Ezmeral Unified Analytics UI and Keycloak are not accessible

Table of contents

Issue

Ezmeral Unified Analytics UI and Keycloak are not accessible.

Attempts to access the UI returns the message "upstream connect error or disconnect/reset before headers. retried and the latest reset reason: remote connection failure, transport failure reason:TLS_error:|268435581:SSL routines:OPENSSL_internal:CERTIFICATE_VERIFY_FAILED:TLS_error_end" as shown in the below screenshot:

Environment

Ezmeral Unified Analytics Version 1.5

Cause

The EZUA UI was not accessible and an 'upstream connect error' was being displayed. To troubleshoot further, HPE support verified the statuses, logs, and descriptions of the relevant pods under the following namespaces: **istio-system**, **keycloak**, and **spire**.

Upon checking the **spire** namespace, we noticed that both the agent and server pods were in a **CrashLoopBackOff** state. After reviewing the pod logs, the following error was identified: '**Transport endpoint is not connected.**' This indicates an issue with the connection to the data storage or underlying infrastructure used by the pods.

Resolution

After investigating the transport endpoint issue, the root cause was identified as being related to the POSIX volume provisioning via the Data Fabric CSI (Container Storage Interface), which is utilized by both the Spire and Keycloak services. When there are issues with the underlying volume, it can result in transport endpoint failures.

Steps Taken to Diagnose and Resolve the Issue:

1. **Diagnosis of Transport Endpoint Issues:** We initially ran the following commands to check for any transport endpoint issues. These commands helped us identify any mounts that were causing problems:

   Checking Mounted Volumes:
   # cat /proc/mounts | grep posix | grep "Transport endpoint is not connected"

   The above command checks the currently mounted volumes and filters for any that have the specific transport endpoint error.

2. **File System Status Check:**

   # df -Th | grep "Transport endpoint is not connected"

   The above command provides information about the file system and highlights any that are not connected properly.

3. **Identifying Affected Containers:** To find the specific containers affected by the transport endpoint issue, we used the following script:

   # for i in `df -Th 2>&1 | grep "Transport endpoint is not connected" | grep "/var/lib/containerd/kubelet/pods/" | awk -F': ' '{print $2}' | cut -d'/' -f1-7`; do tail -n 1 $i/etc-hosts; done

   The above script retrieves the hosts of the affected containers, allowing us to pinpoint which containers are experiencing issues.

4. **Unmounting Affected Volumes:** After identifying the affected mounts, we proceeded to unmount them using the following command:

   # for i in `df -Th 2>&1 | grep "Transport endpoint is not connected" | grep "/var/lib/containerd/kubelet/pods/" | awk -F': ' '{print $2}'`; do umount -l $i; done

   The above command forcefully unmounts the problematic volumes to reset the connections.

5. **Force Deleting the Spire Pods:** Finally, we forcefully deleted the Spire pods to ensure they would restart and attempt to reconnect properly to the volumes. The command used was:

 # for i in `kubectl get po -n spire | awk '{print $1}'`; do kubectl delete po $i -n spire --force; done

The above command retrieves all pods in the Spire namespace and deletes them, allowing Kubernetes to recreate them automatically.

Following the steps outlined above, the transport endpoint issue has been resolved. As a result, the EZUA UI and Keycloak services are now accessible.