ClearPass Operational Report Summary

Derin Mellor

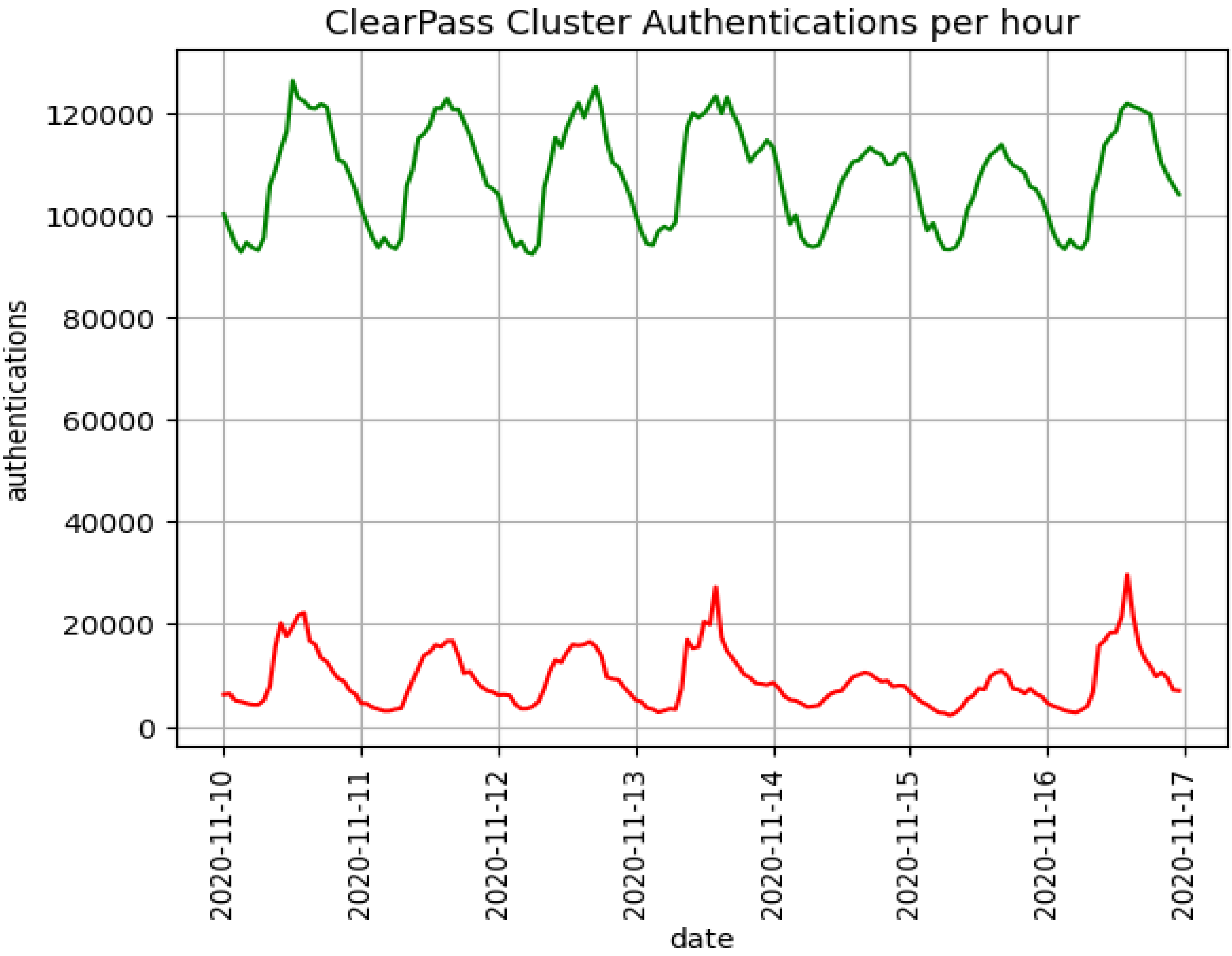
18/12/20

0.03 DRAFT

Time Frame 2020-11-10 to 2020-11-17

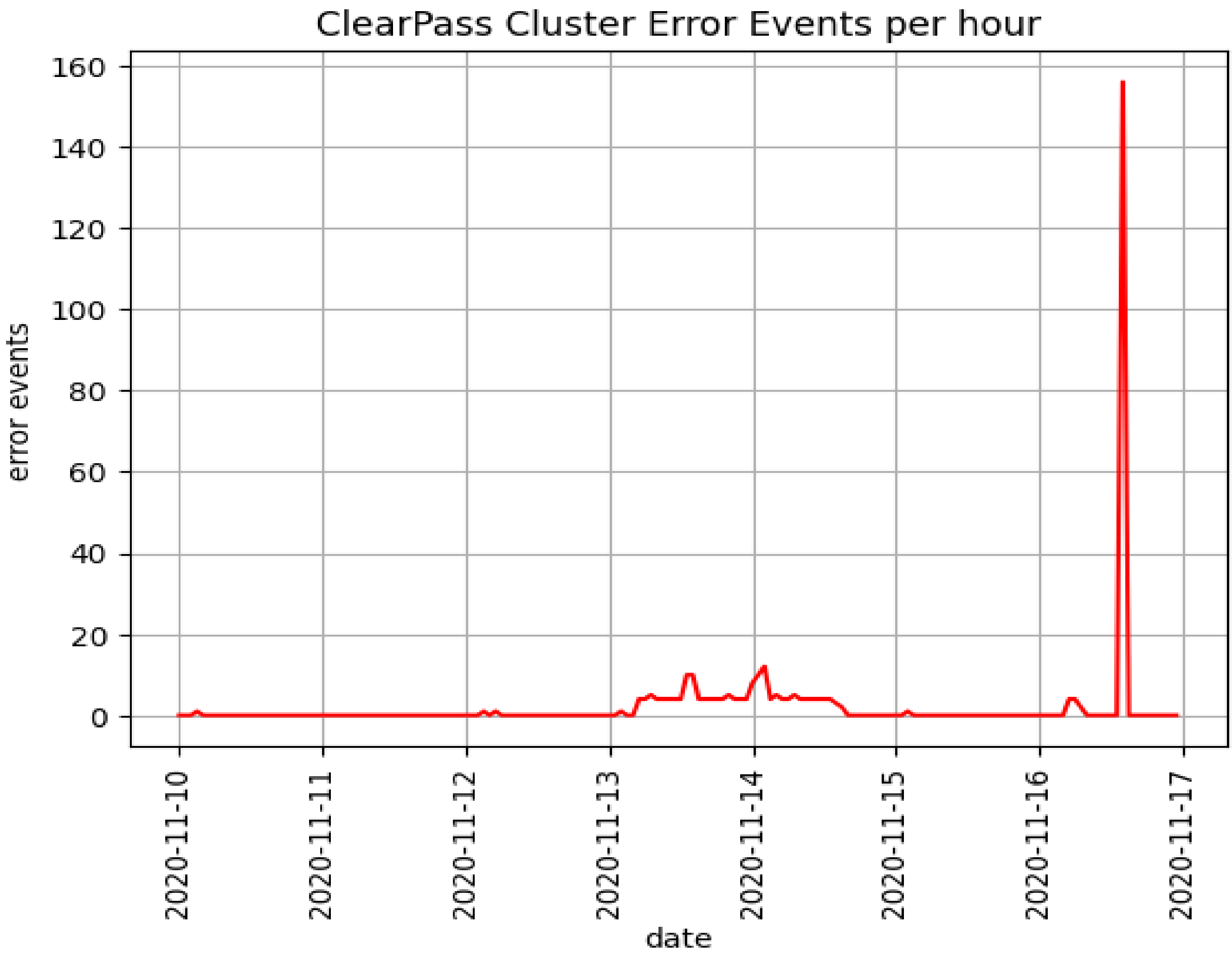
Executive Summary

ClearPass Cluster Authentications per hour



These highlights how the environment is operating. Concern arises where the background failure rate is excessive, in theory there should be none, this is not always possible. It is often dependent on the ClearPass service design - e.g. guest. Spikes are a concern and possibly a serious concern as it might indicate a serious short-term issue - e.g. an authentication source going offline. These should be investigated.

ClearPass Cluster Error Events per hour



This graph summaries the ClearPass cluster's error events. Clearly any error events are not good, but may not be directly related to authentications. If these do correlate with increased authentication failures they should be investigate.

Maximum License Usage

Entry (0)	Access (76175)	Onboard (175)	OnGuard (175)
0	26296	1	0

These highlights the highest licenses used over the time frame of the report. If these are above the limit they will be highlighted in red - more licenses should be purchased. If these are within 10% of the limit they will be highlighted in amber - it may be worth considering more licenses? If less than 50% of licenses are being used they will be highlight in green - it might be worth reducing the supported number of licenses?

Endpoint Status

Total	Disabled	Known	Unknown
27076	0	10650	16426

This shows the number of endpoints that have connected in the time frame of the report. Disabled endpoints are a concern: They should be removed. Known endpoints: It is desirable to have all the endpoints in this state - but may be impossible, this is effectively an audit of the devices (as opposed to infrastructure) connecting to the network. Unknown endpoints: It is highly desirable to keep these to a minimum. However, with 'open' SSIDs (e.g. guests) and randomized MAC addresses may make this impossible.

Typically you wouldn't expect to see more that 1 successful authentication by a device every hour. Fails are another matter.

In this case the maximum authentications per hour (151610) is massively above the total observed devices.

Missing Known Endpoints

Missing	52199

This indicates the number of Known endpoints that have not connected in the time frame of the report. WARNING: This maybe misleading as the Insight database does not indicate whether a Known endpoint has been deleted.

Recommendations

Priority Ordered Review List

- max_license
- events
- wired_endpoint_auths
- wireless_endpoint_auths
- nas_auths
- dot1x_auths
- endpoints_missing
- endpoint_spoof
- session_duration
- device_session_data
- device_session_data_tx
- alerts

This is a priority ordered list of areas that should be reviewed. Associated details are in the ClearPass Operational Report Detailed