AMP for Endpoints Console e il filtro Ultima visualizzazione

Sommario

Introduzione

Questo documento descrive la spiegazione del bug del filtro "Last Seen" a cui si fa riferimento a CSCvh31177 in Advanced Malware Protection (AMP) for Endpoints.

Contributo di Caly Hess, ingegnere Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso al dashboard di Cisco AMP for Endpoints

Componenti usati

Le informazioni di questo documento si basano sul software:

- Cisco AMP for Endpoints console versione 5.4.20190917

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Il filtro per "Ultima visualizzazione" dalla pagina dei computer sulla console visualizza i connettori visualizzati nelle ultime 24 ore che compaiono nell'elenco.

Causa

L'attuale pull di dati "Last Seen" è un singolo lavoro ogni 24 ore. Sebbene i dati riflessi nella pagina Computer e l'output per l'esportazione in formato CSV per "Ultimo visto" siano in tempo reale, il filtro stesso esegue l'esecuzione dei dati in batch da quel singolo processo. Questo è stato implementato per aumentare la velocità dei risultati, in quanto l'analisi in

tempo reale dei timestamp per gli ambienti aziendali di grandi dimensioni potrebbe portare a timeout e blocco del database.

Spiegazione dei computer "visti di recente" in un filtro di oltre 7 giorni

Il computer è rimasto offline per più di 7 giorni fino all'esecuzione del processo "Last Seen".

Esempio reale

- HostA.randomdomain.net ha avuto uno sfortunato incidente con una tazza di caffè piena e la scheda madre non ha effettuato un recupero completo il 10 agosto
- HostA.randomdomain.net è presente nel deposito di riparazione fino al 20 settembre
- Il 21 settembre, HostA.randomdomain.net ritorna alla rete 4 ore dopo l'esecuzione del processo "Last Seen", ma 2 ore prima che l'auditor effettui un'esportazione in CSV dei computer non visti per gli ultimi 30 giorni
- HostA.randomdomain.net è ancora elencato dal lavoro "Last Seen" come oltre 30 giorni non visti. Nonostante sia ora completamente funzionale e senza caffè, il revisore ora lo coglie nella sua esportazione "inattiva"

Soluzione a breve termine

L'esecuzione del processo in sé non richiede 24 ore, ma può richiedere almeno 12 ore. Per aumentare la precisione del filtro, la riprogrammazione automatica del processo dopo il completamento del processo precedente è in fase di sviluppo, che dovrebbe ridurre da 7 a 12 ore di tempo fuori dalla finestra batch.

Soluzione a lungo termine

Una rielaborazione totale del meccanismo "Last Seen" più vicina al tempo reale quando i dati vengono estratti. Questa soluzione richiede l'implementazione di una struttura di database completamente nuova, attualmente in fase di sviluppo con la release proposta nel prossimo anno solare.