Dépanner l'erreur de licence FMC Host Limit : " ; Il vous reste 0 licence hôte FireSIGHT sur xxxxxx" ;

Table des matières

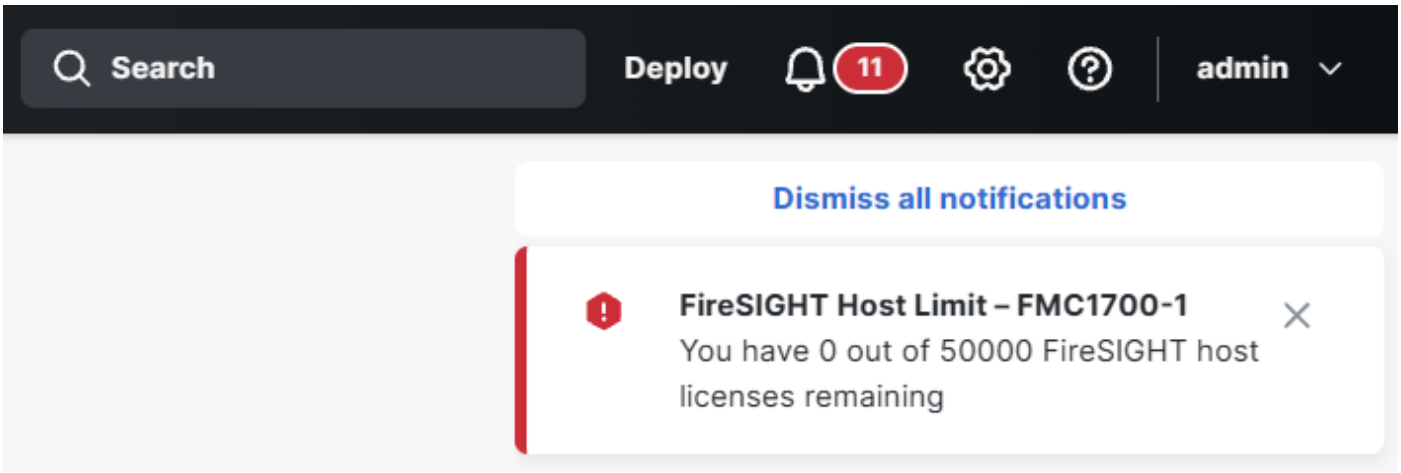
Problème

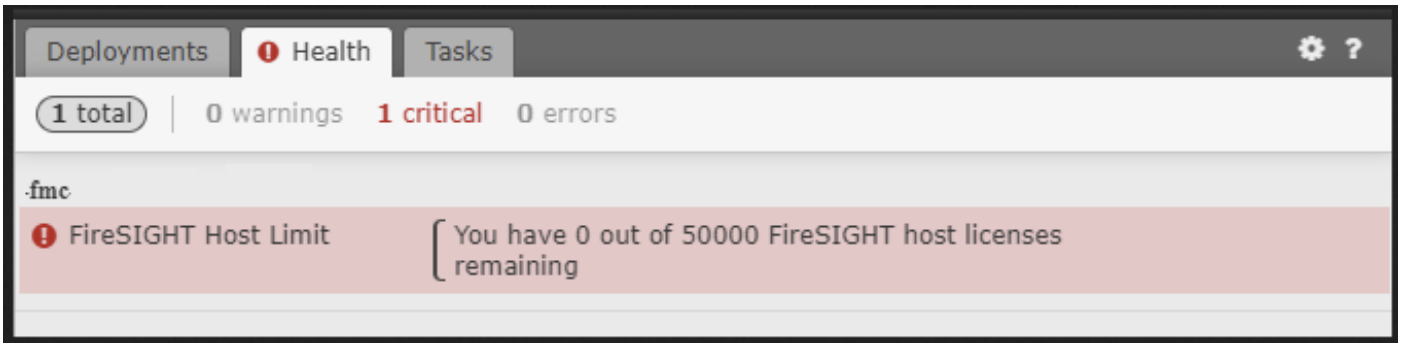
Un FMC (Firewall Management Center) affiche une alerte d'intégrité indiquant que la limite de licence hôte a été atteinte. Le message d'erreur spécifique indique :

Limite d'hôtes FireSIGHT - [nom d'hôte FMC]

Il vous reste 0 licence hôte FireSIGHT sur xxxxxx

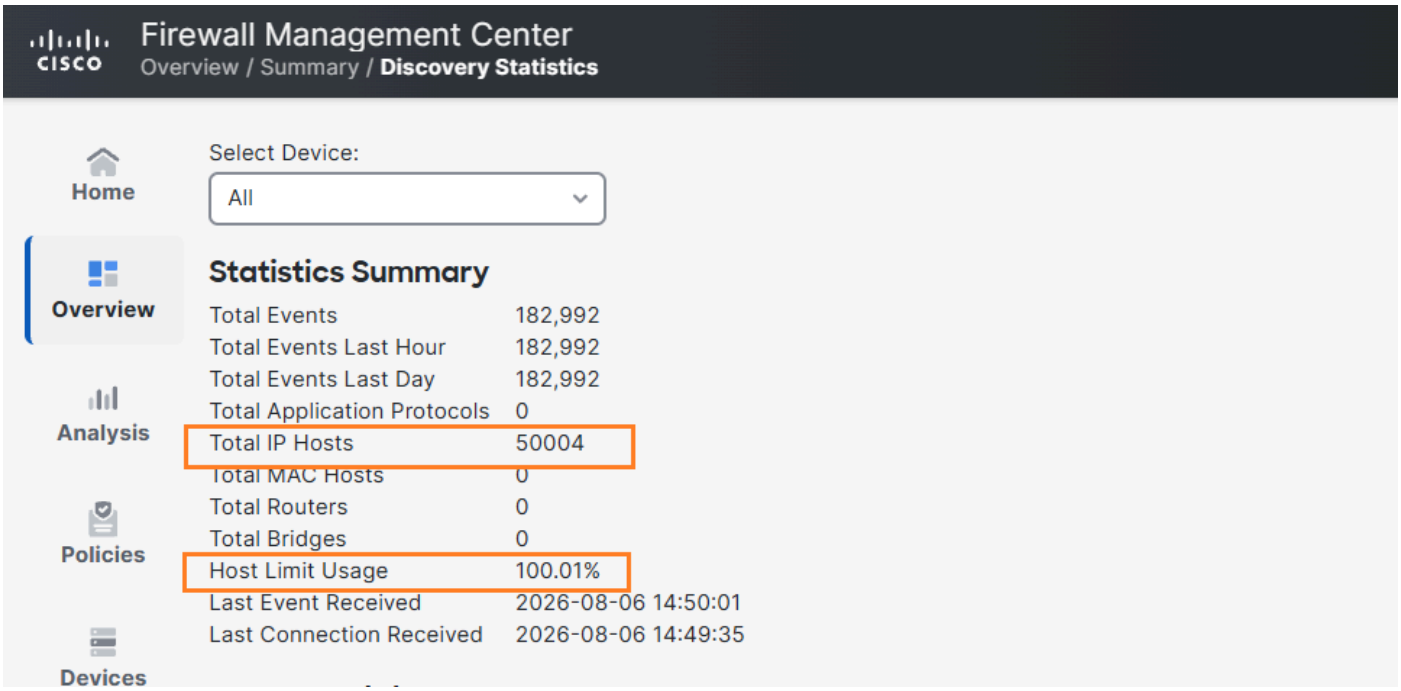
Exemples:





Remarque : Le nombre total de licences d'hôte dépend de la plate-forme FMC.

En outre, dans la page Overview > Summary > Discovery Statistics, il affiche 100% d'utilisation :



Environnement

- FMC 7.7.10. D'autres versions logicielles peuvent également être affectées.
- Détection réseau configurée avec le suivi d'hôte activé.

Résolution

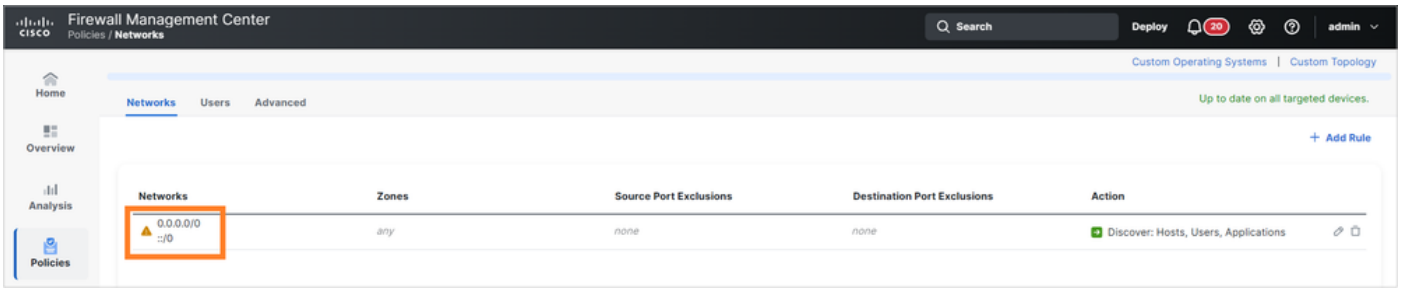
L'alerte de limite d'hôte FMC ne provoque pas de panne du trafic du pare-feu. Le contrôle et l'inspection des accès continuent de fonctionner normalement. L'impact principal est sur la visibilité de l'hôte et le suivi du contexte dans le FMC.

Cette notification apparaît lorsque le FMC a atteint sa capacité maximale de suivi des hôtes dans le mappage réseau et la base de données des hôtes.

Analyse du périmètre de découverte du réseau :

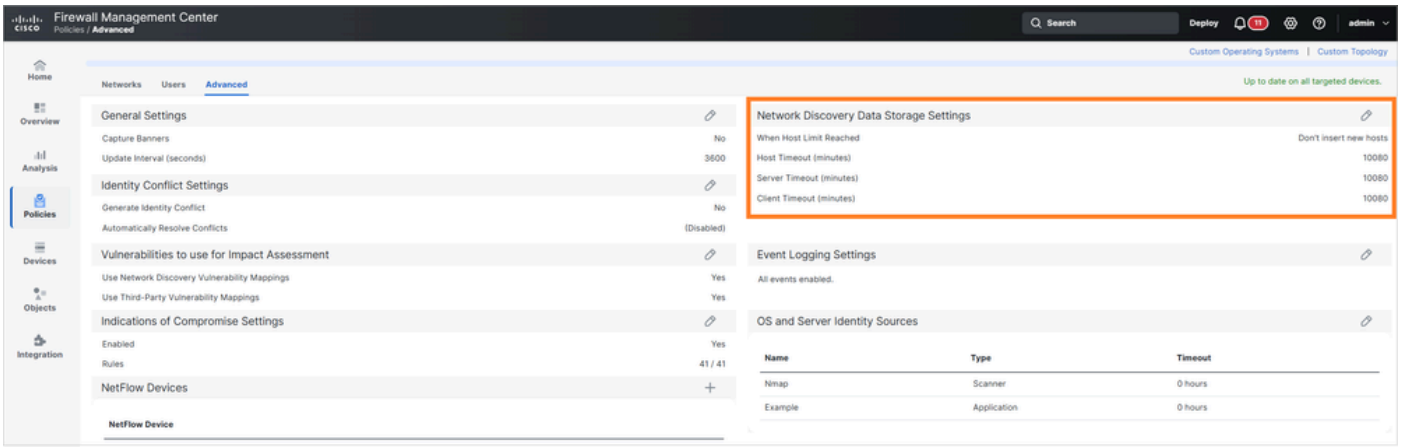
Assurez-vous que la détection est limitée aux réseaux internes requis uniquement. Évitez de découvrir des plages d'adresses publiques, NAT, invité, équilibreur de charge ou transitoires inutiles, sauf si cela est nécessaire pour la visibilité de la sécurité.

Dans ce cas, vous devez modifier la configuration de détection de réseau et spécifier uniquement les réseaux internes que vous souhaitez surveiller. Sinon, les hôtes externes (Internet) peuvent remplir votre base de données de découverte :



Analyse de la configuration actuelle

Vérifiez la limite actuelle de l'hôte en examinant les paramètres de détection du réseau dans Politiques > Détection du réseau > Avancé > Détection du réseau Paramètres de stockage des données :



La configuration affiche généralement :

- Lorsque la limite d'hôtes a été atteinte : Ne pas insérer de nouveaux hôtes
- Délai d'attente hôte : 10080 minutes / 7 jours
- Délai du serveur : 10080 minutes / 7 jours
- Délai du client : 10080 minutes / 7 jours

Avec le paramètre actuel « Ne pas insérer de nouveaux hôtes » et la base de données d'hôtes pleine, FMC n'ajoute pas les nouveaux hôtes découverts tant que le nombre d'hôtes n'est pas inférieur à la limite, ce qui entraîne une visibilité incomplète de l'hôte.

Modification de configuration facultative

Vous pouvez modifier le comportement de la limite d'hôtes pour permettre le suivi continu des hôtes actifs :

Étape 1: Accédez à Policies > Network Discovery.

Étape 2: Cliquez sur l'onglet Avancé.

Étape 3: Sous Network Discovery Data Storage Settings, cliquez sur Edit.

Étape 4: Remplacez When Host Limit Reached par « Don't insert new hosts » et par Drop hosts.

Étape 5: Enregistrez les modifications.

Étape 6: Déployez la configuration pour appliquer les modifications.

Impact et comportement attendus

Avec le paramètre « Drop hosts » activé :

- Aucune panne de trafic de pare-feu attendue.
- Le contrôle et l'inspection des accès se poursuivent normalement.
- FMC supprime l’hôte inactif le plus longtemps du mappage réseau lors de l’ajout d’hôtes nouvellement découverts.
- Le suivi continu des hôtes actuellement actifs est maintenu.
- Le contexte d'hôte historique des hôtes supprimés ne peut plus être visible tant que ces hôtes ne sont pas de nouveau actifs.

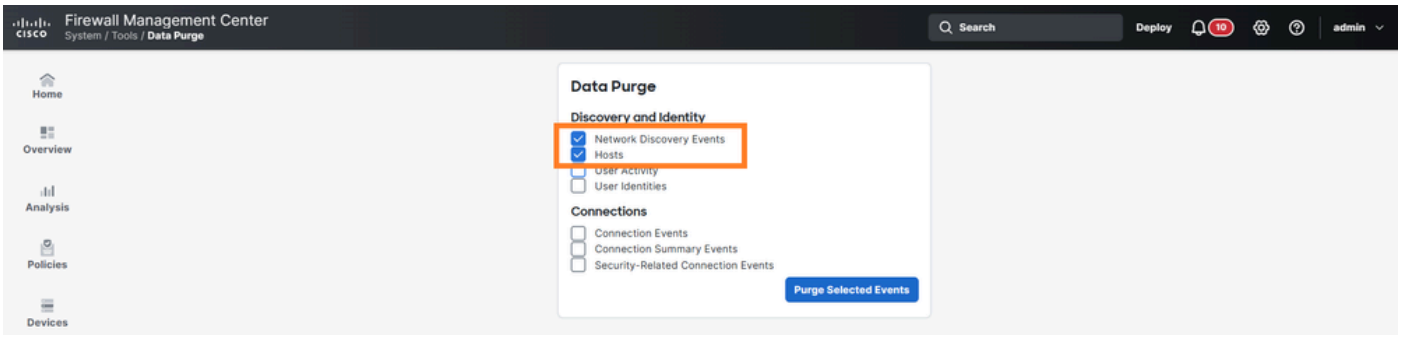
Vérification du délai d'attente hôte :

Les valeurs de délai d'attente par défaut de 10080 minutes (7 jours) sont généralement appropriées. N’envisagez de procéder à des ajustements que si les hôtes inactifs sont conservés trop longtemps.

Nettoyage manuel de l'hôte (si nécessaire) :

Si une réduction immédiate du nombre d'hôtes est nécessaire, les hôtes obsolètes peuvent être supprimés de Analysis > Hosts > Table View of Hosts. Notez qu’il ne s’agit que d’une action de nettoyage. Si la portée de la détection reste trop large, FMC redécouvrira les mêmes hôtes.

Vous pouvez également purger tous les hôtes de la base de données de découverte à partir de Système > Outils > Purger les données :



Motif

La limite de licence d'hôte FireSIGHT est atteinte lorsque le FMC a détecté et effectue le suivi du nombre maximal d'hôtes dans sa carte réseau et sa base de données d'hôtes. Les facteurs contributifs courants sont les suivants :

- Étendue de la découverte du réseau configurée de manière trop large, y compris les plages d’adresses externes ou publiques inutiles.
- Découverte d’adresses NAT, d’équilibreur de charge ou transitoires qui consomment des licences d’hôte.
- Paramètres de délai d’attente des hôtes qui conservent les hôtes inactifs pendant de longues périodes.
- La croissance naturelle du réseau atteint la limite de capacité de l’hôte FMC.

Autres informations utiles

- Guide de configuration des périphériques Cisco Secure Firewall Management Center - Stratégies de détection de réseau
- 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.