AMP pour la console de points finaux et le dernier filtre vu

Contenu

Introduction

Ce document décrit l'explication de la « dernière » bogue vue de filtre référencée à CSCvh31177 dans la protection avancée de malware (AMP) pour des points finaux.

Contribué par Caly Hess, Cisco machinent.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Access à l'AMP de Cisco pour le tableau de bord de points finaux

Composants utilisés

Les informations dans ce document sont basées sur le logiciel de thede :

- L'AMP de Cisco pour des points finaux pour des points finaux consolent la version 5.4.20190917

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Le filtre pour « dernier vu » de la page d'ordinateurs sur la console, connecteurs d'affichages qui ont été vus pendant les 24 dernières heures qui apparaissent sur la liste.

Motif

La traction en cours des « dernières » données vues est un travail singulier toutes les 24 heures. Bien que les données qui sont reflétées dans la page d'ordinateurs et la sortie pour l'exportation à CSV pour « dernier vu » soient en temps réel, le filtre lui-même coule des données par lot de ce travail singulier. Ceci a été mis en application pour augmenter la

vitesse des résultats, en tant qu'analyse en temps réel des horodateurs pour de grands environnements d'entreprise pourrait mener aux minuteries et au verrouillage de base de données.

Explication des ordinateurs « récemment vus » dans un filtre du jour 7+

L'ordinateur était hors ligne pendant les jours 7+ jusqu'après que le « dernier » travail vu a fonctionné.

Exemple du monde réel

- HostA.randomdomain.net a eu un accident fâcheux avec une pleine tasse de coffee et la carte mère n'a pas fait un plein 10ème de reprise en août
- HostA.randomdomain.net se repose maintenant dans le dépôt de réparation jusqu'au 20 septembre
- Le 21 septembre, les retours de HostA.randomdomain.net au réseau pendant 4 heures après que le « dernier » travail vu a fonctionné mais 2 heures avant que l'auditeur fait une exportation à CSV des ordinateurs non vus pour les 30 derniers jours
- HostA.randomdomain.net est encore répertorié du « dernier » travail vu en tant qu'ayant lieu plus de 30 jours non vus. En dépit de lui est maintenant entièrement - fonctionnel et coffee libres, l'auditeur l'attrape maintenant dans son exportation « inactive »

Solution à court terme

Le travail lui-même ne prend pas de pleines 24 heures pour fonctionner, mais il peut prendre au moins 12. Afin d'augmenter la précision du filtre, la remise à plus tard automatique pour le travail après que le précédent se termine est en cours de développement, qui est attendu pour couper n'importe où de 7-12 heures de repos la fenêtre en lots.

Solution à long terme

Une reprise totale du « dernier » mécanisme vu qui a lieu plus près d'un temps réel où les données sont tirées. Cette solution exige l'implémentation d'une structure de base de données entièrement nouvelle qui est actuellement à l'étude avec la release proposée pendant l'année calendaire suivante.