Take The Pain Out of Log Management With Logging-as-a-Service

PUBLIC SECTOR

WHAT IS LOGGING-AS-A-SERVICE?

More devices are producing more log data than ever before, which means collecting, storing, and searching all those logs is much harder. Compounding the challenge is the OMB M21-31 mandate that requires civilian agencies to collect ALL logs. Agencies can no longer leave log data on the floor due to scalability issues.

Just like Software-as-a-Service provides all the benefits of a software solution without any of the infrastructure and administrative overhead, Logging-as-a-Service provides all of the benefits of a log management system without any of the administrative and infrastructure overhead. Logging-as-a-Service does the same thing that log management solutions have always done — collect, store, search, and analyze logs. But LaaS doesn't require racks of servers to administer, storage to manage, back-ups to create and move offsite, or all the other headaches that come with log management solutions.

The reason for using LaaS is simple: organizations need to focus on using log data to identify and solve problems instead of focusing on the incredible effort of supporting a log management solution.

WHY MOVE TO A LOGGING-AS-A-SERVICE SOLUTION?

1. Scale and Performance

Since the volume of log sources keeps increasing going up, traditional on-prem, self-managed solutions simply can't scale fast enough to keep up. The solution to the problem lies in the elasticity of the cloud. A LaaS solution scales up resources as needed. A traditional on-prem logging solution has limitations in compute and storage. But with a cloud-native, elastic Logging-as-a-Service solution, you can ingest ALL data sources. Both hot storage and cold storage can be added as needed to accommodate policies by the organization. Compute can be added to accommodate changing search or ingest needs. And this can be done instantly, without having to budget, acquire, deploy, and configure hardware. The agility of a LaaS solution keeps up with the ever-changing demands of the organization.

2. Easy Ingestion and Centralized Visibility

Most organizations are operating with a mix of on-prem components, private cloud components, and public cloud components with multiple providers. So they need a solution that collects and analyzes all logs across all environments. This isn't as easy as it sounds. You don't want a logging solution that relies on only one type of proprietary ingestion, such as an agent. Instead, you want a logging solution that supports a variety of collection methods — including the ones you are likely already using such as syslog, NXLog, and others. Although not required, using existing log collections methods will dramatically speed up the migration process of moving to a Logging-as-a-Service solution.

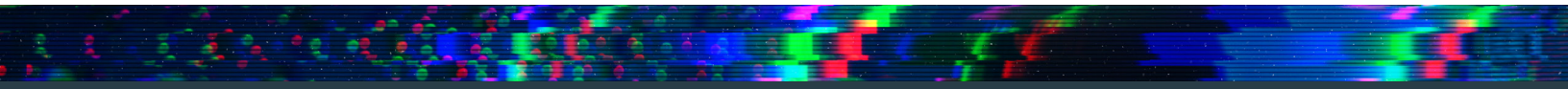
3. TCO

The total cost of ownership of a log management solution is large. License costs are just the tip of the iceberg. You also have CAPEX expenditures for hardware. Then you have heavy administrative costs. You need server admins, storage admins, network admins, and more just to keep the solution up and running. And you need to refresh and re-deploy the hardware every 3-5 years.

None of these costs exist with a Logging-as-a-Service solution. When you are a LaaS customer, you only pay to use the solution. You never have to worry about CAPEX budgets, hardware acquisition or deployment, or administrative overhead. You put all your focus into using the LaaS solution to identify and solve problems, not toward keeping the solution up and running.

WHY CHOOSE DEVO FOR YOUR LOGGING-AS-A-SERVICE SOLUTION?

Devo was designed and built from the ground up to be the ideal Logging-as-a-Service solution. Leveraging all the elasticity and capability of the AWS public cloud, Devo is infinitely scalable. Large organizations use Devo to handle the most demanding ingest and search needs, ingesting terabytes of data every day. Devo gives you 400 days of always hot data, with best in class search performance. For data older than 400 days, Devo archives years of cold data to AWS S3 and offers automatic rehydration of that cold data for compliance and audit use cases. Devo can ingest any data source, structured or unstructured, and is the ONLY LaaS solution that stores ALL your data in its original, raw format. So you never have to worry about losing data after you parse it. And Devo offers a myriad of ingest methods including leveraging your existing log collection methods. Devo also has a native multi-tenant architecture with a parent/child hierarchy that enables organizations to keep data separate and secure between child domains, but gives parent domains the option to roll up data from child domains. And Devo offers the most granular role-based access control for your data, giving you the ability to control search access down to the row and field level based on user roles.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.