ops_brew

secLines: Enterprise Logging as a Service

Delivering Automation, Flexibility, Scalability, Resilience and Control for your SecOps

Expensive Log Storage?
Report on Compliance and custom reports?
Need for faster searching and indexing of logs?
Vendor Lock-in?

Ops_brew is a self-service platform for building and maintaining log collection, normalization, transformation, redirection, and visualization pipelines. Ops_brew easily integrates open source tool chain and/or your existing technology stack to build pipelines and is built on Kubernetes enabling deployment in any environment of choice.

- Build end-to-end log pipelines in hours
- Out of the box RoC
- Identify and Secure sensitive data on the fly
- Fast Enterprise Log Search

Platform Observability

- Health and Performance Monitoring dashboards
- Easy pipeline bottleneck discovery
- Rule based alerting

Cost Saving on expensive SIEM storage

Reduced Ops Overhead

- Infrastructure as Code
- Platform built on Kubernetes
- Abstract Infrastructure Managment

Enhanced Threat Hunting with easy access to aged logs

Config Only & Zero Code Setup

- Drag and Drop pipeline components
- GUI for component configuration

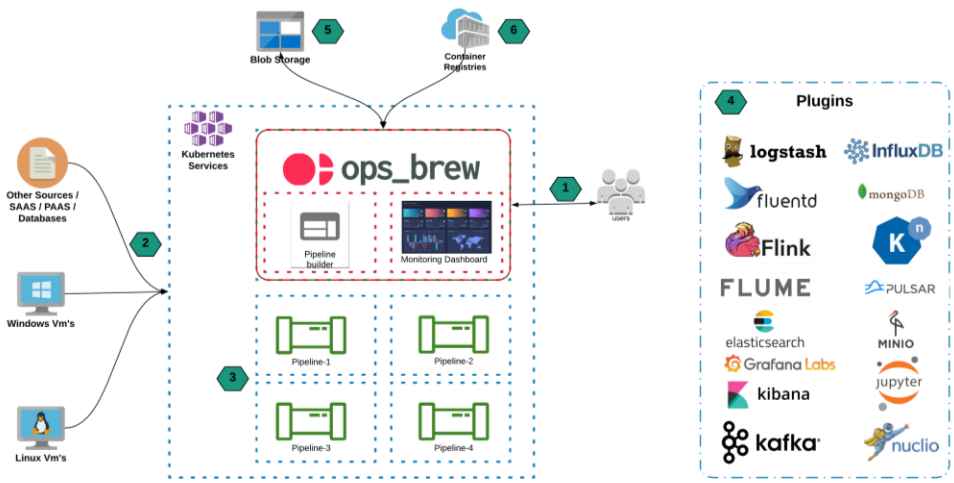
Easy and Cost-effective log archival

| www.adfolks.com

ops_brew

How Ops_brew works, to achieve business benefits

Opsbrew Architecture



Ops_brew on Azure

Our promise to you

Enterprise grade log search with low manageability overhead and seamless and elastic scaling to spikes in log activity

An offer to get you started

- 5 days free consultation
- Sizing estimates of the solution in your Azure environment

Opsbrew WorkFlow

1. Users will login to opsbrew platform and create pipelines. They can also monitor each components in the pipelines for understanding the choke metrics and act quickly using opsbrew's intelligent alerting system.
2. Multiple sources can be configured to send data to the pipelines. ie Windows/Linux logs, SAAS/PAAS, Databases logs send across to Data Collectors. Any agent can be installed/configured on sources.
3. Pipelines will be running on the customer AKS environment and administrator can manage isolation of pipelines by creating different teams.
4. Pipelines are build using the components listed in plugins box. Configuration of the listed components can be done from the web console.
5. Configuration, Logs/Data will be stored in Blob Storage for the longer data retention
6. Container images of all plugins are stored in Azure container registry

Opsbrew Deployment steps

1. Setup AKS cluster using aksctl CLI tool
   eg: aksctl create cluster --name opsbrew --resource-group opsbrew-rg --nodes 2 --location us-east
2. Deploy opsbrew platform to AKS cluster by running the deploy.sh script
3. Wait until opsrew get ready to build pipelines and check the status of pods by running the below command
   kubectl get pods --namespace opsbrew-system
4. Get the IP in which the service is exposed, by running the below command
   kubectl get svc
5. Go to the IP to access Opsbrew platform

Tangible Benefits / Desired Outcomes

- ROC and Evidence collection
- Logging in distributed environments spread across numerous apps, infrastructure and devices
- Monitor high-volume log data in modern dynamic environments.

Why Adfolks?

Adfolks is a Microsoft Azure Gold Partner providing technical services in Data Science and Engineering, Modern Infrastructure, Cyber Security, and CloudOps. We are also the first Kubernetes Certified Service Provider in the Middle East. Adfolks has a successful track record helping enterprises in the region adopt, manage and operate cloud native technologies to drive business value.