Troubleshoot "Failed to create collection: resource already exists" Splunk Error for Umbrella Add-On or Cloud Security App

Contents

Introduction

This document describes how to troubleshoot a "Failed to create collection: resource already exists" error for Umbrella Add-On or Cloud Security App.

Background Information

Some customers can experience an error after configuring the Cisco Umbrella Add-On for Splunk or Cisco Cloud Security App for Splunk. End result no log data is ingested into Splunk. Debug logs in either the Add-On or the App shows this error:

```
HTTPError(response) splunklib.binding.HTTPError: HTTP 500 Internal Server Error -- Failed to create col
```

Cause

This error occurs if you have setup the Add-On or App, previously deleted it, and tried to add it again.

When the app is uninstalled, splunkd normally triggers a reload function syncing the latest configuration with collection data in the database and removes the collection if no corresponding config is found - orphaned collection. However, the reload implementation within KVService fails to do so, leaving this orphaned collection in KVService.

When the app is reinstalled, it does not find the configuration file, as it was removed in the previous step, but when it tries to create it it fails because the KVService still has the collection present within the app context.

Resolution

To resolve the issue upgrade Splunk server to version 9.1.2312.104. If upgrading is not an option open a support ticket with Splunk support. They have a process to cleanup the orphaned collection.

For more information, refer to this splunk support KB: https://splunk.my.site.com/customer/s/article/Failed-

to-create-collection.