AMP for Endpoints Console and the Last Seen Filter

Contents

Introduction

This document describes the explanation of the "Last Seen" filter bug referenced to CSCvh31177 in Advanced Malware Protection (AMP) for Endpoints.

Contributed by Caly Hess, Cisco Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the Cisco AMP for Endpoints dashboard

Components Used

The information in this document is based on thede software:

- Cisco AMP for Endpoints for Endpoints console 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. If your network is live, ensure that you understand the potential impact of any command.

Problem

The filter for "Last Seen" from the computers page on the console, displays connectors that were seen in the last 24 hours that show up on the list.

Cause

The current pull of "Last Seen" data is a singular job every 24 hours. Though the data that is reflected in the Computers page and the output for Export to CSV for "Last Seen" is real-time, the filter itself runs off the batched data from that singular job. This was implemented to increase the speed of the results, as real-time analysis of the timestamps for large

enterprise environments could lead to time-outs and database lock.

Explanation of "Recently Seen" Computers in a 7+ day filter

The machine was offline for 7+ days until after the "Last Seen" job ran.

Real-World Example

- HostA.randomdomain.net had an unfortunate accident with a full coffee mug and the motherboard didn't make a full recovery on August 10th
- HostA.randomdomain.net is now sitting in the repair depot until September 20th
- On September 21st, HostA.randomdomain.net returns to the network 4 hours after the "Last Seen" job ran but 2 hours before the Auditor does an Export to CSV of the computers not seen for the last 30 days
- HostA.randomdomain.net is still listed from the "Last Seen" job as being over 30 days not seen. Despite it now is fully functional and coffee free, the auditor now catches it in his "Inactive" export

Short Term Solution

The job itself does not take a full 24 hours to run, but it can take at least 12. In order to increase the accuracy of the filter, automatic rescheduling for the job after the previous one completes is under development, which is expected to cut anywhere from 7-12 hours of time off the batch window.

Long Term Solution

A total rework of the "Last Seen" mechanism that is closer to real-time when the data is pulled. This solution requires the implementation of an entirely new database structure that is currently in development with the proposed release in the next calendar year.