les CLI ASA que le processus de migration ne peut pas reconnaître; cela bloque la migration.



Remarque L'interface de gestion et les routages statiques associés à l'interface de gestion ne sont pas migrés.

Corriger les erreurs de migration

En cas d'erreur de migration, vous pouvez consulter le **rapport de migration** et **consulter le journal de migration** dans l'écran de **migration FDM**.

Sélectionnez **Télécharger le rapport** et **Journal de téléchargement** dans l'écran de **migration de FDM** pour télécharger le rapport et les journaux de migration.

Les rapports et les journaux doivent pouvoir imprimer les lignes de la configuration ASA qui ont provoqué l'échec de l'analyse. Accédez au périphérique ASA que vous avez choisi pour la migration, mettez à jour la configuration ASA, puis redémarrez la nouvelle migration.

Si l'analyse a réussi, mais que la création du modèle FDM échoue, accédez à **Modèle > Flux de travail** ou **Migration > Flux de travail** pour identifier les échecs et résoudre les problèmes.

Analysez après avoir corrigé les erreurs de migration

Vous pouvez analyser à nouveau la configuration ASA après avoir corrigé les erreurs de migration. Procédez comme suit :

- Dans l'écran **Migration FDM**, cliquez sur **Aller à la configuration**.
- Accédez à la configuration spécifique et apportez les modifications de configuration qui ont entraîné l'échec de la conversion.
- Une fois que vous avez effectué les mises à jour pour la configuration correcte, cliquez sur **Réanalyser la configuration** pour déclencher la migration par rapport à la configuration modifiée.



Remarque

L'option **Réanalyser la configuration** s'applique uniquement lorsque vous avez mis à jour le fichier de configuration et pour la configuration avec des erreurs d'analyse uniquement.

Appliquer la migration

Pour appliquer la migration, vous pouvez choisir l'une des options suivantes :

- [Appliquer la migration maintenant](#)
- [Appliquer la migration ultérieurement](#)

Conformément à la fonctionnalité de modèle d'application de CDO, le modèle FDM qui est créé lors de la migration déploie les modifications sur le périphérique, uniquement sur les éléments suivants : interfaces, NAT, ACL, objets et routes.

Les paramètres DHCP et DNS de données sont restaurés aux valeurs par défaut, car les renseignements sur l'interface auraient changé pendant la migration.

Les autres paramètres, tels que VPN, haute disponibilité, etc., restent les mêmes sur l'appareil.

Appliquer la migration maintenant



Remarque

Avant d'appliquer la migration sur un appareil, vérifiez si l'appareil est **synchronisé**.

Vous pouvez appliquer le modèle FDM à n'importe quel appareil, passer en revue le modèle d'appareil et le déployer ultérieurement sur le périphérique en sélectionnant Géré par FDM le périphérique.

Procédure

-
- Étape 1** Sélectionnez **Appliquer la migration maintenant**.
- a) Dans la liste déroulante **Sélectionner le périphérique FTD**, sélectionnez Géré par FDM le périphérique pour lequel vous souhaitez appliquer le modèle d'appareil FDM.
- L'état du périphérique doit être « **Synchronisé** » avec la connectivité « **Online** ».
- b) Cliquez sur **Select** (Sélectionner) pour sélectionner le périphérique Géré par FDM.
- Étape 2** Cliquez sur **Next** (suivant).
- Étape 3** Dans la ligne **Mapper les interfaces**, l'outil de migration récupère une liste des **Interfaces de modèles** et des **Interfaces d'appareils** sur le périphérique Géré par FDM. Par défaut, l'outil de migration de pare-feu mappe les interfaces dans ASA et le périphérique Géré par FDM en fonction de leurs identités d'interface. Cliquez sur **Continue** (Continuer).
- Pour plus de renseignements sur le mappage des interfaces ASA avec les appareils Géré par FDM, consultez [Mapper les interfaces ASA avec les interfaces de Firewall Threat Defense](#).
- Étape 4** Passez en revue les renseignements sur le modèle FDM à appliquer au périphérique Géré par FDM, puis cliquez sur **Appliquer le modèle**.
- Étape 5** Dans la ligne **Done (Terminé)**, vous pouvez effectuer les opérations suivantes :
- Vous avez appliqué avec succès la configuration migrée vers le périphérique Géré par FDM sélectionné.
- Cochez la case **Supprimer le périphérique de modèle utilisé pour la migration**.
La sélection de la case à cocher supprime le modèle d'appareil créé à partir de l'ASA en direct. Cela supprimera également le périphérique de modèle, les journaux de migration et les fichiers associés à la migration.
Remarque Cette case à cocher s'affiche uniquement lorsque l'ASA actif est sélectionné dans la page **Inventaire** et uniquement si l'utilisateur a créé le périphérique de modèle.
 - Cochez la case **Enregistrer la configuration migrée comme un modèle**.
Remarque Cette case à cocher s'affiche uniquement lorsque le modèle FDM est appliqué avec succès et est cochée par défaut.
Si la case n'est pas cochée, le modèle FDM n'est pas enregistré.
Si vous rencontrez une erreur lors de l'application du modèle FDM, accédez à **Appareil > Flux de travail** pour afficher les erreurs et résoudre les problèmes.
Remarque Vous pouvez accéder à ces modèles FDM à partir de la page **Appareils et services**. Pour plus de renseignements sur les modèles FDM, consultez [Modèles](#).
Remarque Une fois le modèle FDM enregistré avec succès, vous pouvez effectuer les actions suivantes :
- Effectuez l'une des actions suivantes :
- Cliquez sur **Aperçu et déploiement** pour déployer la configuration.
Vous pouvez vérifier la liste des objets qui seront déployés dans la page **Aperçu et déploiement**.

- Cliquez sur **Go to Devices (Aller vers les appareils)** qui vous offre la possibilité de déployer la configuration.

(Facultatif) Tâches de post-migration

- Accédez au modèle FDM pour examiner les résultats de la migration.
- Optimisez les configurations à l'aide des fonctionnalités CDO.
- Déployez le modèle FDM sur le périphérique.

Prise en charge des périphériques gérés par FDM avec migration de l'interface d'accès de gestion



Remarque La fonctionnalité Apply Template (Appliquer un modèle) n'est pas prise en charge pour un périphérique cible doté d'une interface d'accès de gestion. Modifiez le modèle FDM manuellement avant de l'appliquer sur le périphérique Géré par FDM cible.

Lorsque vous appliquez un modèle FDM migré sur un périphérique cible dont l'interface d'accès de gestion est configurée, la fonctionnalité d'application du modèle échoue en raison d'une incompatibilité dans les interfaces mappées. Sur le périphérique Géré par FDM cible, la configuration de l'interface d'accès de gestion et les routes statiques correspondantes doivent être conservées pour assurer la connectivité avec CDO. Par conséquent, pour éviter les échecs de connectivité, vous devez configurer manuellement les interfaces d'accès de gestion, ainsi que les routes statiques requises en suivant ces étapes, puis appliquer le modèle FDM. Cette section décrit la procédure à suivre pour assurer la réussite de la migration.

S'il existe plusieurs interfaces d'accès de gestion et que les interfaces sont configurées de manière incorrecte ou inutilisées, vous devez mettre à jour le périphérique cible Géré par FDM pour conserver uniquement l'interface d'accès de gestion configurée, afin que les interfaces inutilisées puissent être utilisées pour la configuration migrée.

Procédure

Étape 1

Mettez à jour l'interface physique dans le modèle en modifiant l'adresse IP et le masque de sous-réseau des interfaces de données afin qu'ils soient identiques à ceux de l'interface d'accès de gestion.

Remarque L'interface d'accès de gestion du périphérique Géré par FDM cible doit être mappée avec l'interface d'accès de gestion dans le modèle FDM. L'adresse IP et le masque de sous-réseau du modèle FDM doivent être les mêmes que ceux du périphérique Géré par FDM cible.

- a) Accédez à la page **Inventaire**.
- b) Cliquez sur l'onglet **Modèle**.
- c) Cliquez sur l'onglet **Threat Defense** et sélectionnez le modèle de périphérique FDM.
- d) Choisissez **Interface** dans **Panneau de gestion**.
- e) Cliquez sur **Modifier** dans la boîte de dialogue **Modification de l'interface physique**.
- f) Saisissez l'**adresse IP** et le **masque de sous-réseau de l'hôte distant**.
- g) Cliquez sur **Save** (enregistrer).

Étape 2

Ajoutez l'interface de données en tant qu'interface d'accès de gestion dans les paramètres du modèle :

- a) Accédez à la page **Inventaire**.
- b) Cliquez sur l'onglet **Modèle**.
- c) Cliquez sur l'onglet **Threat Defense** et sélectionnez le modèle de périphérique FDM.
- d) Accédez aux **paramètres** sur le côté droit du volet de **gestion**.
- e) Dans le volet **Interface de données**, cliquez sur + pour ajouter une interface en tant qu'interface d'accès de gestion.

Remarque Assurez-vous que l'interface de données a un nom, un état et l'adresse IP.

- f) Cliquez sur **Save** (enregistrer).

Étape 3

Ajoutez ou mettez à jour les routes statiques avec les interfaces associées sur le périphérique. Lorsque vous mappez l'interface d'accès de gestion à une interface supplémentaire, définissez la configuration de routage pour le périphérique Géré par FDM sélectionné.

Pour plus de renseignements sur l'ajout ou la mise à jour des routes statiques, consultez [Configurer la statique pour les périphériques de menace](#).

Appliquer la migration ultérieurement

Procédure

Étape 1

Sélectionnez **Appliquer la migration plus tard**.

Un modèle de migration est enregistré. Vous pouvez enregistrer le modèle créé et appliquer le modèle au périphérique géré par FDM plus tard.

Remarque Vous pouvez accéder aux modèles FDM à partir de la page **Inventaire**.

Une fois le modèle FDM enregistré avec succès, vous pouvez effectuer les actions suivantes :

- Accédez au modèle FDM pour examiner les résultats de la migration.
- Optimisez le modèle FDM à l'aide des fonctionnalités CDO.
- Accédez au périphérique géré par FDM de destination et sélectionnez le modèle FDM qui doit être appliqué.
- Déployez le modèle FDM sur le périphérique.

Étape 2

Cliquez sur **Done (Terminé)**.

La page **Inventaire** s'affiche avec le modèle FDM présélectionné.

CDO vous permet d'effectuer toutes les actions liées aux modèles, telles que les politiques de révision, les configurations, etc.

Étape 3

Lorsque vous êtes prêt à appliquer le modèle FDM :

1. Sélectionnez l'appareil géré par FDM cible dans la page **Inventaire**.
2. Cliquez sur **Appliquer le modèle** dans le panneau **Actions du périphérique**.

L'écran **Appliquer la configuration du périphérique** s'affiche.

3. Sélectionnez le modèle FDM que vous souhaitez appliquer sur le périphérique.
4. Cliquez sur **Apply**.

Remarque L'adresse IP de l'interface de gestion qui s'exécute sur le périphérique reste inchangée.

Affichez les actions de migration

L'écran du **Tableau de migration** affiche les éléments suivants :

- Le nom de la migration. Par défaut, CDO génère le nom de la migration en fonction du nom du périphérique. Vous pouvez également personnaliser ce nom. Voir ([Facultatif](#)) [Mettre à jour le nom de la migration](#)
- Horodatage de la dernière activité de migration effectuée sur le périphérique.
- Affiche l'état de migration du périphérique. Pour plus de renseignements sur les états de migration, consultez [États de migration et description](#).
- Vous permet d'effectuer diverses actions telles que renommer, télécharger le journal, etc. Pour plus de renseignements sur les actions, consultez [Actions et descriptions](#).

Tableau 1 : États de migration et description

États de migration	Description
Analyse	Migration en cours.
Erreur d'analyse	L'analyse est terminée, avec des erreurs.
Erreur de conversion	La conversion est terminée avec des erreurs.
Modèle créé	La migration est terminée. Le modèle FDM est créé avec succès, mais avec des erreurs de validation.

Pour plus de renseignements sur la correction des erreurs de migration, consultez [Corriger les erreurs de migration](#)

Tableau 2 : Actions et Description

Action	Description
Curriculum vitae	Reprend à partir de l'étape où le processus de migration s'est arrêté. Par exemple, si la migration est terminée, le processus reprend à partir de l'application du modèle FDM.
Renommer	Renommez le nom de la migration.
Flux de travail	Affiche l'écran du flux de travail.

Action	Description
Télécharger le journal	Vous permet de télécharger les fichiers journaux au format TXT. Ceci est un journal d'analyse.
Télécharger le rapport	Vous permet de télécharger les détails du rapport au format HTML.
Configuration	Vous permet d'afficher la configuration ASA par rapport à laquelle la migration a été effectuée.
Supprimer	Supprime la migration et ses fichiers associés, comme les fichiers journaux.

À propos des filtres de migration :

Si vous souhaitez sélectionner un autre appareil ASA ou un modèle à migrer vers le modèle FDM, utilisez l'une des options suivantes :

- Filtrer par appareil
- Filtrer par option Effacer

Filtrer par appareil

Vous pouvez utiliser de nombreux filtres différents sur la page **Migrations** pour trouver les objets que vous recherchez. Le filtre de migrations vous permet de filtrer par périphérique, par état et par intervalle de temps.

Tableau 3 : Attributs de filtre et descriptions

Attribut de filtre	Description
Filtrer par appareil	Vous permet de sélectionner un appareil spécifique pour la migration.
Province	<ul style="list-style-type: none"> • Erreur : affiche la liste de migration basée sur les erreurs d'analyse. • Terminé : affiche la liste de migration basée sur le modèle FDM créé avec succès.
Time Range (plage de temps)	Début, fin : affiche la liste des appareils en fonction des dates de début et de fin de migration sélectionnées.

Filtrer par option Effacer

1. Cliquez sur **Clear (Effacer)** pour effacer la barre de filtre.
2. Cliquez sur l'icône (+).
3. Sélectionnez un appareil dans la liste ou recherchez-le par nom et sélectionnez-le.
4. Cliquez sur **Sélectionner**.

L'écran **Migration FDM** s'affiche.

Déployer la configuration

La dernière étape consiste à déployer les modifications de configuration que vous avez apportées au périphérique.

Pour plus de renseignements, consultez [Déployer la configuration du périphérique](#).

Reportez-vous aux sections [Gestion des appareils FDM avec Cisco Defense Orchestrator](#) et [Gestion de FMC avec Cisco Defense Orchestrator](#) pour savoir comment CDO peut gérer les différents aspects d'un appareil géré par FDM et ses politiques de sécurité.



ANNEXE **A**

Télémétrie

- [Cisco Success Network \(Réseau de succès Cisco\)](#), à la page 25

Cisco Success Network (Réseau de succès Cisco)



Remarque CDO ne gère pas les paramètres de Cisco Success Network. L'interface utilisateur gestionnaire d'appareil gère les paramètres et fournit les renseignements de télémétrie.

Cisco Success Network est un service en nuage activé par l'utilisateur. Lorsque vous activez Cisco Success Network, une connexion sécurisée est établie entre le périphérique et Cisco Cloud pour diffuser des informations et des statistiques d'utilisation.

Pour plus de renseignements, consultez [Cisco Success Network-Telemetry Data](#).



ANNEXE **B**

Foire aux questions

- [FAQ sur la résolution de problèmes, à la page 27](#)

FAQ sur la résolution de problèmes

- Q.** Pourquoi l'analyse prend-elle plus de temps?
- A.** Si la taille du fichier de configuration ASA est importante, l'analyse prend plus de temps. Le fichier de configuration en cours d'exécution de votre ASA doit faire moins de 4,5 Mo et compter 22 000 lignes. Pour plus de renseignements, consultez [Confirmation de la taille de la configuration d'exécution ASA](#).
- Q.** Que dois-je faire lorsque je trouve des erreurs d'analyse lors de la migration?
- A.** Reportez-vous à **Examiner le rapport de migration** et à **Examiner les journaux de migration** pour les détails de l'erreur.
- Q.** Je rencontre des erreurs d'analyse lors de la migration. Comment les corriger?
- A.** Accédez à la page **Migration**, cliquez sur **Download Logs (Télécharger les journaux)** pour le périphérique en question et corrigez les erreurs.
- Q.** J'obtiens des erreurs de conversion lors de la génération du modèle FDM. Que dois-je faire?
- A.** Accédez à la page de **Migration**, cliquez sur **Flux de travail** du périphérique spécifique pour afficher les erreurs.
- Q.** Que faire lorsqu'un modèle FDM est créé avec des erreurs?
- A.** Si votre modèle FDM est créé avec des erreurs de validation, vous pouvez rechercher le modèle FDM dans la page **Inventaire**. Cliquez sur **Flux de travail** dans le panneau **Devices Actions (Actions des périphériques)** où vous pouvez afficher les détails de l'erreur.
- Q.** CDO ne parvient pas à écrire dans le journal des modifications. Pourquoi?
- A.** Lorsque vous intégrez une ASA à CDO, CDO enregistre une copie du fichier de configuration en cours d'exécution de l'ASA dans sa base de données. En règle générale, si ce fichier de configuration en cours d'exécution est trop volumineux (4,5 Mo ou plus), s'il contient trop de lignes (environ 22 000 lignes) ou s'il y a trop d'entrées de liste d'accès pour un seul groupe d'accès, CDO ne pourra pas le faire. gérer ce périphérique de manière prévisible. Pour plus de renseignements, consultez [Confirmation de la taille de la configuration d'exécution ASA](#).

Vous pouvez également contacter votre équipe de compte Cisco pour obtenir de l'aide afin de réduire en toute sécurité la taille de votre fichier de configuration sans perturber vos politiques de sécurité.

- Q.** CDO valide-t-il la syntaxe du fichier de configuration ASA avant sa migration?
- A.** Non. CDO ne valide pas la syntaxe du fichier de configuration ASA avant de le migrer vers un modèle FDM. Si vous essayez de migrer un modèle ASA que vous avez intégré vers CDO et que la migration échoue, consultez le rapport de migration et le journal de migration dans l'écran de migration FDM. Vous devrez peut-être vérifier la syntaxe du fichier de configuration.
- Q.** Pourquoi certaines de mes listes d'accès et objets réseau n'ont-ils pas été migrés?
- A.** CDO migre uniquement les objets référencés. Les objets d'une liste de contrôle d'accès, qui sont définis, mais non référencés à un groupe d'accès, ne sont pas migrés. De plus, certaines des raisons courantes pour lesquelles CDO ne parvient pas à migrer certains éléments peuvent être l'une ou plusieurs des raisons suivantes :
- Listes d'accès ICMP sans code ICMP
 - Listes d'accès TCP/UDP sans configuration de groupe d'accès
 - Listes d'accès IP non mappées aux profils VPN de site à site
 - Tout objet réseau ou groupe faisant référence à des listes d'accès qui ne fait pas l'objet d'une migration
 - Interfaces appelées arrêt

Consultez le **Rapport de migration** pour plus de renseignements sur les éléments qui n'ont pas été migrés.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.