LOGGLY

Loggly Playbook

10 steps to successfully adopting a log management solution

By Pranay Kamat

With a solution like Loggly, there's a lot more to log management than searching your logs to find a bug or troubleshoot an operational issue. We conducted in-depth interviews with a set of highly satisfied customers to understand how they are setting up Loggly and using it on a daily basis to improve their DevOps processes. Based on this research, we have developed this playbook that guides you on how your team can get the most out of Loggly in 10 easy steps. This playbook is suitable for users new to Loggly as well as those who are currently using Loggly.

1

Send all your logs

- Send all your logs: application, server, Docker, containers, microservices, database, mobile, network, etc. Having a complete picture of your application is more valuable than looking separately at individual parts.[1]
- Send logs from all your environments and instances: development, QA staging, and production.
- Send logs from your AWS sources such as Amazon S3, Amazon CloudWatch, Amazon CloudTrail, Amazon ELB, and Amazon CloudFront.
- Send logs in JSON whenever you can.

[1] Concerned about cost? Don't worry. We have pricing plans that discount the less critical data that you may not have thought about storing due to cost.

2

Tag your logs

- Include meaningful tags when you send a log event. This allows you to search, categorize, and correlate your logs easily. Examples of tags include systemid to indicate the system where it originated, geographical location, severity of the error, etc.
- Insert custom tags using the Loggly Derived Fields feature.

3

Segment your logs

- Create Source Groups to organize and filter data as development, QA, staging, or production; you can also use Source Groups to restrict access for certain types of users such as partners, contractors, and consultants.

4

Archive your logs

- Specify a new or existing Amazon S3 bucket and archive your logs if you have compliance requirements.

5

Select preconfigured dashboards

- Install Loggly's App Packs for Linux, Apache, Nginx, CloudWatch, CloudTrail, and ELB and get insights quickly.

6

Integrate with your incident management tool to receive alerts

- Add a webhook or email integration for PagerDuty, OpsGenie, or VictorOps.

7 Integrate with your collaboration tool to receive alerts

- Add a webhook for Slack, HipChat, or Microsoft Teams.

8 Integrate with your issue and project tracking tool

- Set up integration with JIRA.

9 Save your popular searches

- Check out our tips and tricks on our Lucene-based search query syntax.
- Save your common searches. A saved search is available to everyone in your team.

10 Invite your team

- Invite other members of your team including engineering, Ops, support reps, and product managers.
- Restrict user access to specific data based on Source Groups.
- Set up Single Sign-On if you have an existing identity provider.

Following the steps in this playbook will not only make you productive more quickly but will also increase the ultimate value you gain from a centralized log management service.

As you get more familiar with Loggly, be sure to test out Loggly Live Tail (to monitor a release, for example—you can even send logs to a Slack channel, HipChat room, or Datadog) and Anomaly Detection for proactively detecting issues that you may not expect.

If you are new to Loggly, you can see the benefits first-hand with a full-featured 30-day trial.

LOGGLY

FREE TRIAL