

Migration de FMC sur site vers le cloud (cdFMC) avec contrôle du cloud de sécurité

Table des matières

[Problème](#)

[Environnement](#)

[Résolution](#)

[Motif](#)

[Autres informations utiles](#)

- [Problème](#)
 - [Environnement](#)
 - [Résolution](#)
 - [Motif](#)
 - [Autres informations utiles](#)
-

Problème

Un utilisateur a besoin d'aide pour migrer son appliance virtuelle de production Firewall Management Center (FMCv300) vers un FMC fourni dans le cloud (cdFMC) dans le locataire Security Cloud Control (SCC). Les préoccupations particulières comprennent :

- Déterminez quelles parties du processus de migration peuvent provoquer des temps d'arrêt et comment minimiser l'impact sur la production.
- Obtenez des instructions détaillées sur le workflow de migration.
- Déterminez ce que vous devez faire avec le FMCv300 une fois la migration terminée.
- Planifier une approche de migration progressive pour plusieurs périphériques Firewall Threat Defense (FTD) dans des configurations à haute disponibilité (HA).
- Précisez si la configuration FMC locale doit être importée manuellement dans cdFMC avant de lancer l'assistant de migration.

Environnement

- Source FMC : Appareil virtuel FMCv300, version 7.6.5. D'autres plates-formes matérielles (HW) et logicielles (SW) peuvent également être déployées.
- Target (cible) : Client cdFMC provisionné.
- Les périphériques gérés sont des FTD de différentes versions matérielles et logicielles, par exemple :
 - 2x Secure Firewall 3130, FTD 7.6.4, configuré en paire haute disponibilité.
 - 2x Firepower 2130, FTD 7.4.4, configuré en paire haute disponibilité.
 - 1x FTDv dans Azure, 7.6.4, configuration autonome.

Résolution

Conditions préalables à la migration et validation des versions

Les versions d'environnement répondent aux conditions requises pour la migration vers cdFMC :

- FMC 7.6.5 répond aux exigences minimales documentées pour le workflow de migration.
- Les versions FTD 7.6.4 et 7.4.4 correspondent au minimum documenté pour la migration.
- cdFMC prend en charge les catégories de version FTD dans l'environnement.

Étapes de validation avant la migration

Avant de lancer la migration, validez les conditions suivantes :

- Aucun déploiement en attente sur FMCv300.
- Les deux paires haute disponibilité sont saines et synchronisées.
- Sauvegarde FMCv300 terminée.
- Espace disque FMC suffisant disponible (au moins 10 % libre).
- Résolution DNS à partir du chemin de gestion FTD.
- Connectivité sortante autorisée des interfaces de gestion FTD vers cdFMC sur les ports de gestion du cloud requis (TCP 443 et TCP 8305).

- FMCv300 dispose d'un accès HTTPS sortant à SCC.

Processus d'importation de configuration

Il n'est pas nécessaire d'importer manuellement la configuration FMCv300 sur site dans cdFMC avant d'exécuter l'assistant de migration. Le workflow « Migrate FTD to cdFMC » gère l'importation de la configuration dans le cadre de la tâche de migration :

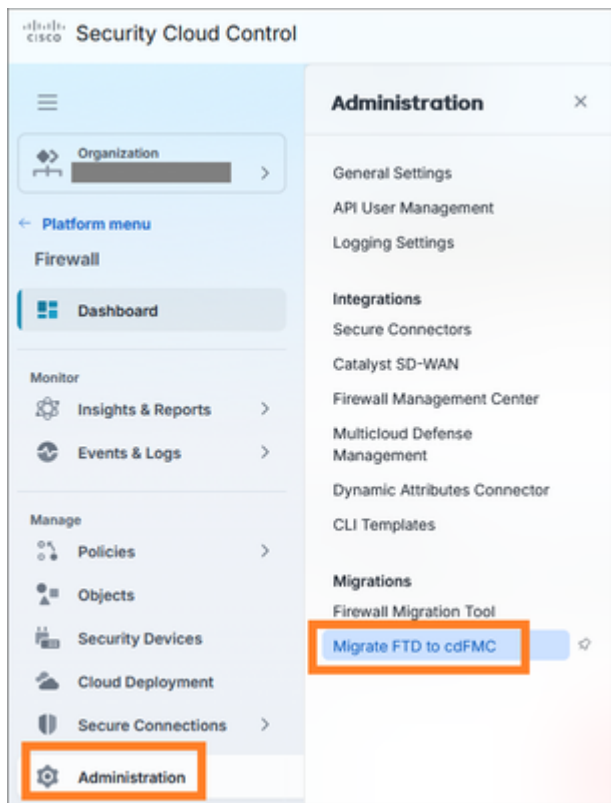
1. Le SCC se connecte au FMCv300 local.
2. Il exporte la configuration appropriée à partir du FMC local.
3. Il importe des politiques/objets partagés dans cdFMC.
4. Il importe la configuration spécifique au périphérique, telle que les interfaces et le routage.
5. Il enregistre les périphériques FTD sélectionnés sur cdFMC.
6. La période d'évaluation de 14 jours commence une fois la migration terminée.

Si vous créez manuellement des stratégies ou des objets dans cdFMC avant la migration avec les mêmes noms que les éléments sur le FMCv300, le flux de travail de migration peut utiliser l'élément cdFMC existant au lieu d'importer la version locale, ce qui peut entraîner des résultats inattendus.

Séquence de migration recommandée

Phase 1 : Configuration préalable à la migration

1. Déployez cdFMC dans votre client SCC.
2. Intégrez le FMCv300 actuel au SCC.
3. Confirmez les licences Smart pour cdFMC.
4. Démarrez le workflow de migration à partir de Firewall > Administration > Migrations > Migrate FTD to cdFMC :



5. Utilisez l'option de pause après l'importation de la stratégie partagée pour révision :

 **Security Cloud Control**

Migrate FTD to cdFMC

Migrate FTD from On-Prem FMC to cloud

Organization

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Cloud Deployment

Secure Connections

Administration

Platform services

Favorites

Security Devices

Platform Management

1 Before you begin

2 Select On-Prem FMC **On-Prem FMC: FMC**

3 Select Devices

Select FTD device(s) to migrate from On-Prem FMC to cloud, and specify an action in bulk or per device.

Last Synced time : 7 minutes ago [Sync from On-Prem FMC now](#)

Search Name

☐	Name	Domain
☐	FTD3140-HA	Global

0 device(s) selected

☒ Pause migration to review imported shared policy ⓘ

☐ Auto deploy to FTDs after successful migration ⓘ

Migrate FTD to cdFMC

Phase 2 : Exécution de la migration

Au cours de la fenêtre de maintenance, migrez les périphériques selon une approche progressive :

1. Commencez par le FTD autonome (impact le plus faible).
2. Migrez la première paire haute disponibilité.
3. Valider l'intégrité et les fonctionnalités du périphérique.
4. Migrez la deuxième paire haute disponibilité.

Phase 3 : Validation post-migration

Après chaque migration de périphérique ou de paire haute disponibilité :

1. Vérifiez l'état du périphérique dans cdFMC.
2. Confirmez l'état HA, le cas échéant.
3. Consulter les aperçus/avertissements de déploiement.
4. Déploiement depuis cdFMC.
5. Validez le trafic et la visibilité des événements.

Plan de migration en trois phases avec gel de la configuration

L'approche recommandée consiste à effectuer des migrations FTD en trois phases, chacune se déroulant à des dates distinctes, avec un minimum de trois jours de surveillance post-mise en service par phase. Cette approche réduit les risques et permet de valider les éléments suivants :

- Déploiement de politiques à partir de cdFMC.
- État de santé du périphérique.
- État de haute disponibilité pour les deux paires haute disponibilité.
- Visibilité des événements/analyses dans le cloud.
- Tout problème opérationnel avant de passer à la phase suivante.

Implémentation du gel de configuration

Mettez en oeuvre un gel de la configuration pendant la période de migration/d'évaluation avec cette approche :

- Meilleure option : Gelez toutes les modifications de configuration liées à FTD sur FMCv300 et cdFMC jusqu'à ce que chaque phase soit validée et validée.
- Option minimale : Gelez les périphériques migrés ainsi que les politiques/objets partagés utilisés par les périphériques migrés et non migrés.
- Évitez de modifier les mêmes politiques/objets partagés dans FMCv300 et cdFMC lors de la migration progressive.
- Éviter les modifications majeures pendant la période d'évaluation.

processus de modification d'urgence

Pour les changements urgents pendant la migration :

- Appliquez la modification uniquement au gestionnaire faisant autorité actuel pour ce périphérique :
 - Périphériques non encore migrés : FMCv300.
 - Périphériques déjà migrés : cdFMC.
- Documentez la modification, la stratégie/l'objet affecté, l'horodatage et la portée du périphérique.
- Rapprochez la modification une fois la phase terminée, en particulier si elle affecte les objets partagés ou les stratégies partagées.

Gestion de la période d'évaluation

Considérations importantes pour la fenêtre d'évaluation de 14 jours :

- Suivez la fenêtre d'évaluation de 14 jours pour chaque phase/tâche de migration.
- Ne laissez aucune phase atteindre la validation automatique de manière involontaire.
- Si la surveillance de trois jours est réussie, validez cette phase manuellement au lieu d'attendre les 14 jours complets.

Processus de déclassement FMCv300

Ne mettez pas le FMCv300 hors tension ni ne le retirez immédiatement après la migration du périphérique. Maintenez le FMCv300 disponible jusqu'à :

- Tous les périphériques FTD ont été correctement migrés.
- Les déploiements de cdFMC ont réussi.
- Les analyses/événements cloud sont confirmés.
- La migration est engagée.

- Toutes les exigences de conservation des journaux/événements sont satisfaites.
- Une sauvegarde FMCv300 finale est conservée conformément à la politique de l'entreprise.

Une fois ces conditions remplies, FMCv300 peut être retiré de l'utilisation active et mis hors service conformément aux processus de retrait standard des machines virtuelles.

Motif

Il s'agit d'une migration planifiée de FMC sur site vers cdFMC. La migration est motivée par la nécessité d'exploiter les fonctionnalités de gestion basées sur le cloud et de mettre hors service l'appliance virtuelle FMCv300 existante.

Autres informations utiles

- [Migration de FTD vers cdFMC - Documentation Cisco](#)
- [Assistance technique de Cisco et téléchargements](#)

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.