Console AMP for Endpoints et dernier filtre détecté

Contenu

Introduction

Ce document décrit l'explication du bogue de filtre « Last Seen » référencé à CSCvh31177 dans Advanced Malware Protection (AMP) for Endpoints.

Contribué par Caly Hess, ingénieur Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au tableau de bord Cisco AMP for Endpoints

Components Used

Les informations de ce document sont basées sur le logiciel :

- Cisco AMP for Endpoints for Endpoints version 5.4.20190917

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.

Problème

Le filtre « Dernière vue » de la page des ordinateurs de la console affiche les connecteurs qui ont été vus au cours des dernières 24 heures et qui apparaissent dans la liste.

Motif

L'attraction actuelle des données « Last Seen » est un travail singulier toutes les 24 heures. Bien que les données qui sont reflétées dans la page Ordinateurs et la sortie pour Exporter vers CSV pour « Last Seen » soient en temps réel, le filtre lui-même exécute les données battues à partir de cette tâche unique. Ceci a été mis en oeuvre pour accélérer les

résultats, car l'analyse en temps réel des horodatages des environnements des grandes entreprises pourrait entraîner des délais d'attente et un verrouillage de la base de données.

Explication des ordinateurs récemment vus dans un filtre de plus de 7 jours

La machine a été déconnectée pendant plus de 7 jours jusqu'à l'exécution du travail « Last Seen ».

Exemple concret

- HostA.randomdomain.net a eu un malheureux accident avec une tasse de café complète et la carte mère n'a pas complètement récupéré le 10 août
- HostA.randomdomain.net se trouve maintenant dans le dépôt de réparation jusqu'au 20 septembre
- Le 21 septembre dernier, HostA.randomdomain.net revient sur le réseau 4 heures après l'exécution du travail « Last Seen », mais 2 heures avant que l'Auditeur effectue une exportation vers CSV des ordinateurs non vus depuis les 30 derniers jours
- HostA.randomdomain.net figure toujours dans la liste de la tâche « Dernière vue » comme étant de plus de 30 jours non vu. Bien qu'il soit maintenant pleinement fonctionnel et sans café, le vérificateur l'attrape maintenant dans son exportation « inactive »

Solution à court terme

Le travail lui-même ne prend pas 24 heures, mais il peut en prendre au moins 12. Afin d'améliorer la précision du filtre, le rééchelonnement automatique de la tâche après la fin de la précédente est en cours de développement, qui devrait couper entre 7 et 12 heures de temps de la fenêtre de traitement par lots.

Solution à long terme

Refonte totale du mécanisme « Dernière vue » qui est plus proche en temps réel lorsque les données sont retirées. Cette solution nécessite la mise en oeuvre d'une structure de base de données entièrement nouvelle qui est en cours d'élaboration avec la publication proposée au cours de la prochaine année civile.