Identity Service Engine Log Analytics

How to Maintain and Monitor ISE using Log Analytics

Ethan Glaser
Technical Consulting Engineer

Session ID: TACSEC-2018

Agenda

01 Introduction

02 What is Log Analytics

03 How To Enable Log Analytics

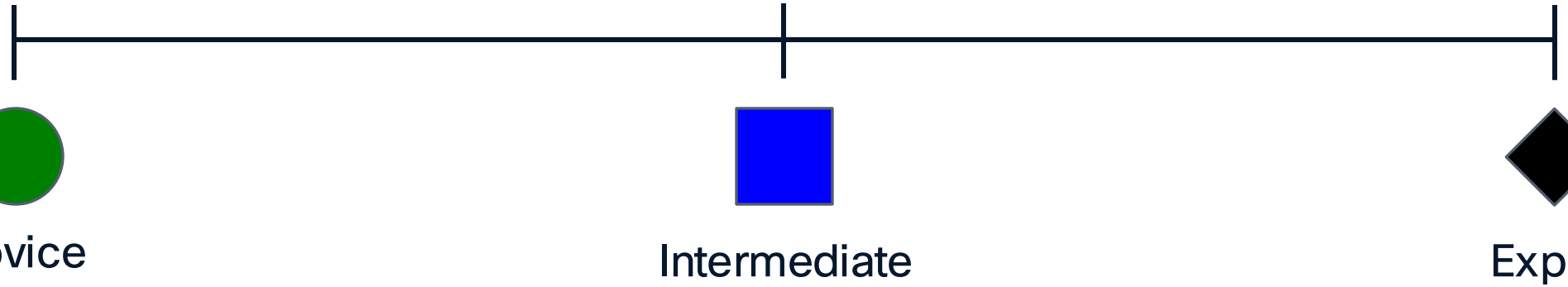
04 Dashboards & Visualizations

05 Custom Visualizations

06 Troubleshooting Examples

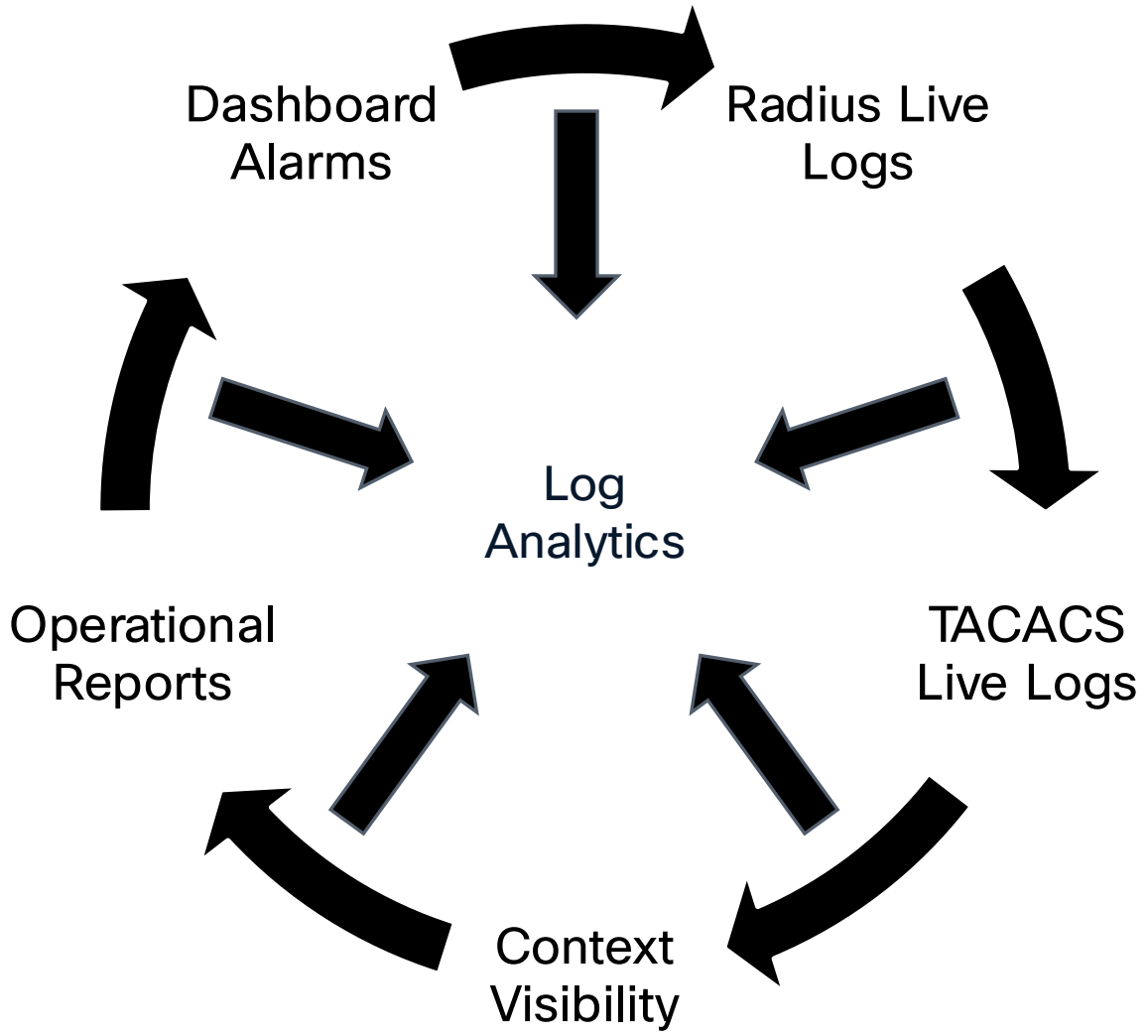
07 Conclusion

About Myself



What is Log Analytics

What Is Log Analytics



Log Analytics Design

ElasticSearch

Designed to store, search, and analyze large volumes of data quickly in near real-time

LogStash

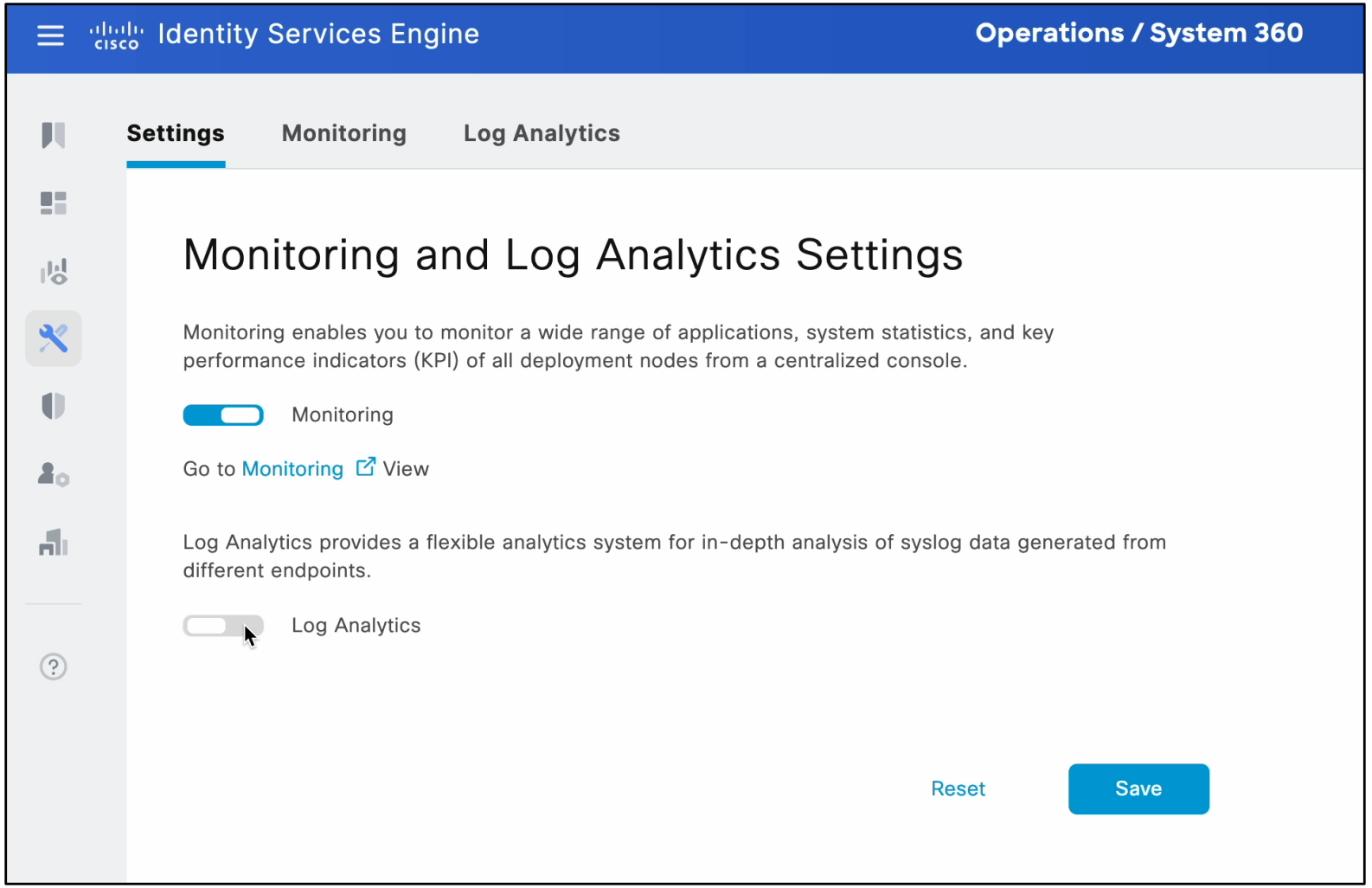
Data processing pipeline that ingests, processes, and transforms data from multiple sources

Kibana

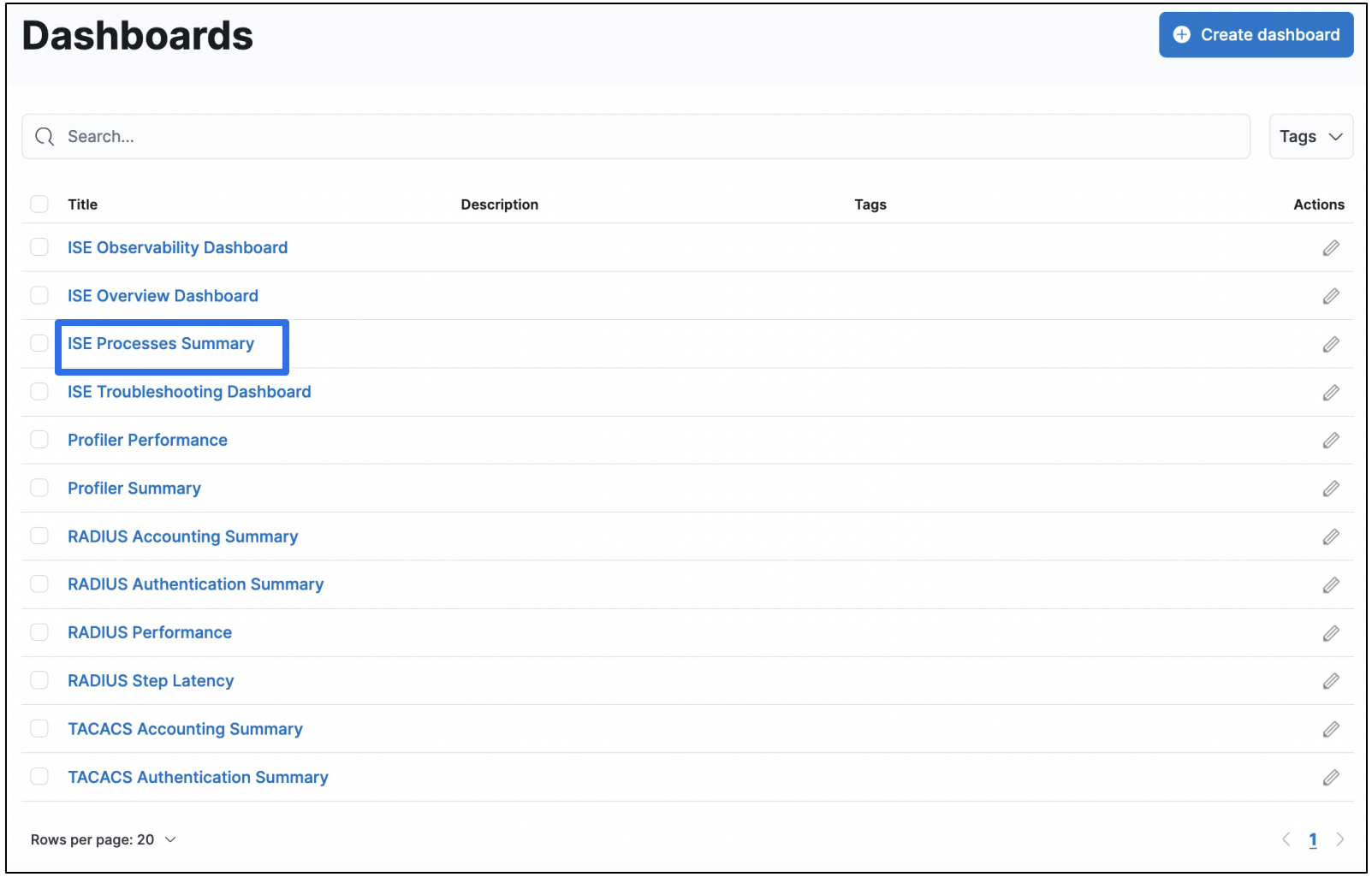
Data Visualization platform that allows users to create interactive dashboards, charts, and graphs

How to Use Log Analytics

How to Enable Log Analytics



Default Dashboards



ISE Processes Summary

The ISE Processes Dashboard contains visualizations of ISE services state of operation over time

We can see the exact time when services go down, how long they are down for, and when they start back up again.

The chart is broken into three state:

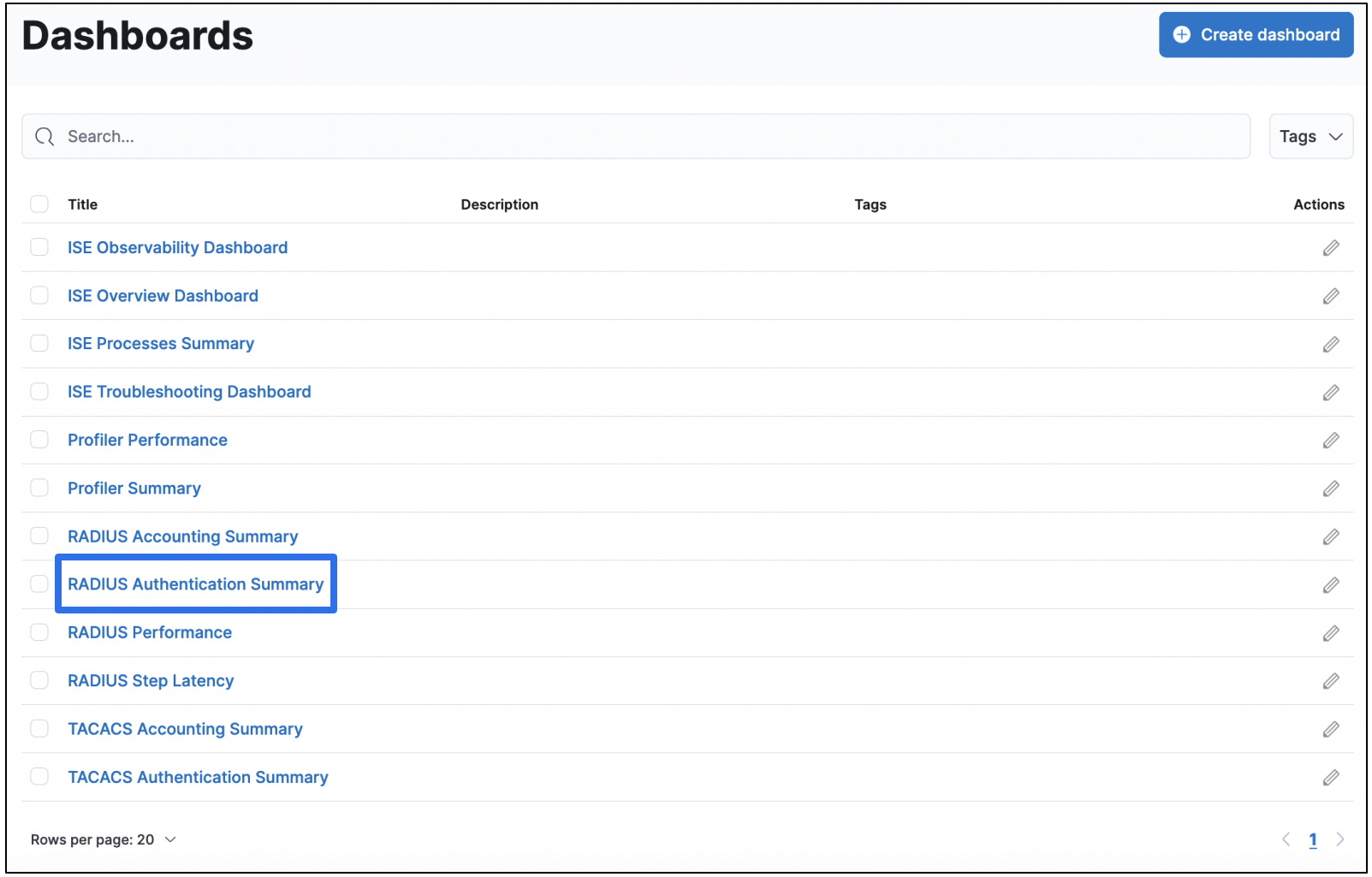
1- up

0- down, and

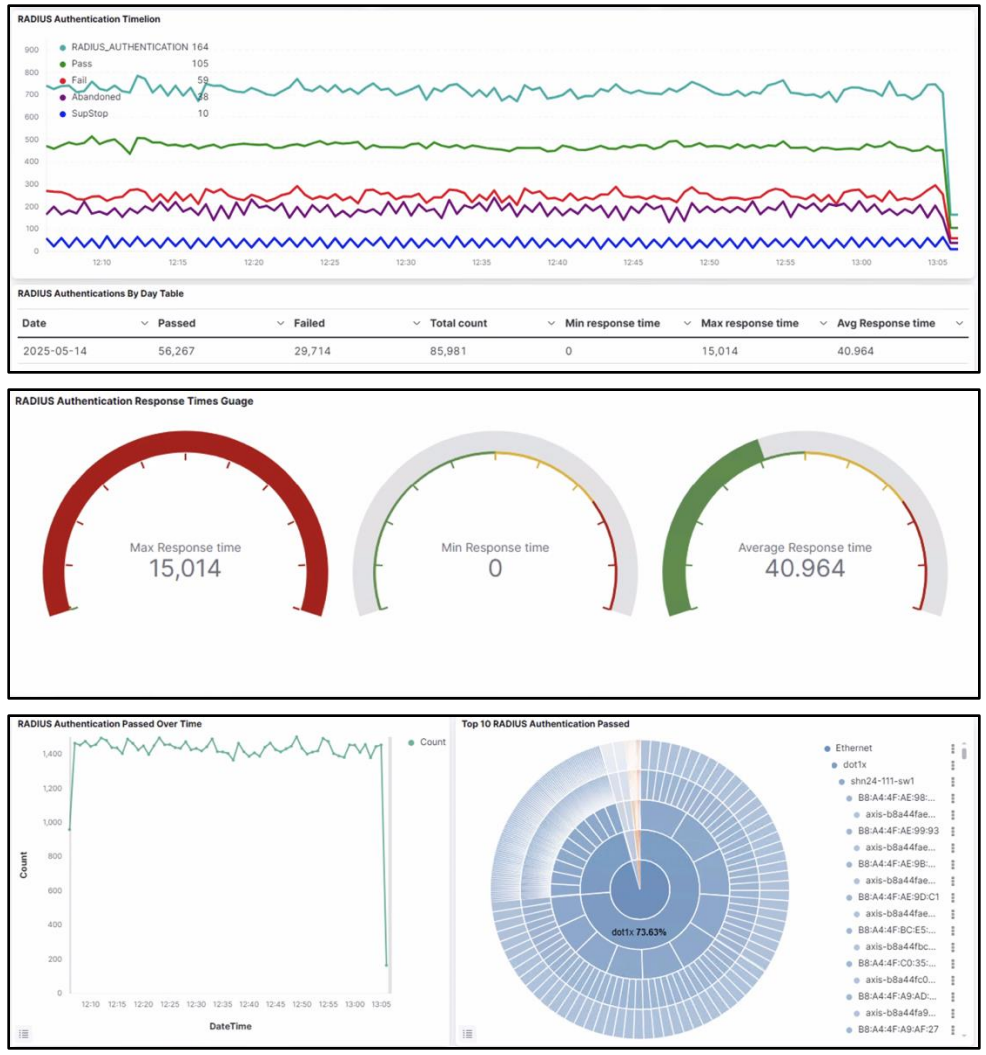
-1- started

ISE Processes Summary

Default Dashboards



Radius Authentication Summary

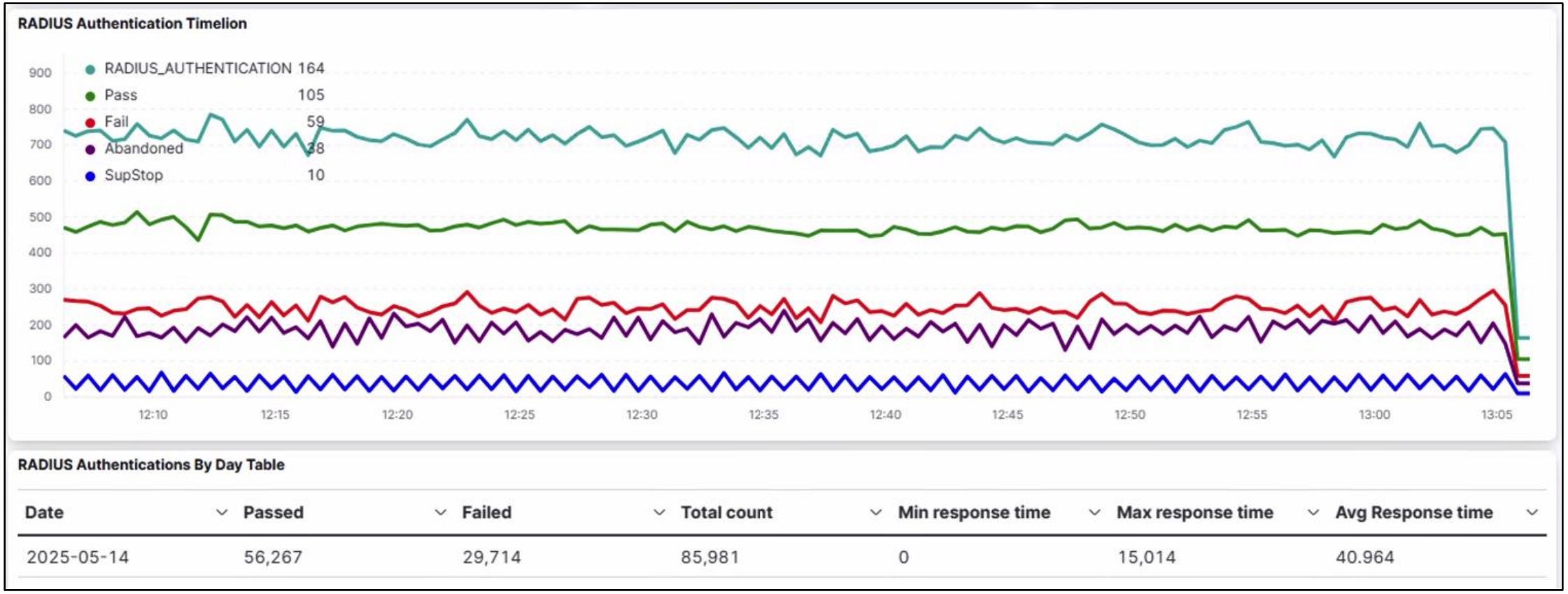


The Radius Authentication Summery Dashboard provides insights into:

- Total amount of authentication
- Authentications over a time interval
- Authentications Response time
- Transactions per Second

We can break information down further, deciphering the information based on policy sets, authorization policies, NAS Port type, Identity store, and even filter it down per user and/or device.

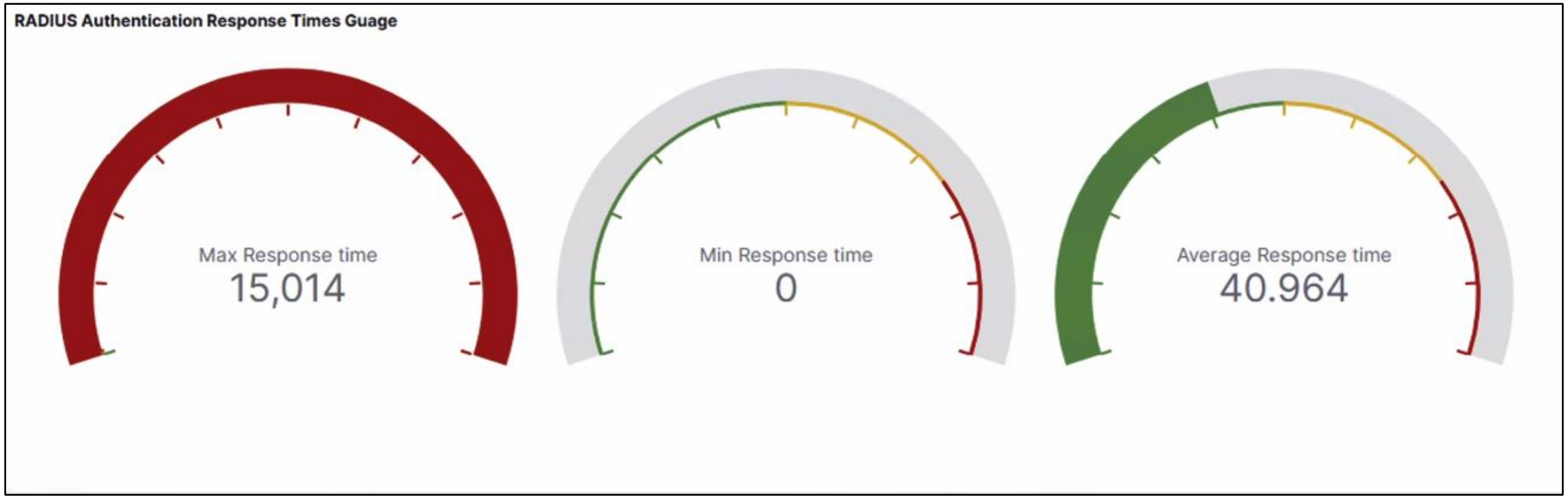
Radius Authentication Summary



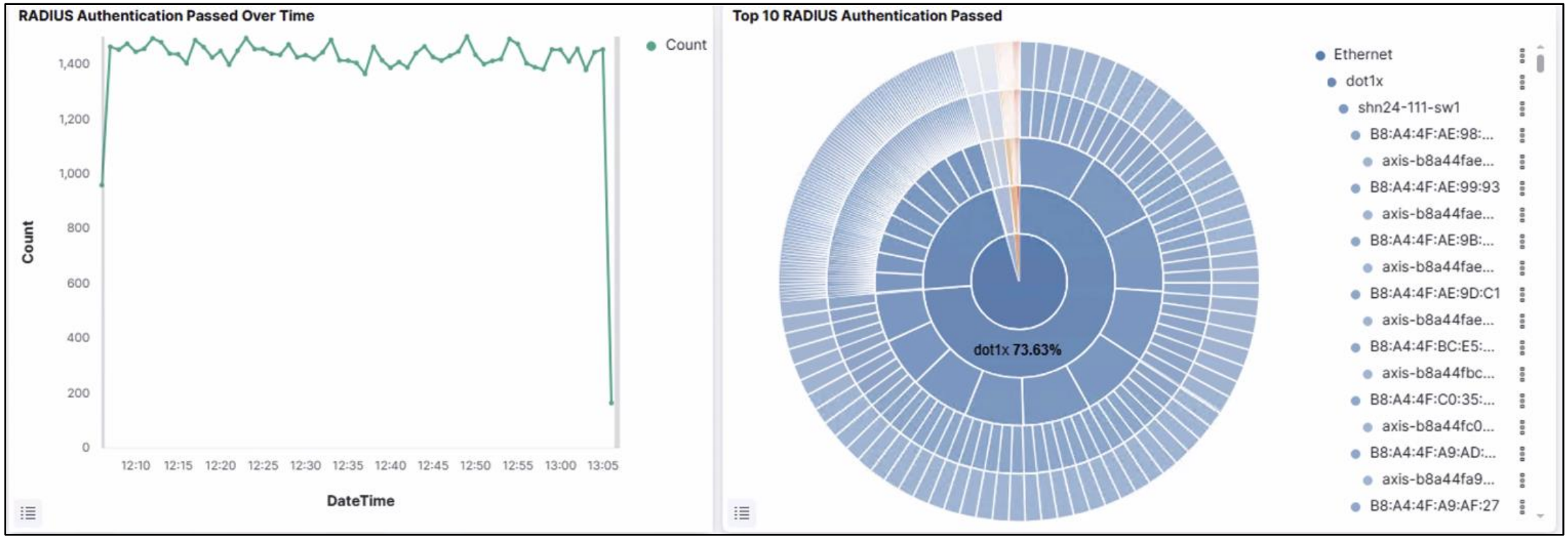
RADIUS Authentications By Day Table

Date	Passed	Failed	Total count	Min response time	Max response time	Avg Response time
2025-05-14	56,267	29,714	85,981	0	15,014	40.964

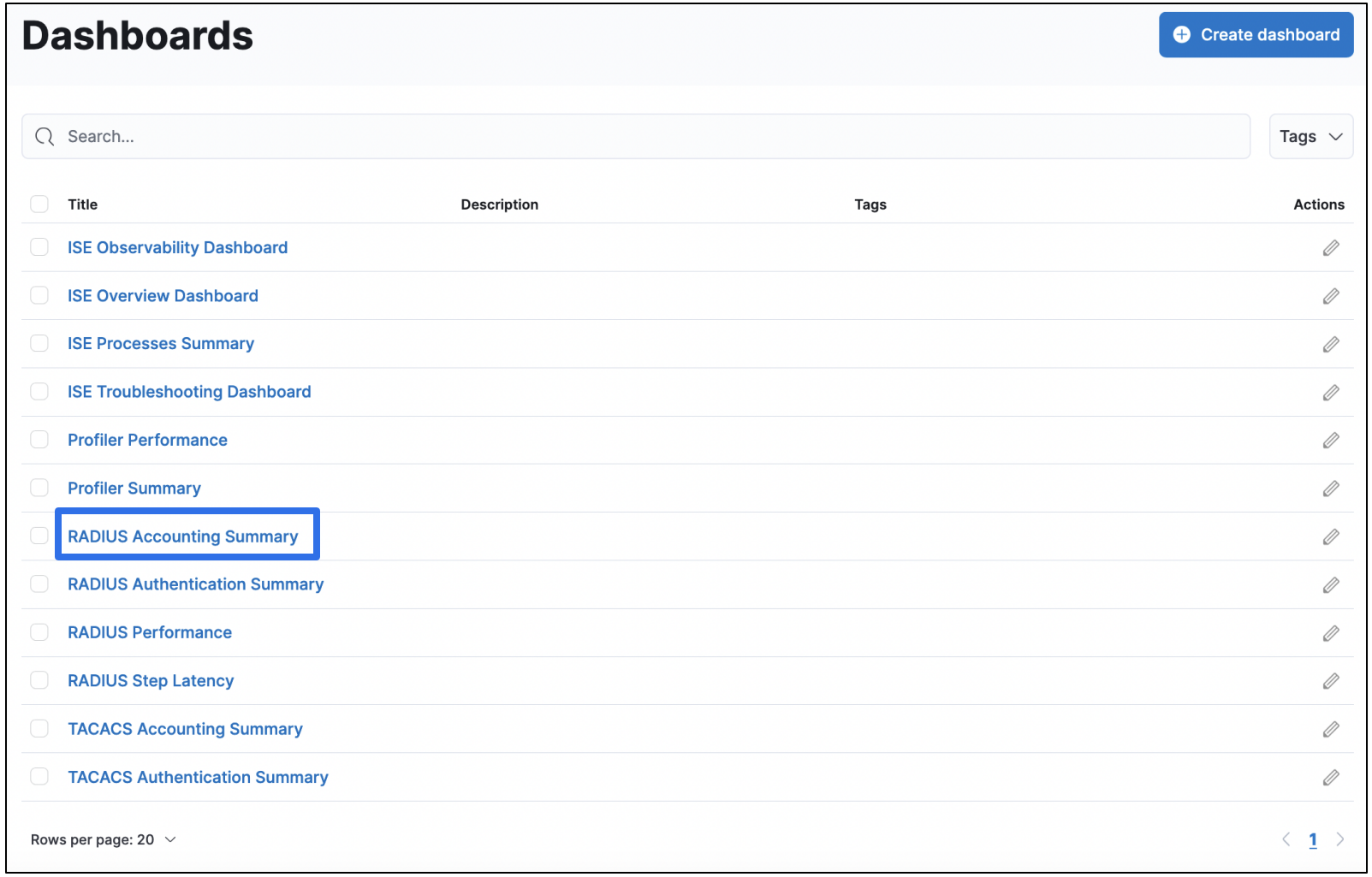
Radius Authentication Summary



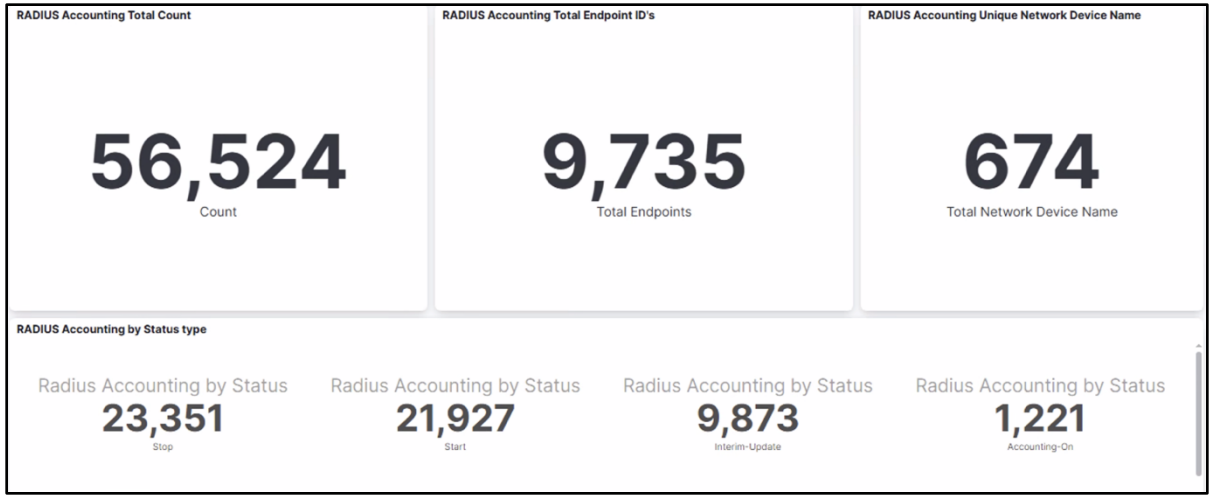
Radius Authentication Summary

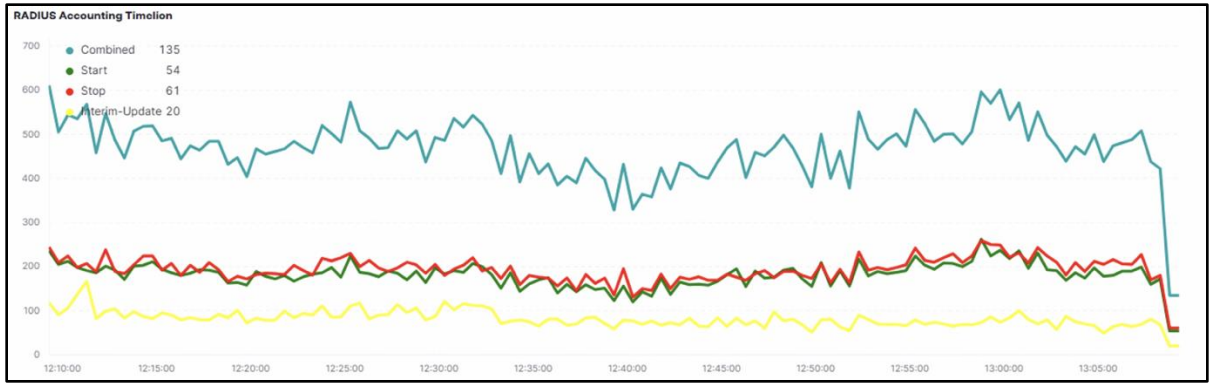


Default Dashboards



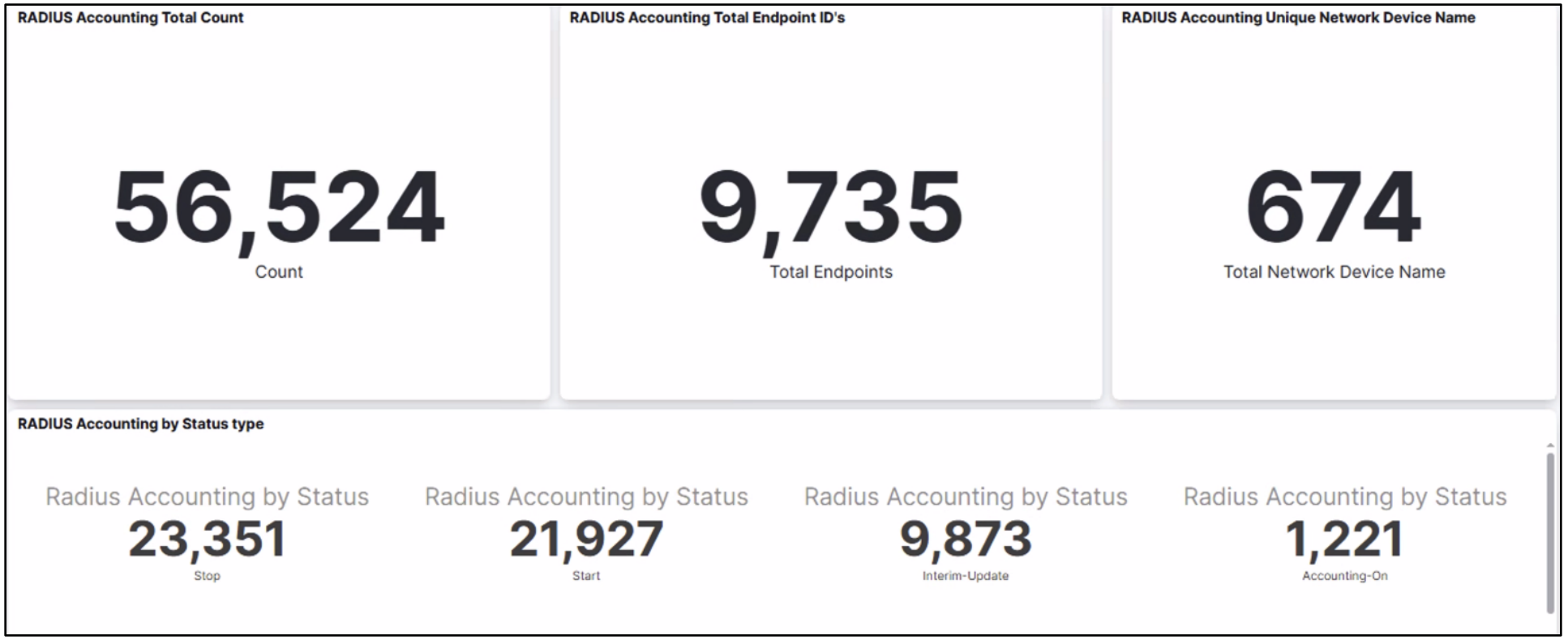
Radius Accounting Summary



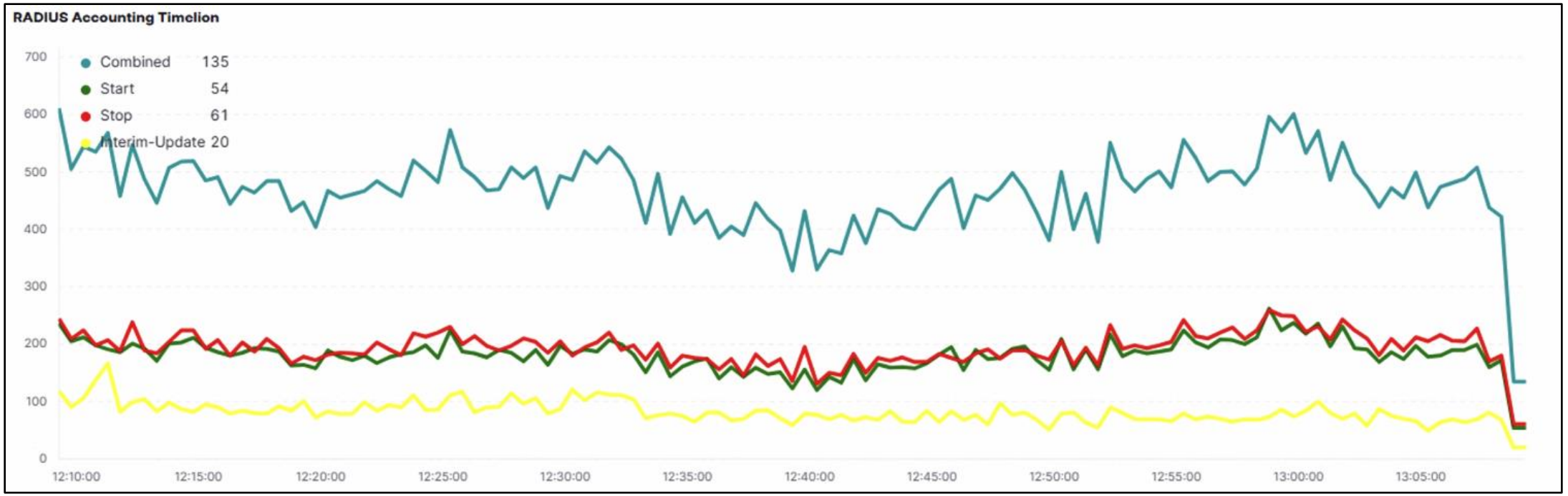


The Radius Accounting Summery dashboard can be further paired with the Authentication dashboard to find information on our accounting statistics overtime based on different status types.

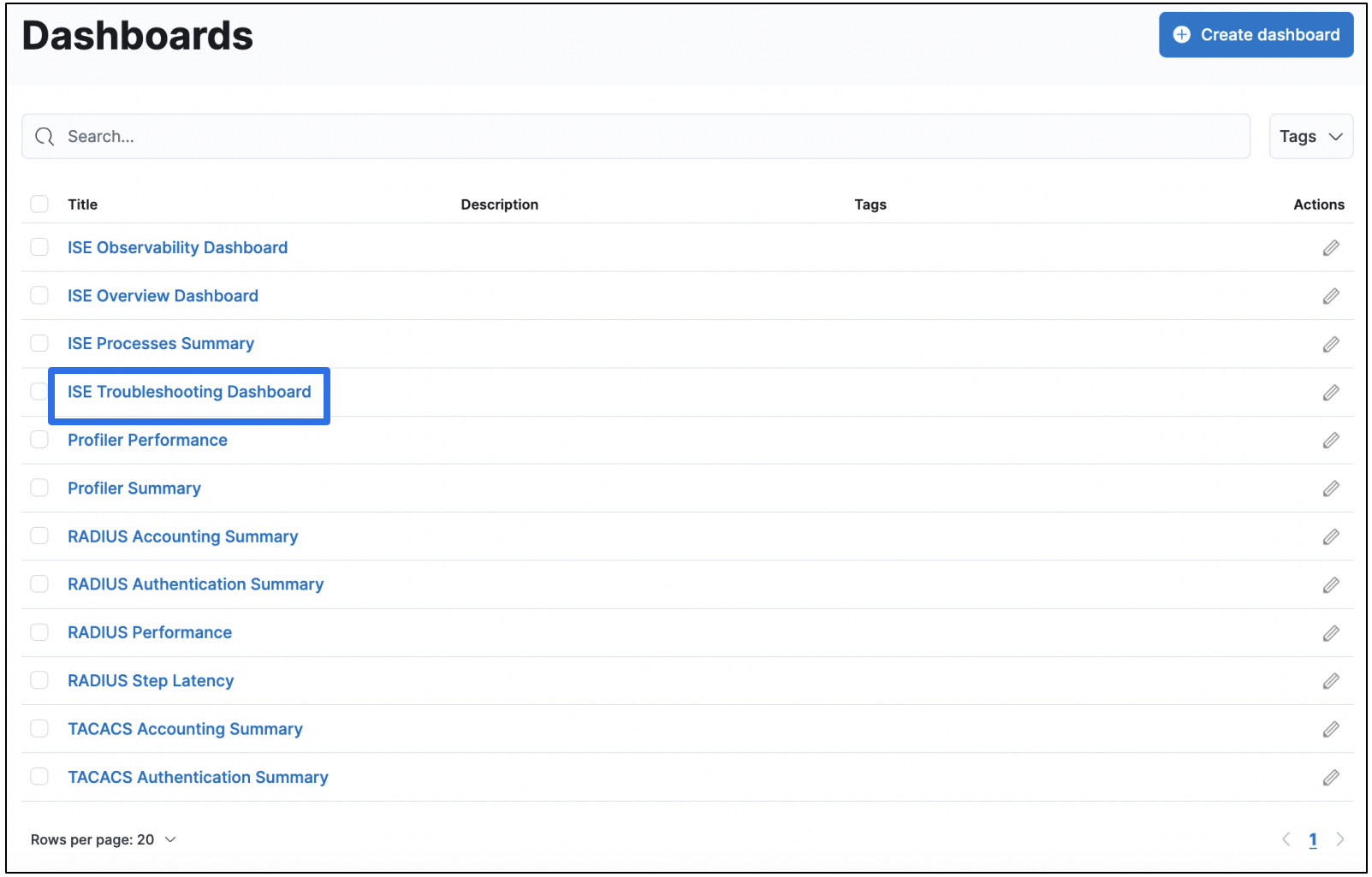
Radius Accounting Summary



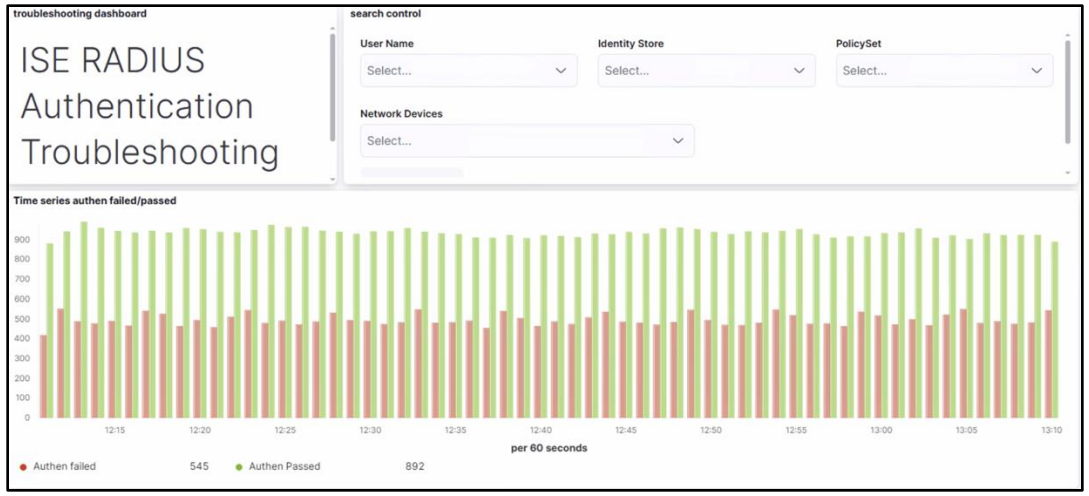
Radius Accounting Summary

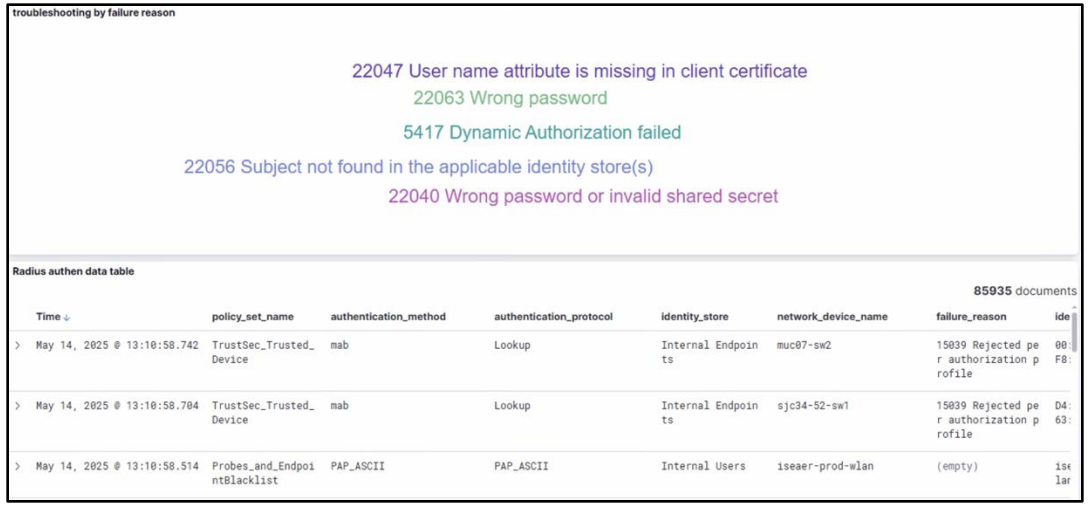


Default Dashboards



ISE Troubleshooting Dashboard

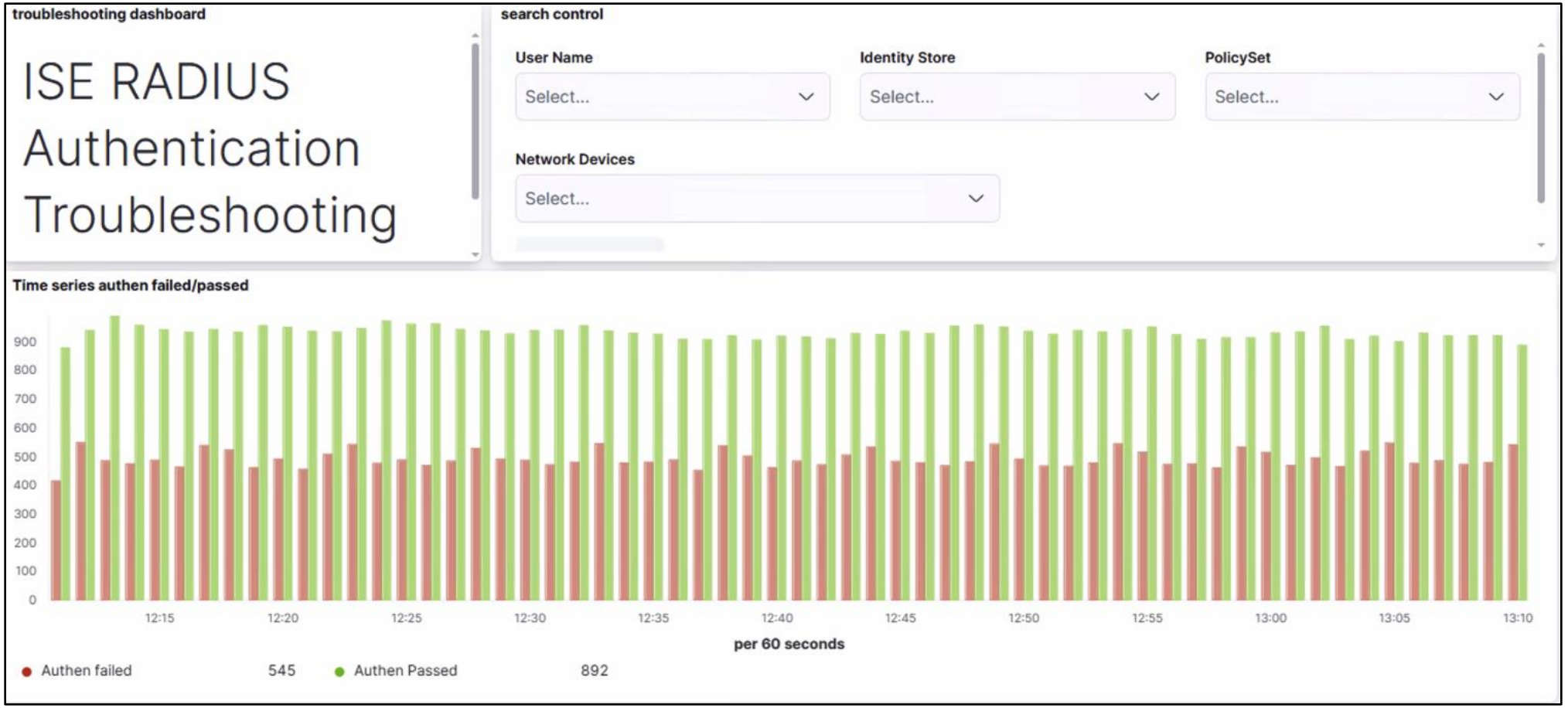




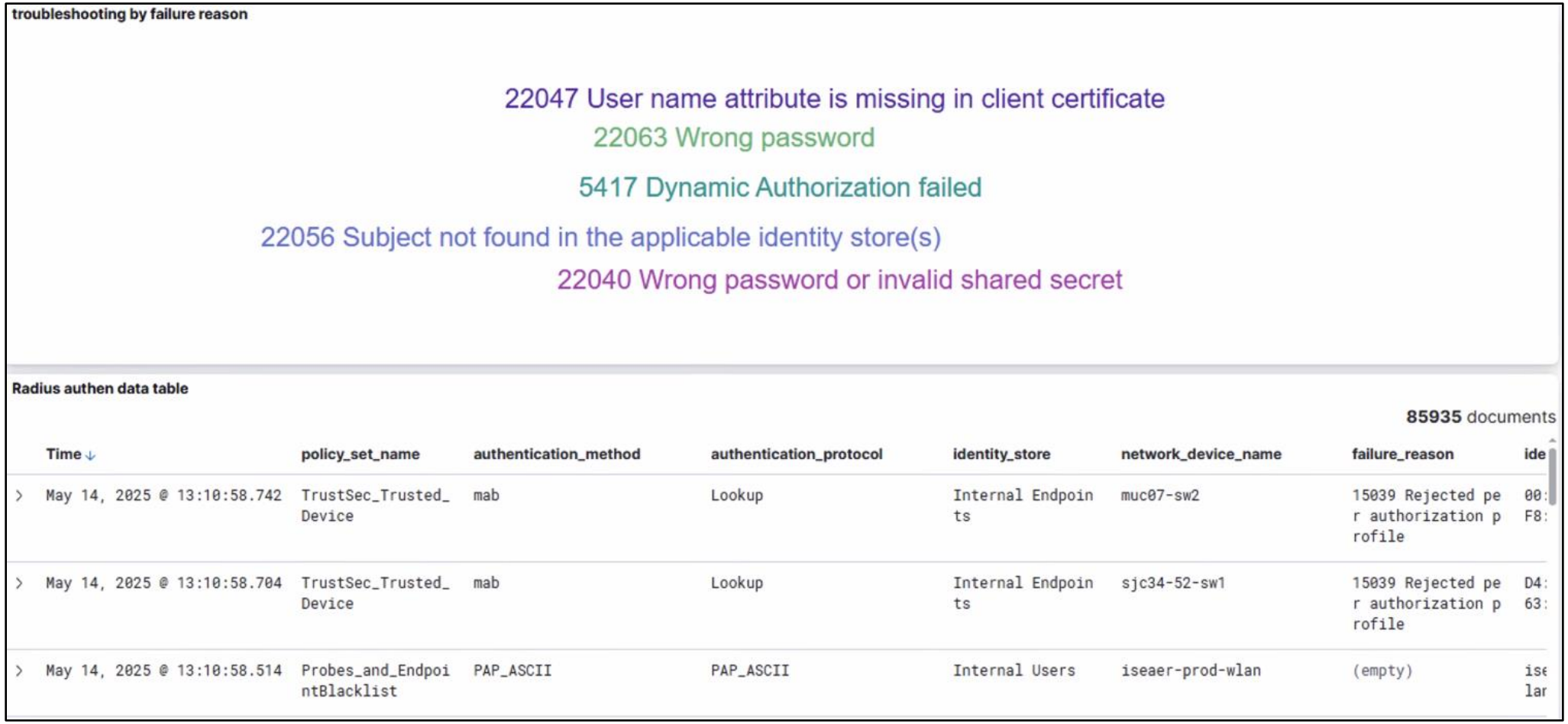
The ISE Troubleshooting Dashboard provides data on passed vs failed authentications and breaks these authentications down both overtime in a chart.

It will also provide a heat map of the authentication failure reasons to tell what is the most popular authentication failure.

ISE Troubleshooting Dashboard



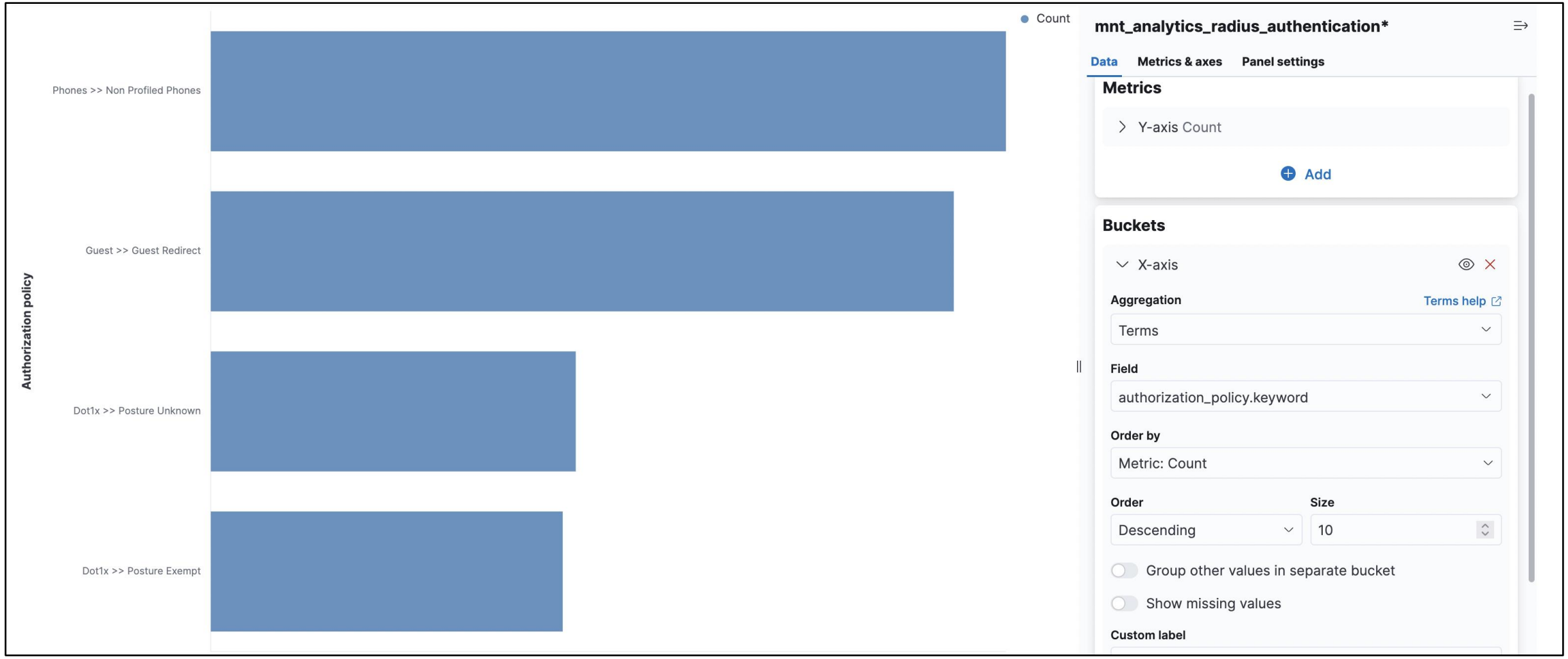
ISE Troubleshooting Dashboard



Time	policy_set_name	authentication_method	authentication_protocol	identity_store	network_device_name	failure_reason	ide
May 14, 2025 @ 13:10:58.742	TrustSec_Trusted_Device	mab	Lookup	Internal Endpoints	muc07-sw2	15039 Rejected per authorization profile	00:F8:
May 14, 2025 @ 13:10:58.704	TrustSec_Trusted_Device	mab	Lookup	Internal Endpoints	sjc34-52-sw1	15039 Rejected per authorization profile	D4:63:
May 14, 2025 @ 13:10:58.514	Probes_and_EndpointBlacklist	PAP_ASCII	PAP_ASCII	Internal Users	iseaer-prod-wlan	(empty)	ise lar

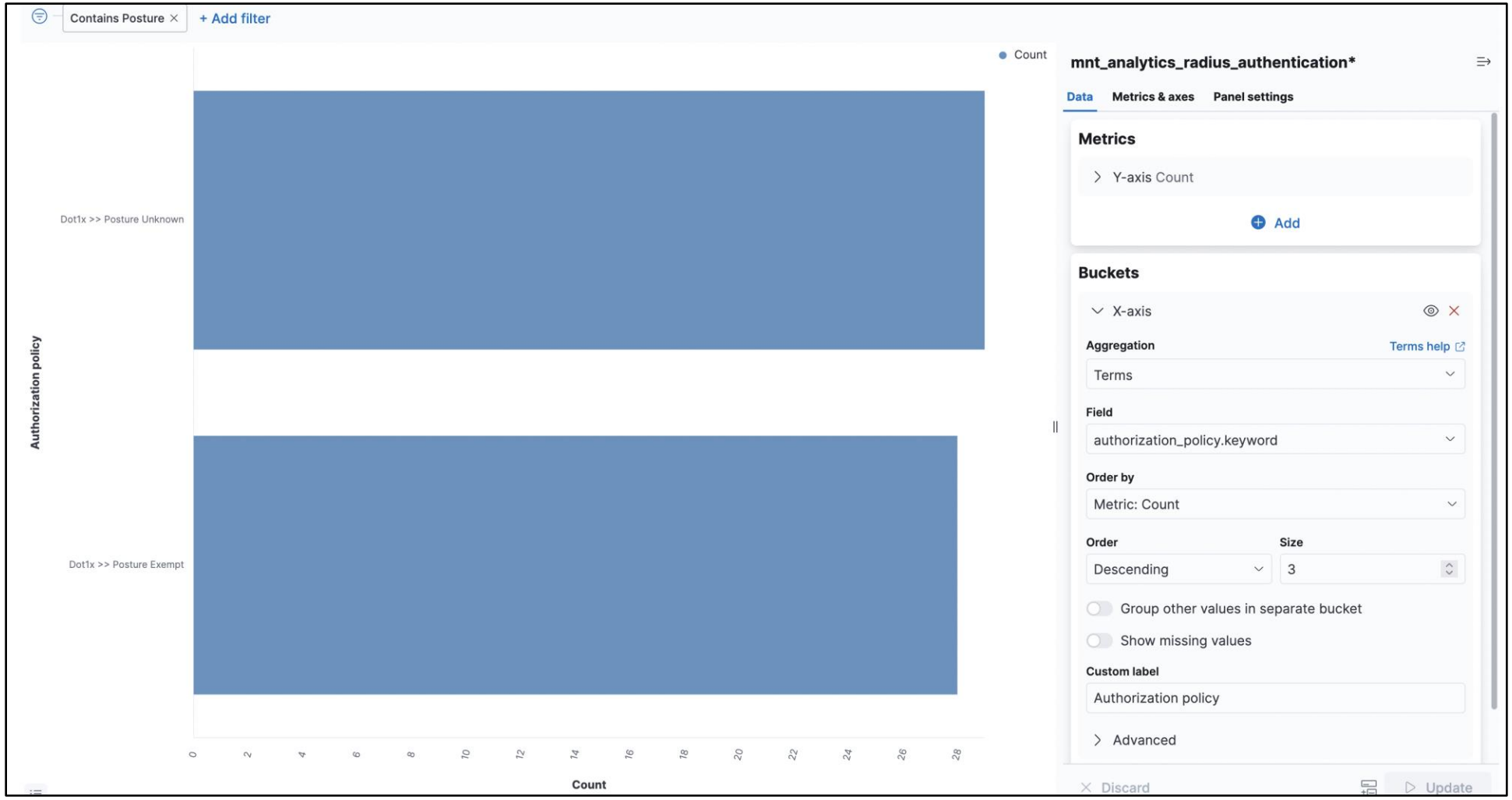
Custom Visualizations

Create Custom Visualizations

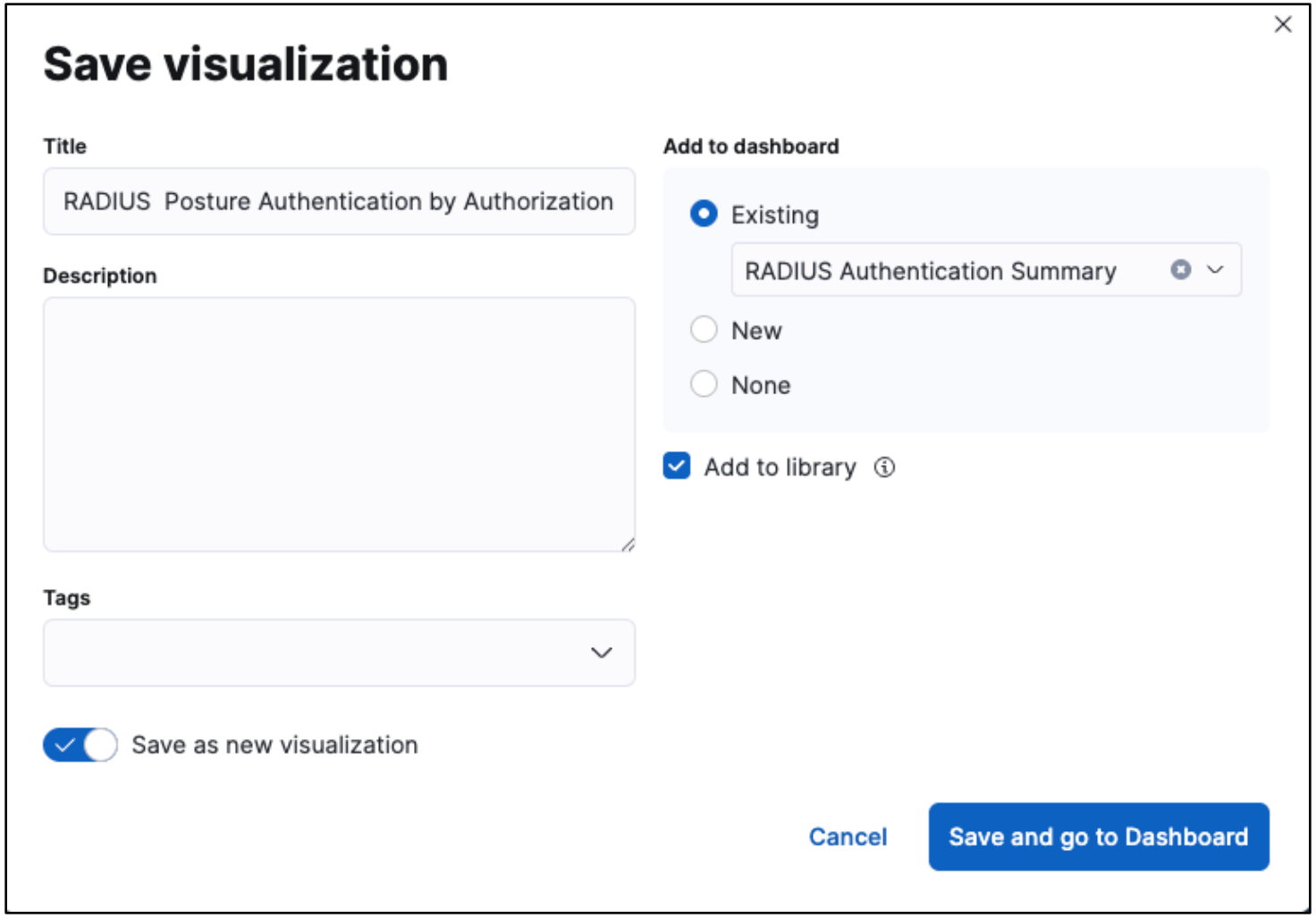


DSL Queries

Create Custom Visualizations

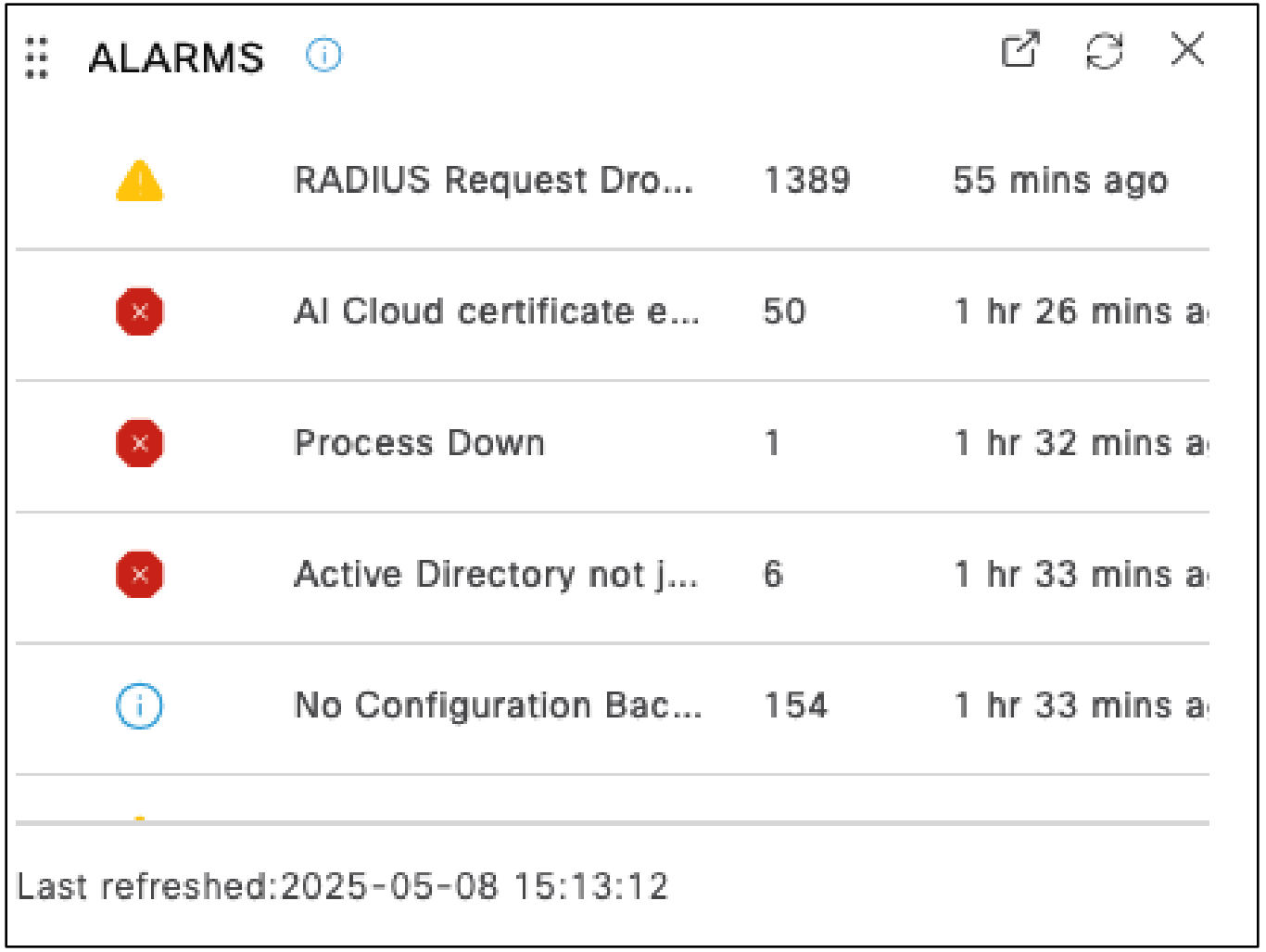


Create Custom Visualizations

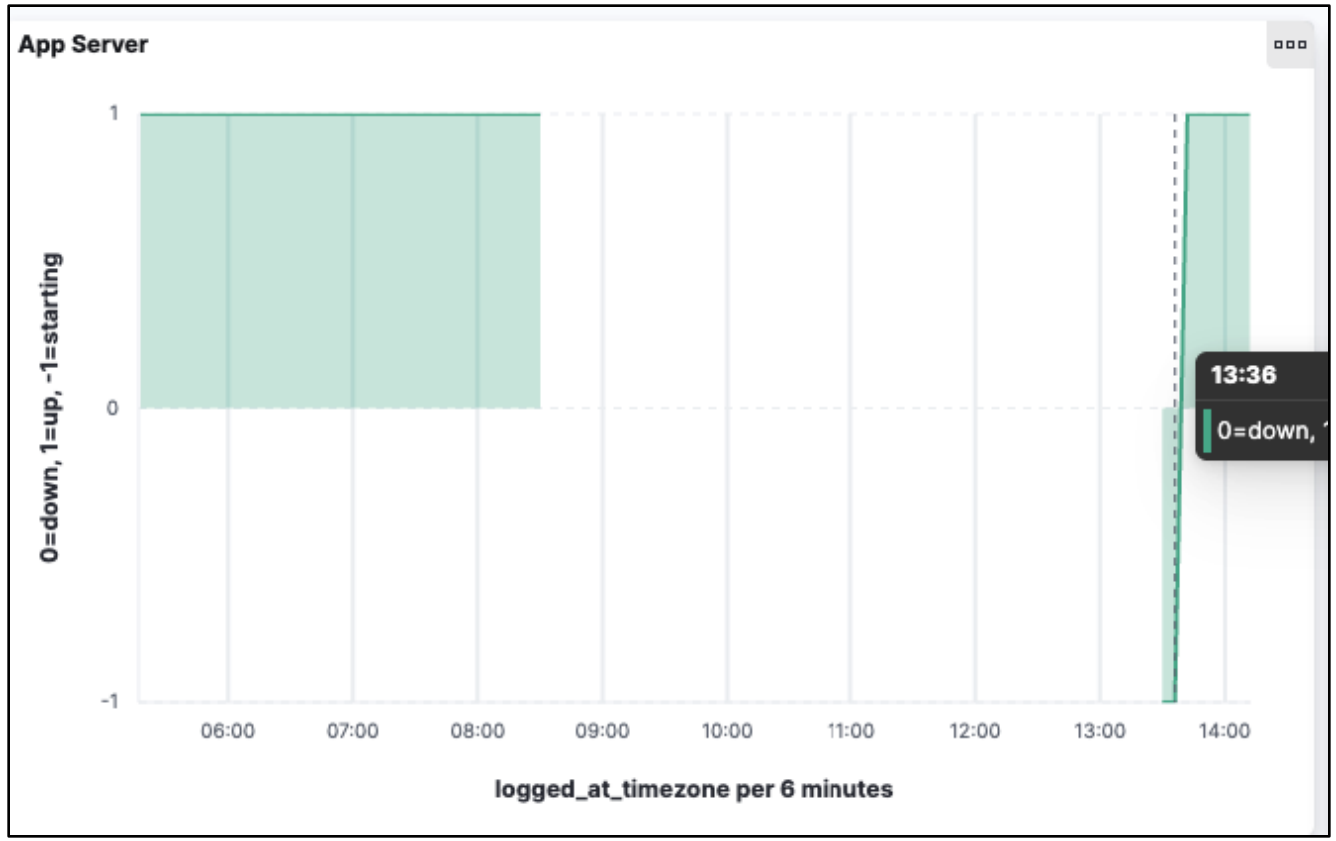


Troubleshooting Examples

Application Server Went Down



Application Server Went Down

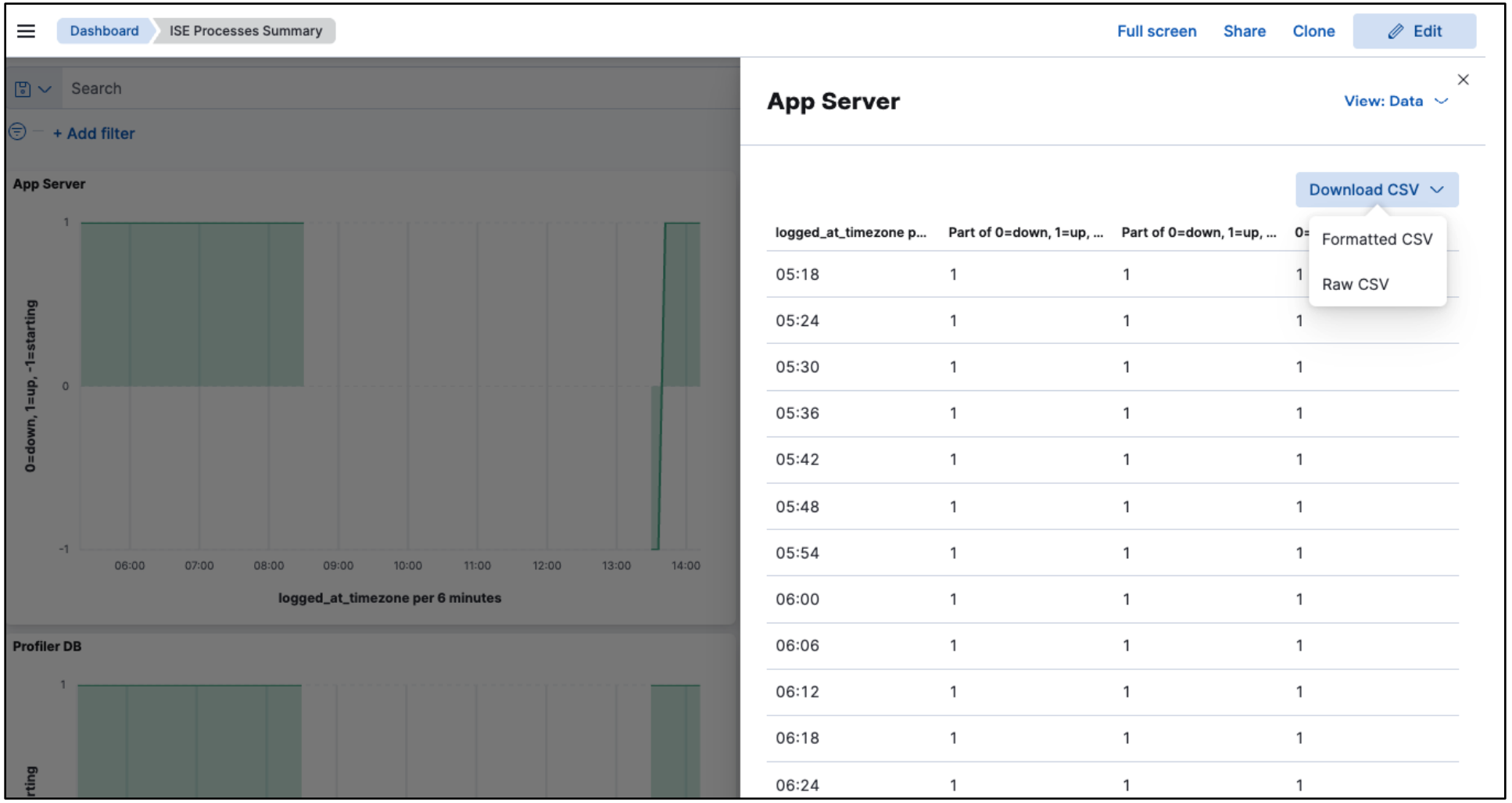


Using Log Analytics, we can see the white gap, when the chart lie is a 0 is when the server is down.

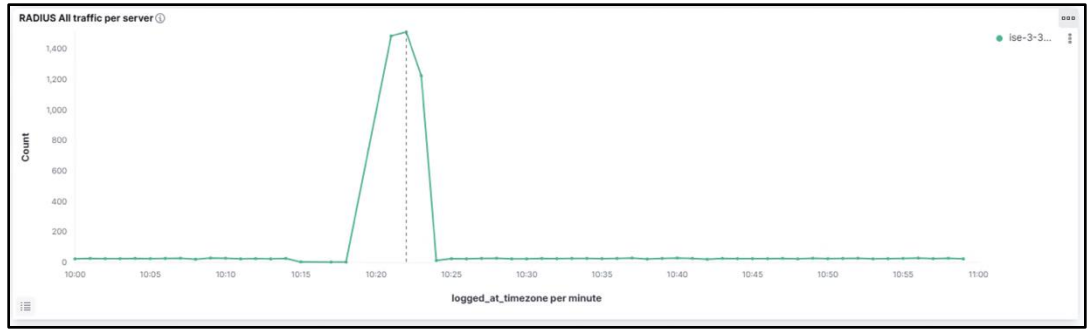
We can highlight over the cart to get the exact time intervals for every point.

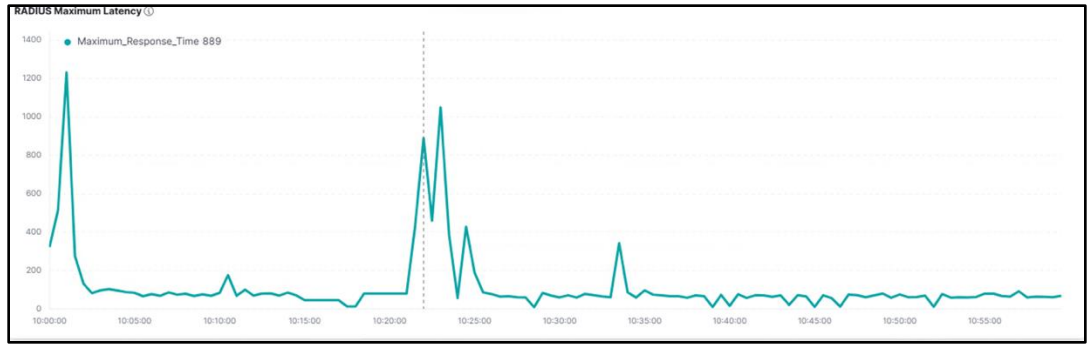
When the graph dips below 0 to -1 is when the service goes back into initializing, and then we can see it go from initializing back to running.

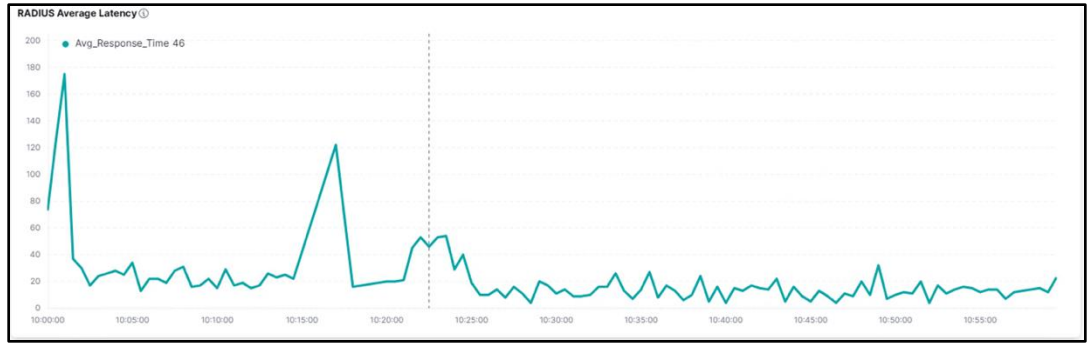
Application Server Went Down



High Authentication Latency on PSN





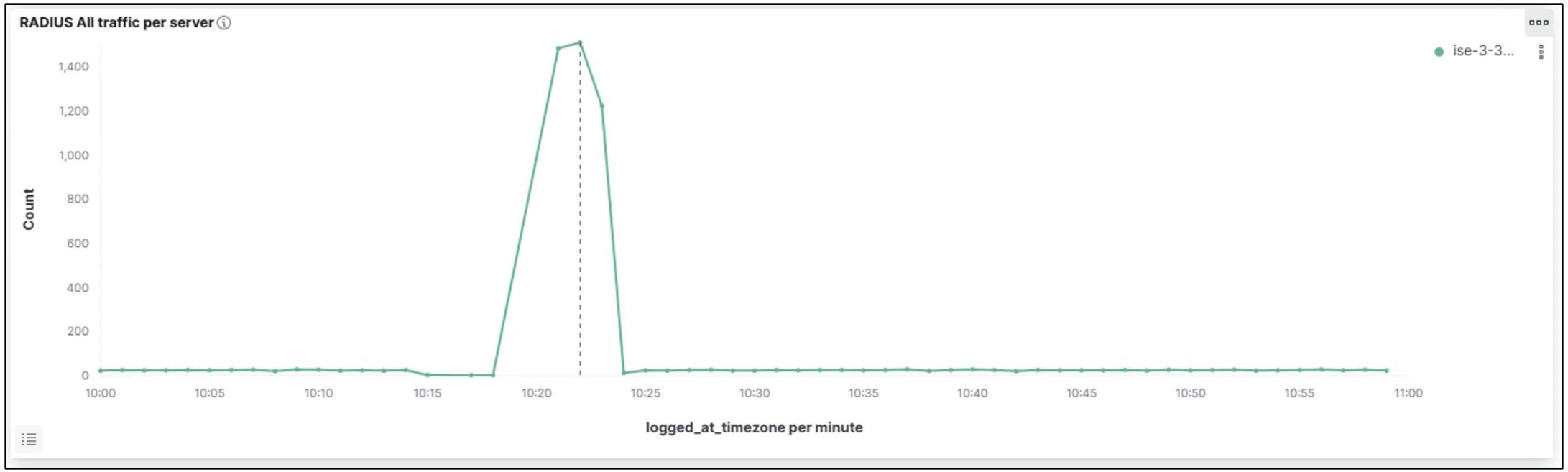


With Log Analytics we get an in-depth real time investigate the latency.

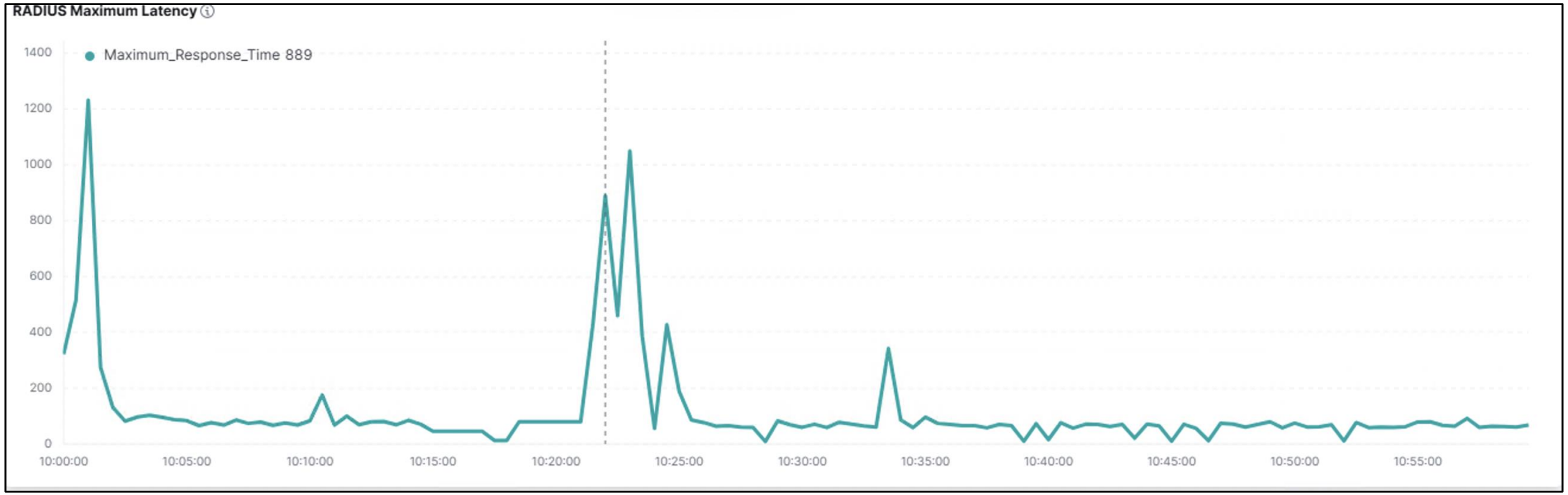
Under the Radius Performance Dashboard, we can view the overall traffic to a node, the maximum amount of latency on the node, and the average latency on the node.

From here we can take the time where the peaks match up and narrow our time filters on the dashboard to get a more in-depth view

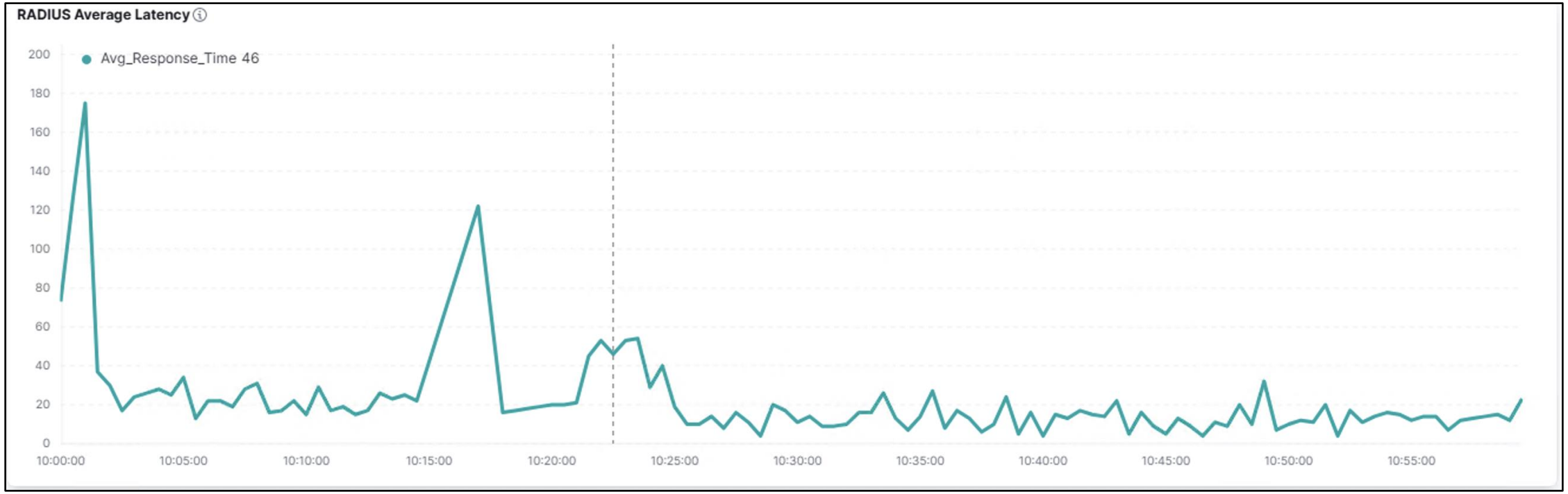
High Authentication Latency on PSN



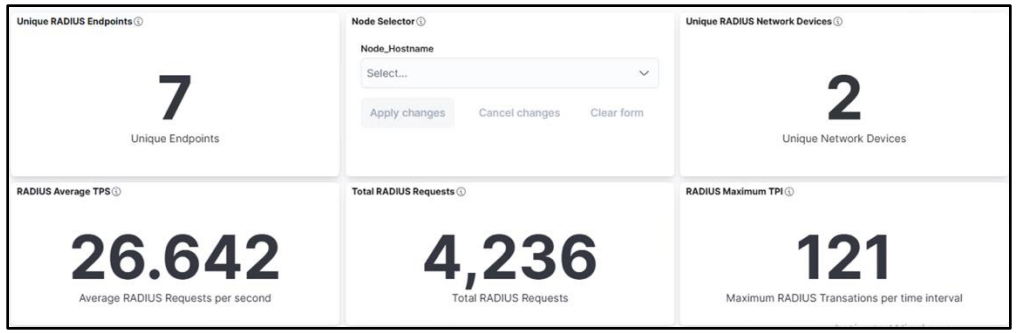
High Authentication Latency on PSN

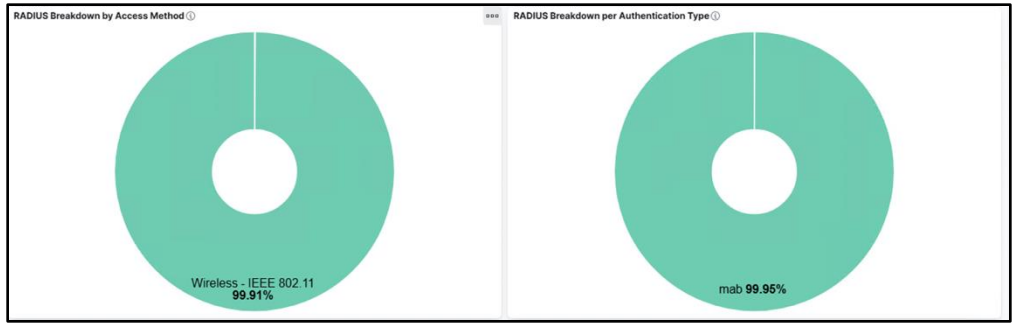


High Authentication Latency on PSN



High Authentication Latency on PSN



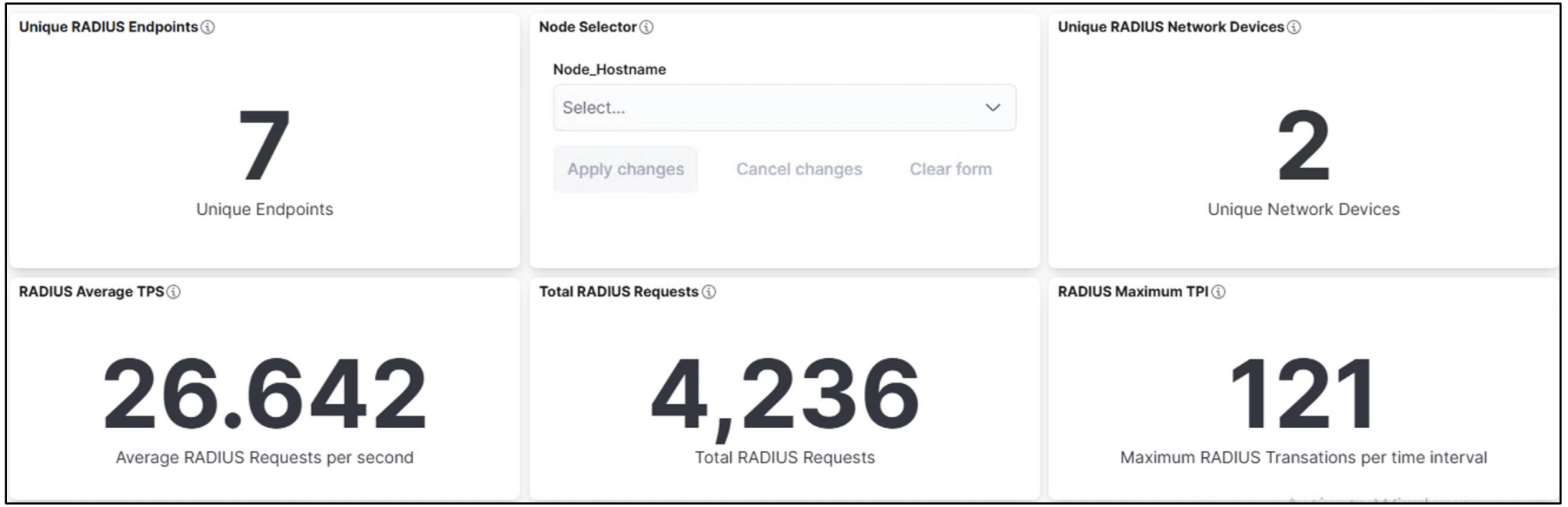


Here we get a better understanding of the total amount of radius traffic we received along with the TPS.

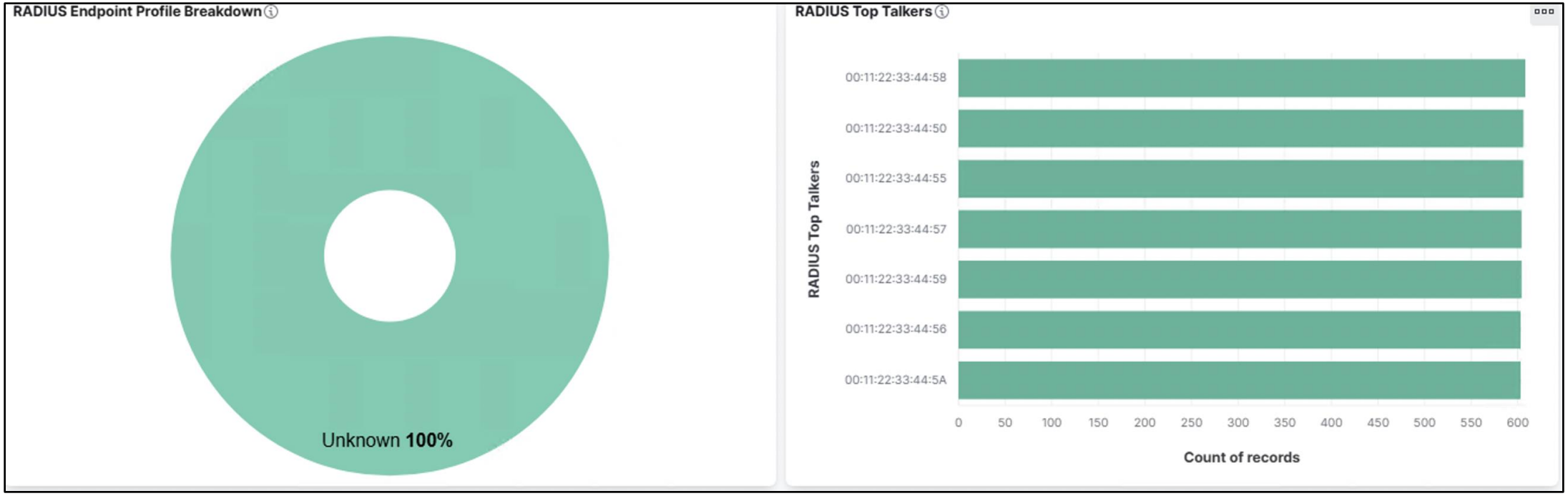
Additionally, we can highlight which NADS were sending the traffic, the type of authentications being received at this time, and the top radius talkers.

Now we can narrow down the time, type of endpoints, type of authentications, and NAD devices that were causing the High Auth Latency

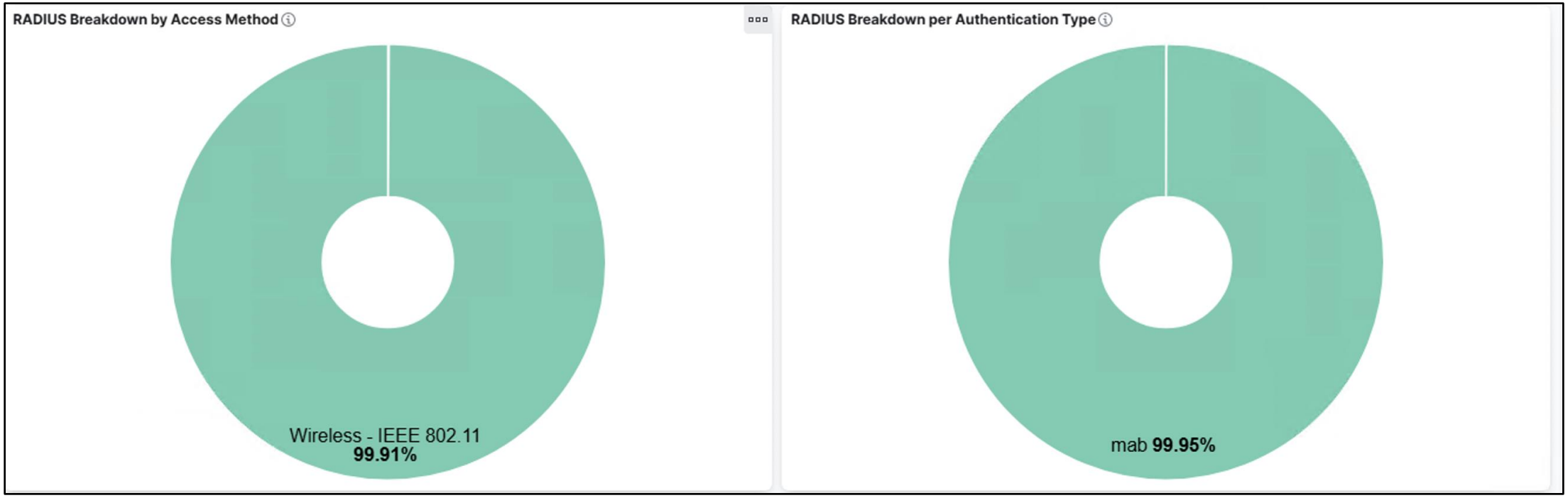
High Authentication Latency on PSN



High Authentication Latency on PSN



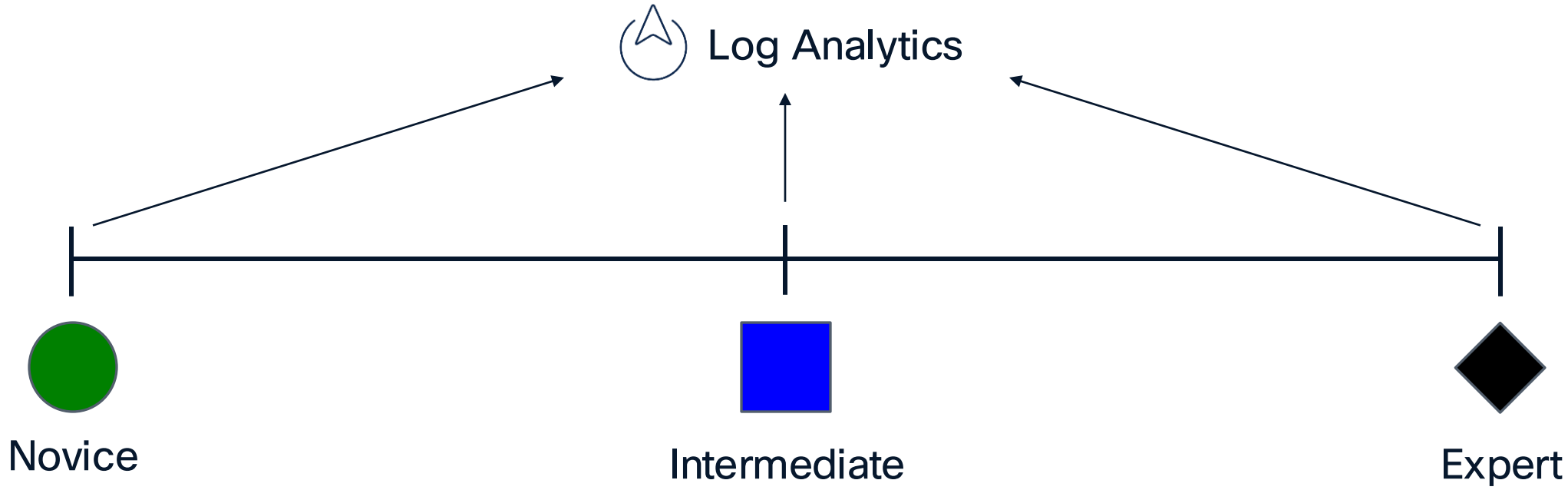
High Authentication Latency on PSN



Key Take Aways

- Visualize Your Data to Make Intuitive Decisions
- Customize Your Monitoring Experience to Your Deployment
- Get Real Time Analysis for Troubleshooting Support

Conclusion



References

- https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/admin_guide/b_ise_admin_3_3/b_ISE_admin_33_maintain_monitor.html#Cisco_Concept.dita_6903790d-f80e-49e0-9ee8-ce2a1b9c5f74
- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/220863-understand-log-analytics-elk-stack-on-ci.html
- https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html

Q&A

Complete your session evaluations

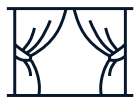
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: etglaser@cisco.com

Thank you


CISCO