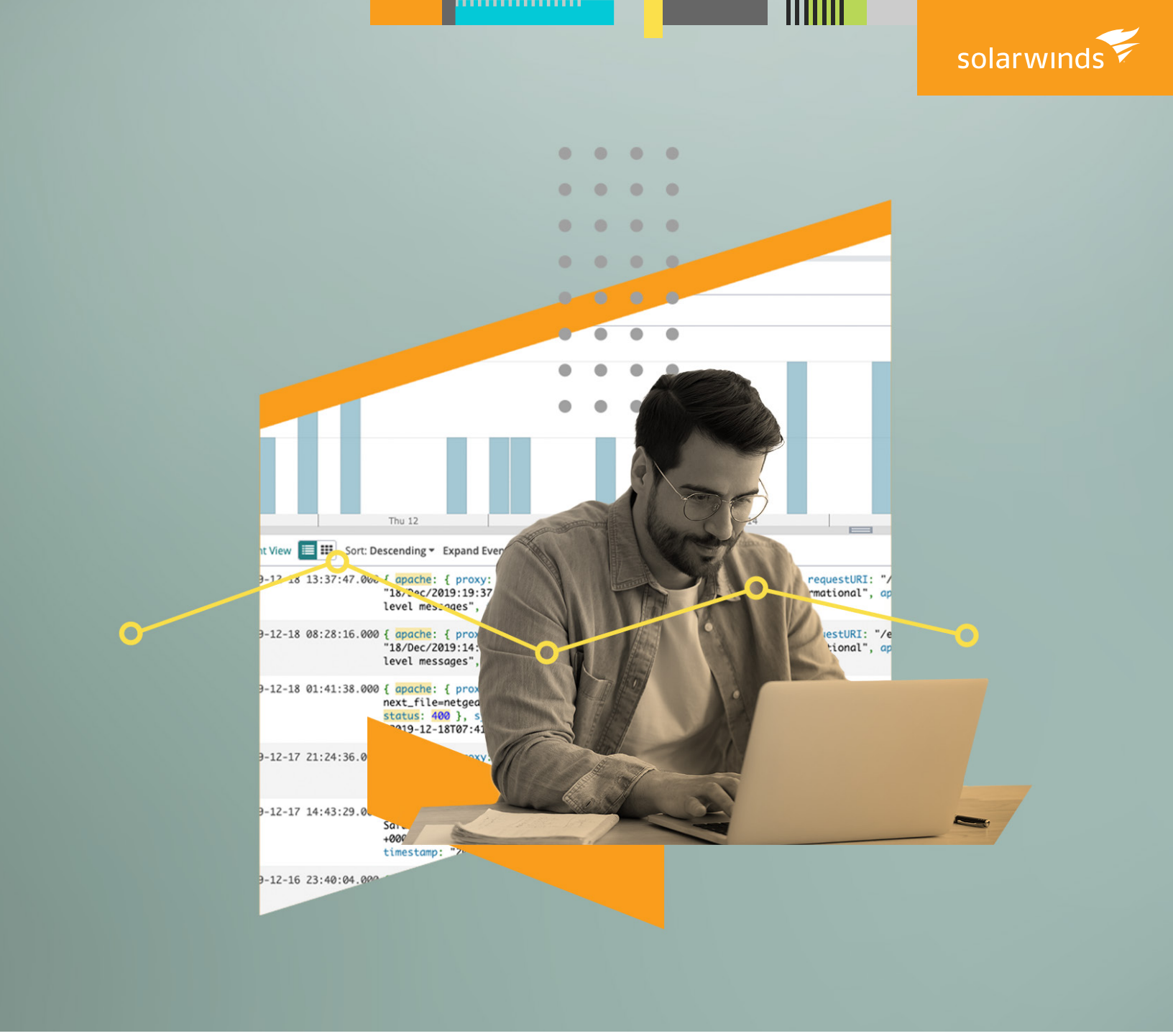

eBOOK

SolarWinds Loggly Playbook

10 steps to successfully adopting a log management solution

by Dave Wagner and Pravesh Ramachandran

SolarWinds Loggly Playbook

10 steps to successfully adopting a log management solution

With a comprehensive solution like SolarWinds® Loggly®, there's more to log management than simply searching your logs to find a bug or troubleshoot operational issues—a LOT more! We conducted in-depth interviews with a set of highly satisfied customers to understand how they are setting up and using Loggly daily to improve their DevOps processes. Based on this research, we have developed this playbook to guide you on how your team can get the most value from Loggly in 10 easy steps.

This playbook is suitable for users new to Loggly and those who are currently using Loggly.

1. SEND ALL YOUR LOGS

- Send logs from all your environments and instances across the application lifecycle: 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, so you can analyze your logs like a structured and query-able database.
- In short—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 or missing critical data because you didn't capture it.

Concerned about costs? Don't worry. In addition to flexible pricing plans that adapt to the less critical data you may not have considered storing due to cost, Loggly offers visibility into the data volume being indexed and stored with Log Usage Dashboards and detailed views of data volumes associated with specific searches and source groups, allowing you complete visibility and control to proactively manage and prioritize your log data volume.

2. TAG YOUR LOGS

- Include meaningful tags when you send a log event. This allows you to search, categorize, group, and correlate your logs more easily and quickly. Examples of such custom tags include systemid

to indicate the system where it originated, geographical location, severity of the error, etc.—information by which you'll want to organize, analyze, and manage logs from given sources. And, you should endeavor to be as consistent about your tagging nomenclature as possible to maximize your ability to…

- Insert these custom tags using the Loggly derived fields feature. Derived fields let you define custom parsing rules for log events, allowing you to add structure to logs, create new fields, and index events in ways that matter to you and your use cases. This extends the powerful built-in Loggly parsing rules, so you have instant access to information in logs without having to manually search.

3. SEGMENT YOUR LOGS

- Create Source Groups (also known as Log 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. You can also understand your log volume usage by Source Group, so you should factor this into your Source Group nomenclature and taxonomy. Because you can also filter log volume usage by these groups, it gives users and groups of users the cost-effective ability to manage only those logs of importance to their specific needs.

4. ARCHIVE YOUR LOGS

- If you have, or expect to have, compliance requirements for your log data, you should specify a new or existing Amazon S3 bucket and automatically archive your logs. This gives you a cost-effective method of ensuring your historical record of events is maintained for the duration mandated by your compliance requirements.

5. START WITH PRE-CONFIGURED DASHBOARDS

- Use Loggly pre-configured dashboards to get instant insights across the most popular log sources. You can then easily extend and customize dashboards to fit your specific requirements. Dashboards are valuable to ensure a shared understanding across members of the technical team using Loggly and across both the technical and business organization.

6. INTEGRATE WITH YOUR INCIDENT MANAGEMENT TOOLS TO RECEIVE ALERTS

- Add a webhook, email integration for PagerDuty, or other alert endpoints. This ensures workflow-process integration with your existing event management tools and processes.

7. INTEGRATE WORKFLOW WITH YOUR COLLABORATION TOOLS TO RECEIVE ALERTS

- Add a webhook for Slack, Microsoft Teams, or other collaboration tools to ensure appropriate members of your broader teams can benefit from Loggly proactive notification capabilities, further extending workflow integration.

8. INTEGRATE WITH YOUR ISSUE AND PROJECT TRACKING TOOL

- Because events occurring during development can significantly impact development decisions, team productivity, and ultimately production deployment, it's important to implement integration with your development project tracking and management tools. With Loggly, it's easy to set up integration with GitHub or Atlassian Jira.

9. SAVE YOUR MOST POPULAR AND PRODUCTIVE SEARCHES (AND USE THEM FOR PROACTIVE ALERTING)

- Check out our tips and tricks on our Lucene-based search query syntax.
- Save your common searches. A saved search is available to everyone on your team and can be used to proactively alert you and your teams to potential issues before they become critical, service-impacting events.

10. INVITE AND INCLUDE YOUR ENTIRE TEAM

- Invite other members of your team including engineering, development, Ops, support reps, and product managers. There's no cost for additional users, and the benefits of cross-team collaboration are significant in terms of speeding root cause analysis in complex environments—everyone is working from a shared understanding and knowledge base.
- 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 can make you more productive more quickly and increase the ultimate value you gain from a centralized log management service.

As you get more familiar with Loggly, be sure to test out the workflow integration between SolarWinds AppOptics™ and Loggly—the ability to drill down from performance traces to related log entries—enabling fast, and more focused than ever, root cause analysis and mean time to repair (MTTR).

If you're new to Loggly, you can see the benefits first hand with your logs in a full-featured trial.

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT management software. Our products give organizations worldwide—regardless of type, size, or complexity—the power to monitor and manage their IT services, infrastructures, and applications; whether on-premises, in the cloud, or via hybrid models. We continuously engage with technology professionals—IT service and operations professionals, DevOps professionals, and managed services providers (MSPs)—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures and applications. The insights we gain from them, in places like our THWACK community, allow us to solve well-understood IT management challenges in the ways technology professionals want them solved. Our focus on the user and commitment to excellence in end-to-end hybrid IT management has established SolarWinds as a worldwide leader in solutions for network and IT service management, application performance, and managed services. Learn more today at www.solarwinds.com.

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx