CASTRA

The Castra Elastic Logger for USM Appliance

A faster, more advanced solution to pair with your existing USM instance

“ElasticSearch is fast! Based on our testing on lab and production systems, we’re seeing 50x-100x speed improvements”

Do you need to add long-term logging to your USM Appliance?

Do you want to combine the search power of Elastic with your advanced USM platform?

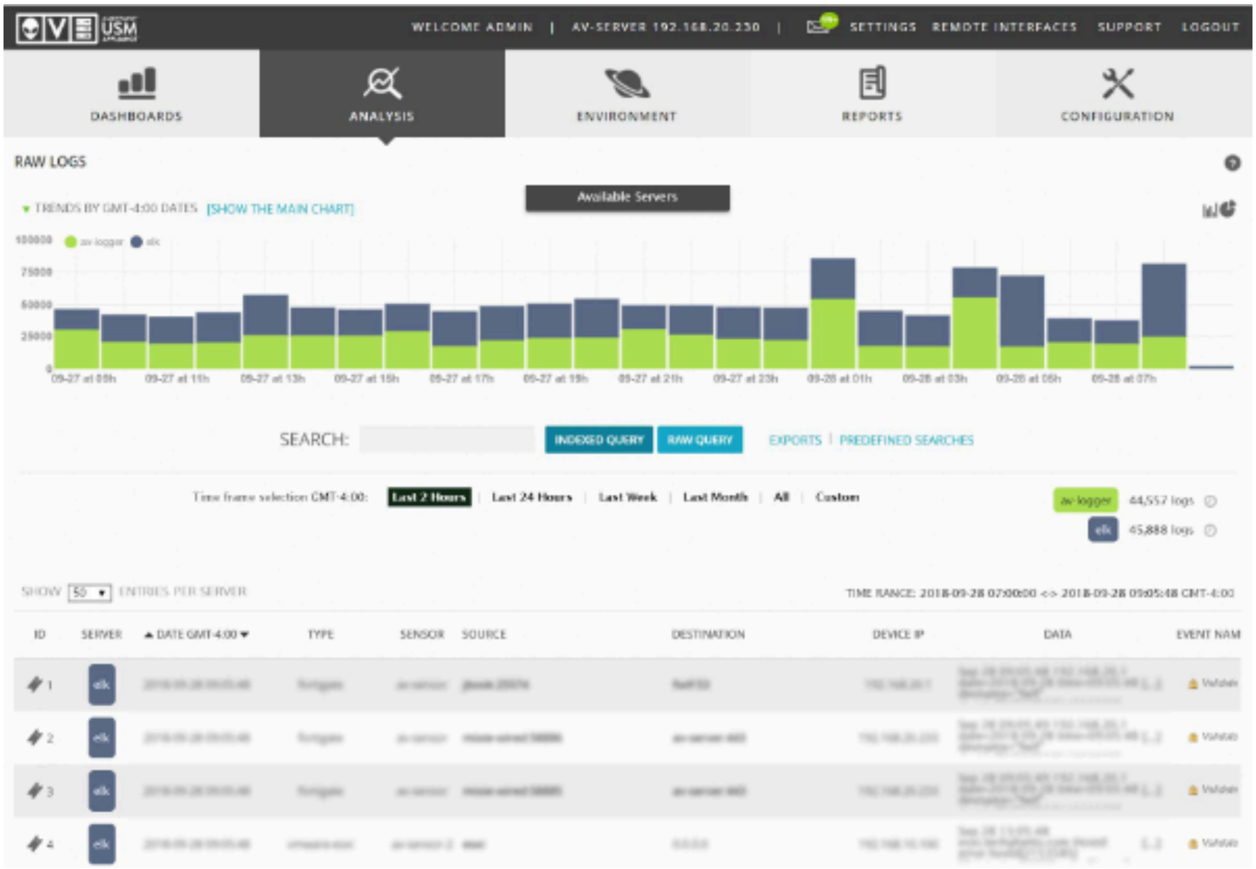
If you are looking to expand your raw log storage while adding new possibilities for analytics, visualization and reporting, Castra’s Elastic Logger is for you.

Castra has developed a powerful log management tool meant to become, expand or replace your existing USM Appliance Logger.

It is a fully-integrated, drop-in replacement that is built using the ultra-fast ElasticSearch engine (a standard ELK stack) but incorporates several custom components that allow it to connect transparently to your USM Appliance as if it were a "real" Logger.

Treat it like any other long-term Logger.

It brings fully indexed, rapid search capability to your log data, plus all of the benefits of the Kibana UI for advanced reporting and visualizations.



av-logger 44,557 logs

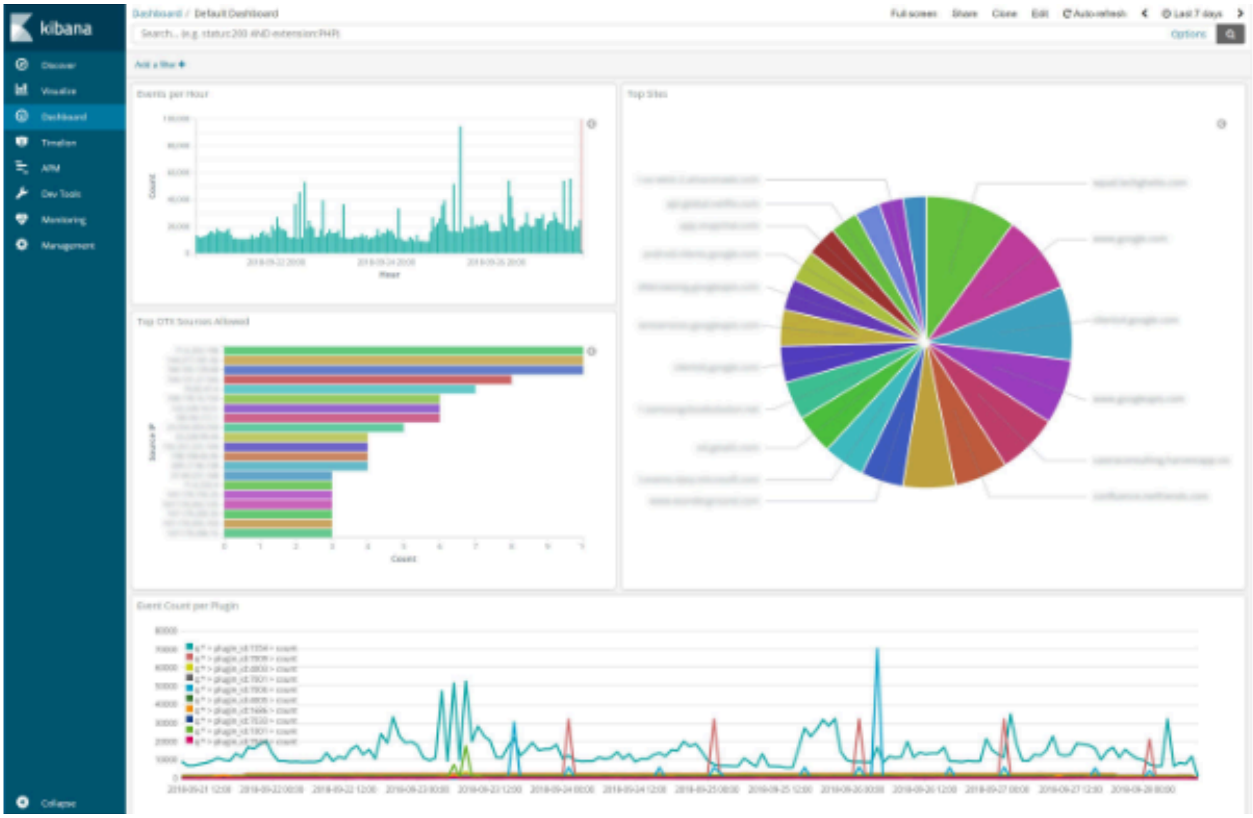
elk 45,888 logs

TIME RANGE: 2018-09-28 07:00:00 <-> 2018-09-28 09:05:48 GMT-4:00

From your USM Appliance UI, it appears like a standard Logger, and you can search Raw Logs normally.

Reports configured to run against the Logger also work as-is.

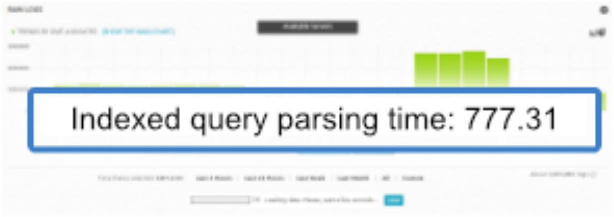
And outside of the full USM Appliance integration, you also get the full Kibana interface with its visualization and reporting capabilities that have helped make the ELK stack so popular.



Speed

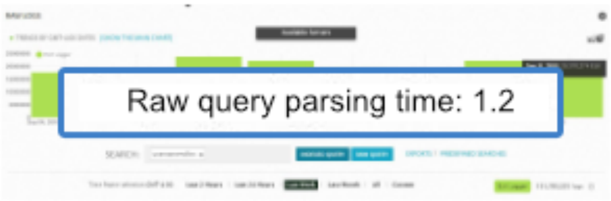
Most importantly, ElasticSearch is fast! Based on our testing on lab and production systems, we're seeing 50x-100x improvements over the normal USM Appliance Logger. Searches that took over 20 minutes on the Logger took less than 20 seconds on Castra's Elastic Logger. Reports that ran for over 45 minutes on the Logger took under 1 minute on Castra's Elastic Logger. This makes your analysts' lives much better and more productive while making the overall USM Appliance platform more valuable for your security monitoring.

Traditional Search



Indexed query parsing time: 777.31

ElasticSearch



Raw query parsing time: 1.2

Speed increases apply to more than just Raw Logs searches, the Castra Elastic solution is *fully* integrated, bringing its speed increases to USM and appears to the system just like a normal Logger.

Expandability

Since it uses the ElasticSearch engine, this also opens up other possibilities such as X-Pack, providing machine learning and anomaly detection using your log data. There are many other behavioral anomaly products out there, that can also sit on top of a Elastic data pool and provide new security insights for your environment.

Scalability

With Castra's ElasticSearch you're not limited by the amount of data you need to store. Need 4TB, 8TB, more? No problem, increase the storage size or add more nodes! Need redundancy? Also no problem, add more nodes! Elasticsearch was built to run as a cluster, so it can scale to dozens or even hundreds of TB of data.