Atténuer “ ; Non disponible” ; État des fonctions de sécurité

Table des matières

Introduction

Exigences

- Conditions préalables

Solution

- Supprimer le remplacement de l'ordinateur pour revenir au niveau du cluster

Informations connexes

Introduction

Ce document décrit comment dépanner et résoudre les fonctions de sécurité ESA et CES affichant « Non disponible » sur les politiques de messagerie.

Contribution d'Alan Macorra et de Mathew Huynh Ingénieurs Cisco CX.

Exigences

Conditions préalables

- Tout ESA (Email Security Appliance)/CES (Cloud Email Security) sur toute version d'AsyncOS.
- Périphérique sous licence avec clés de fonction disponibles pour les services de sécurité.
- Compréhension des différents niveaux de configuration et de remplacement des clusters.

Fond

Le périphérique ESA (Email Security Appliance)/CES (Cloud Email Security) n'exécute aucune analyse de sécurité à partir de services tels que :

- Antispam

- Antivirus
- Protection avancée contre les malwares
- Graymail
- Filtres contre les attaques
- DLP (sortant uniquement)

Les touches de fonction sont disponibles et peuvent être vérifiées sur l'interface graphique ou l'interface de ligne de commande.

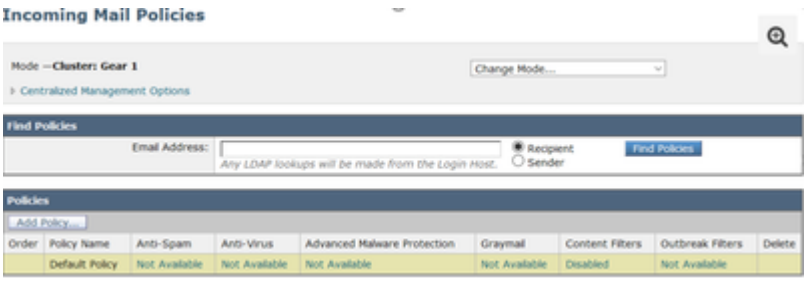
IUG: Administration système > Touches de fonction

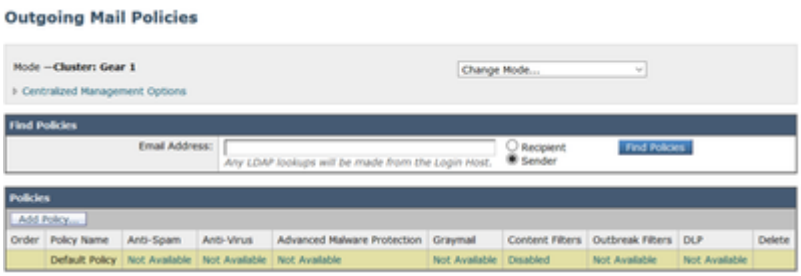
CLI : touches de fonction

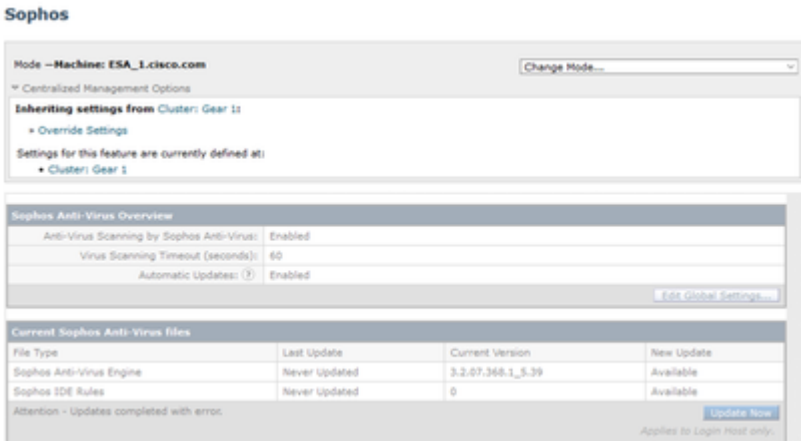
Les fonctions de sécurité des stratégies de messages entrants et sortants affichent « Non disponible » même si le service est activé.

Problème

- Les touches de fonction sont disponibles sur le périphérique, mais les services affichent « Non disponible » lors de l'exécution d'analyses.
- Lorsque vous cliquez sur le lien « Non disponible » dans les stratégies de messagerie, il redirige vers les paramètres globaux de ce service de sécurité spécifique. Le service est alors activé et l'imposition de modifications ne modifie pas l'état « Non disponible » sur les stratégies de messagerie.







Solution

Ce problème se produit lorsque les clés de fonction expirent avant le renouvellement et la réinstallation de la licence. Dans ce cas, le Contrat de licence d'utilisateur final (CLUF) doit être accepté à nouveau. Comme les périphériques ont été activés avant l'expiration, les clés de fonction initiales ont été réinstallées/renouvelées, le CLUF n'a pas été présenté à nouveau et le ou les périphériques ont été définis au niveau du cluster.

Pour résoudre ce problème, vous devez remplacer les paramètres de l'ESA/CES par des paramètres de niveau machine afin de permettre au CLUF de se présenter pour acceptation. Ce faisant, le périphérique enregistre les clés pour le renouvellement et réactive les fonctionnalités.

Remarque : Le mode de configuration auquel vous êtes actuellement connecté s'affiche dans l'angle supérieur gauche où il affiche Mode — Cluster/Group/Machine. Selon le mode, ce qui est affiché peut être différent de la sortie initiale fournie, qui est déjà en Mode Machine.

Avertissement : Lors de la création de remplacements pour cette solution, assurez-vous que vous NE sélectionnez PAS Move Configuration, car cela force la configuration au niveau du cluster dans un mode non configuré pour le service spécifique. Si cette option est sélectionnée lors de la suppression de la substitution, la fonctionnalité revient à l'état non configuré (non activé).

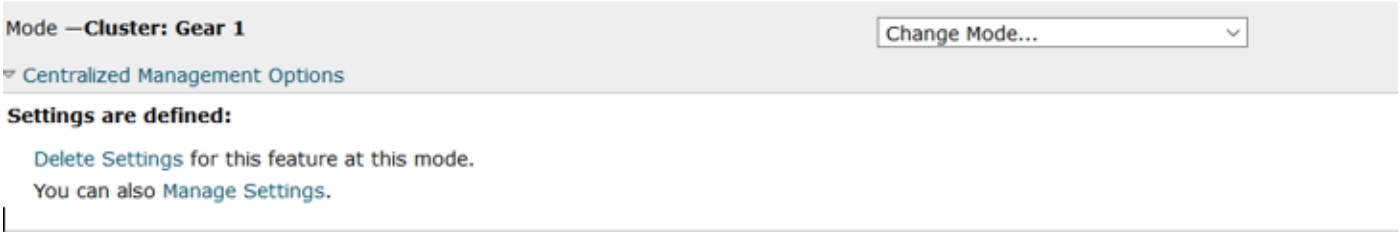
Sur chaque service de sécurité qui affiche "Non disponible" :

1. Cliquez sur le lien Non disponible de la page Stratégies de messages entrants ou sortants.
2. Cette commande redirige vers les paramètres globaux par moteur.
3. Sélectionnez Change Mode... et, dans le menu déroulant, sélectionnez la machine actuellement connectée.

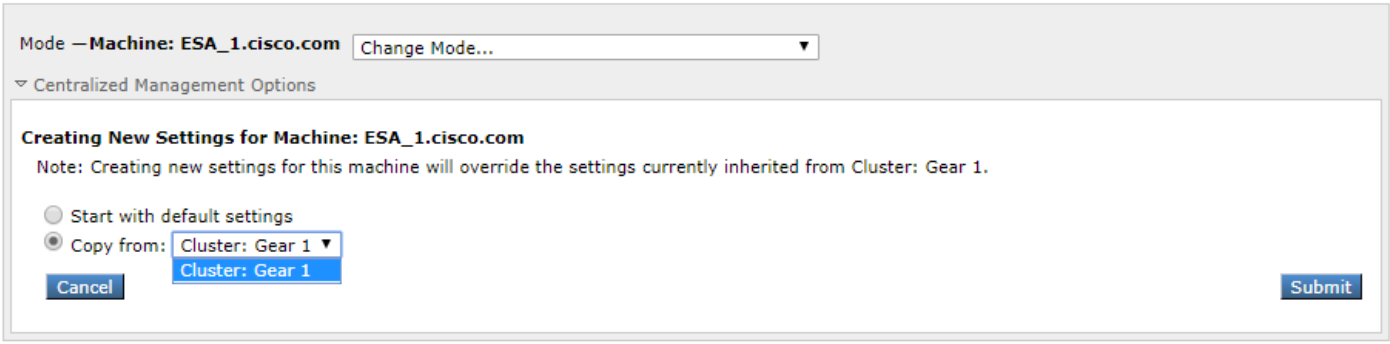
4. Cliquez sur Override Settings.
5. Sélectionnez Copier à partir de : Cluster (copie les paramètres actuellement activés du niveau du cluster vers votre ordinateur).
6. Cliquez sur Submit.
7. La configuration indique qu'elle est activée. Cliquez sur le bouton Edit Global Settings (Modifier les paramètres généraux).
8. Le CLUF s'affiche. Vous pouvez le lire et l'accepter.
9. Validez les modifications en enregistrant ce paramètre.
10. Répétez les étapes pour vos autres fonctions, qui nécessitent une réactivation.

Exemple de résultat :

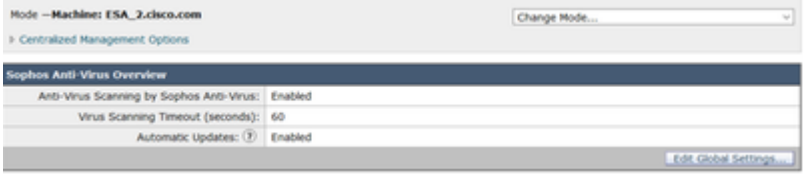
À l'aide de la liste déroulante de droite, changez-la pour la machine à laquelle vous êtes connecté :



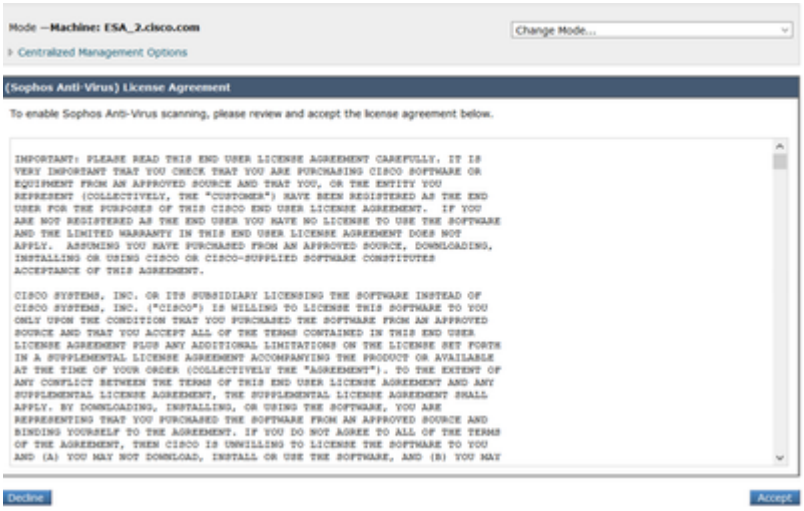
Copie des paramètres du cluster vers le remplacement de l'ordinateur :



Sortie du paramètre de remplacement :



Après avoir cliqué sur Modifier les paramètres généraux... le CLUF s'affiche :



Acceptez le CLUF et les modifications que vous avez apportées.

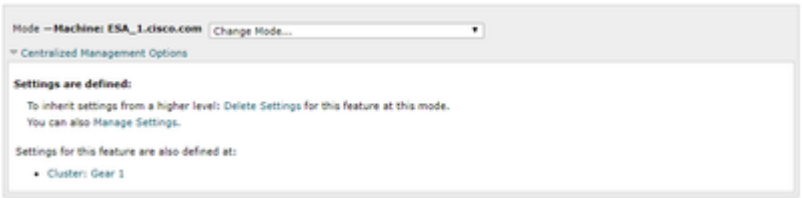
Les paramètres de Sophos sont reflétés dans la stratégie de messagerie et ne sont plus affichés comme « Non disponible ».

Supprimer le remplacement de l'ordinateur pour revenir au niveau du cluster

Pour supprimer les paramètres de remplacement de la machine :

1. Accédez à Machine Mode dans le menu déroulant.
2. Cliquez pour développer les options de gestion centralisée.
3. Cliquez sur le bouton Delete Settings.
4. Cliquez sur le bouton Delete et les paramètres reviennent au niveau supérieur (Group ou Cluster, selon la configuration).
5. Vérifiez que les paramètres sont correctement configurés au niveau supérieur sélectionné.
6. Validez les modifications pour enregistrer ce paramètre.

Exemple de résultat :



Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- Assistance et documentation techniques - Cisco Systems

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.