AMP für Endgeräte-Konsole und der Filter für die letzte Erkennung

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Problem](#)
[Ursache](#)
[Erläuterung der "kürzlich erkannten" Computer in einem 7+ Tage-Filter](#)
[Praxisbeispiel](#)
[Kurzfristige Lösung](#)
[Langfristige Lösung](#)

Einführung

Dieses Dokument beschreibt die Erklärung des "Last Seen"-Filterfehlers, auf den CSCvh31177 in Advanced Malware Protection (AMP) für Endgeräte verweist.

Mitarbeiter: Caly Hess, Cisco Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriff auf das Dashboard von Cisco AMP für Endgeräte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Software:

- Cisco AMP für Endgeräte Konsolenversion 5.4.20190917

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Der Filter "Last Seen" (Letzte Anzeige) von der Computerseite der Konsole zeigt Anschlüsse an, die in den letzten 24 Stunden angezeigt wurden und in der Liste angezeigt werden.

Ursache

Das aktuelle Abrufen von Daten aus "Last Seen" ist eine einmalige Aufgabe alle 24 Stunden. Obwohl die Daten, die auf der Seite Computer angezeigt werden, und die Ausgabe für "Letztes Mal in CSV exportieren" in Echtzeit erfolgt, wird der Filter selbst von den Batch-Daten dieses einzelnen Auftrags ausgeführt. Dies wurde implementiert, um die Ergebnisse zu

beschleunigen, da eine Echtzeitanalyse der Zeitstempel für große Unternehmensumgebungen zu Zeitüberschreitungen und zum Sperren von Datenbanken führen könnte.

Erläuterung der "kürzlich erkannten" Computer in einem 7+ Tage-Filter

Die Maschine war 7+ Tage offline, bis der Auftrag "Letztes Mal gesehen" ausgeführt wurde.

Praxisbeispiel

- HostA.randomdomain.net hatte einen unglücklichen Unfall mit einem vollen Kaffeekrug, und das Motherboard erholte sich am 10. August nicht vollständig.
- HostA.randomdomain.net befindet sich nun bis zum 20. September im Reparaturlager.
- Am 21. September kehrt HostA.randomdomain.net 4 Stunden nach Ausführung des Auftrags "Last Seen" zum Netzwerk zurück, 2 Stunden, bevor der Auditor einen Export der Computer, die in den letzten 30 Tagen nicht gesehen wurden, in CSV durchführt.
- HostA.randomdomain.net wird immer noch im "Last Seen"-Job als über 30 Tage aufgelistet, die nicht gesehen werden. Obwohl es jetzt voll funktionsfähig und kaffefrei ist, fängt der Auditor es nun in seinem "inaktiven" Export ein

Kurzfristige Lösung

Der Job selbst dauert nicht 24 Stunden, aber er kann mindestens 12 Stunden dauern. Um die Genauigkeit des Filters zu erhöhen, wird die automatische Umplanung für den Job nach Abschluss des vorherigen in der Entwicklung begriffen, die voraussichtlich zwischen 7-12 Stunden Zeitabstand des Batch-Fensters verändern wird.

Langfristige Lösung

Vollständige Überarbeitung des Mechanismus "Letztes Mal gesehen", der näher an Echtzeit ist, wenn die Daten abgerufen werden. Diese Lösung erfordert die Implementierung einer völlig neuen Datenbankstruktur, die derzeit mit der vorgeschlagenen Version im nächsten Kalenderjahr entwickelt wird.