33.4 Troubleshooting Analytics Server

33.4.1 Launching Access Manager Dashboard Displays a Blank Page

When you launch Access Manager Dashboard, it displays a blank screen. This can happen when time is not synchronized between Administration Console and Analytics Server. The time must be same on both servers. To understand if the issue is with time synchronization, you can check the log file at `/opt/novell/nam/dashboard/logs/catalina.out`. If the time is not synchronized, you will get the log information similar to the following example:

```
Security exception for user JWT expired at 2020-08-09T11:03:39+0530.
 Current time: 2020-08-09T16:21:44+0530
```

If the time is synchronized but Access Manager Dashboard URL launches a blank page, then you must perform the following on Administration Console Dashboard:

1 Click **Troubleshooting > Certificates**.

2 Click the certificate for Analytics Server.

3 Click **Re-push certificates**.

33.4.2 Graphs Do Not Display Any Data When You Launch Access Manager Dashboard

When you launch the dashboard, it does not display data on the graphs. Also, the health of devices that are displayed on the graphs for Identity Server, Access Gateway, Access Gateway Clusters, and Identity Server Clusters is unavailable. This happens because the realtime index, where the events are received and stored, does not exist on the Analytics Server.

To resolve this issue and view the realtime data graphs, perform the following steps:

1 Connect to Analytics Server by using SSH.

2 Run the following command to verify if the realtime events are getting stored in the realtime index:

GUI command: Click **Access Manager Dashboard**> **Dev tools** `GET realtime/_search`

3 (Conditional) If you get the error `"IndexMissingException[[realtime] missing]","status":404`, run the following command to list all indexes that are present within Analytics Server:

GUI command: Click **Access Manager Dashboard** > **Dev tools** `GET _cat/aliases?v`

33.4.3 Clearing the Existing Realtime Data to View the Imminent Data on the Graphs

If you want to clear the existing realtime data to view only the latest data on the dashboard, you must perform the following steps:

1 Use the SSH client to connect to Analytics Server.

2 Delete the realtime index data by using the following command:

GUI command: Click **Access Manager Dashboard** > **Dev tools** `POST realtime/_delete_by_query`

```
{
   "query": {
      "match_all": {}
   }
}
```

It takes few minutes for the data to be reflected on the graphs.

33.4.4 Cannot Launch Access Manager Dashboard After Reimporting Analytics server

After importing or re-importing an Analytics Server, you cannot access Access Manager Dashboard. This happens when there is an issue with certificates. To resolve this issue, re-push the certificates. For information about re-pushing the certificates, refer the steps mentioned in .

33.4.5 The Analytics Server Health Is Not Reported to Administration Console

When you check the health of Analytics Server from Administration Console (**Devices > Analytics Servers**), the health for a specific Analytics Server displays the not responding icon. When you click on the icon, the `Server is not reporting` status message is displayed. To resolve this issue, you must restart the dashboard service and JCC service by running the following commands on the specific Analytics Server:

`rcnovell-dashboard restart`

`rcnovell-jcc restart`

33.4.6 Access Manager Dashboard Does Not Display the Graphs, but Displays the Health Status of the Devices

When you launch Access Manager Dashboard, the graphs are unavailable, but the **Identity Server**, **Access Gateway**, **Access Gateway Clusters**, and **Identity Server Clusters** graphs display the health status of all devices.

All the services run properly, but the graphs are not generated. This issue occurs when Analytics Server does not receive the required events.

Use the following three different ways to validate the issue:

Using ElasticSearch query

1 Log into **Access Manager dashboard**.

2 Navigate to **Devtools**.

3 Type the following commands for each query:

   3a To verify if index contains any data: `GET realtime/_count`

   3b To check the count of login events:

```
GET realtime/_count

                                          {
                                            "query": {"match": {
                                                    "eventID":
"002E000A"
                                          }}
                                          }
```

   3c Verify the event fields:

```
GET realtime/_search

                                          {
                                            "query": {"match": {
                                                    "eventID":
"002E000A"
                                          }}
                                          }
```

Logstash Print Statements

4 Launch Access Manager Dashboard using SSH client.

5 Navigate to `/etc/logstash/conf.d/events`

6 Using vi editor, open `02-01-output.conf file`.

7 Uncomment `"stdout { codec => rubydebug }"` in each if/else conditional block.

8 Save the file.

9 Restart logstash using `rcnovell-logstash restart`.

10 Monitor the incoming events in the log file named `tailf /var/log/logstash-stdout.log`. After the events reach dashboard, logstash parses the sends them to the console named `logstash-stdout.log file`. The events are also sent to ElasticSearch.

11 In the console the parsed events are in the following format:

```
{
        "loginCount" => 1,
            "authsid" =>
"2aa85a63c5df1cac21da72c8fbd08d83b4df3e09220c45850bbc3f3bf719397b",
       "browserName" => "Firefox",
       "countryCode" => "GB",
      "contractName" => "PostAuthentication Login",
        "deviceName" => "Windows",
       "failedCount" => 0,
            "eventID" => "002E000A",
          "deviceID" => "idpBD772894488FE113",
      "update_event" => "true",
          "sessionID" =>
"043111f04425f7a086e8abb7507299531df6b34c470494b7ccd491e4cac94da3",
        "createDate" => "2020-06-21T11:34:15.747Z",
          "sourceIP" => "194.32.31.1",
          "userName" => "user0",
         "eventType" => "null"
                    }
```

12 Verify the Connectivity

Check the connectivity using the command:

```
netstat -na | grep 1468
  tcp       0       0 10.0.0.1:38930       10.0.0.101:1468
ESTABLISHED
```