This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

About system logs

In this article

System logs

Types of logs

Audited system events

Support bundles

Further reading

GitHub Enterprise Server keeps error and message logs for system events. Logs are useful for identifying user, application and system-level actions and exceptions.

System logs

By default, system logs for GitHub Enterprise Server are automatically rotated every 24 hours and are retained for seven days. System logs include system-level events, application logs, and Git events data. As log files are often being written to and can be large in size, it may be beneficial to extract and parse relevant log entries on a host separate to your GitHub Enterprise Server instance.

You can forward system logs to a third-party system or server for longer retention. For more information see "Log forwarding."

In addition to reviewing your system logs, you can monitor activity in your enterprise in other ways, such as viewing audit logs, push logs and managing global webhooks. For more information, see "Monitoring activity in your enterprise."

Types of logs

Listed below are the main logs used by the GitHub Enterprise Server appliance and their functions:

Path	Description
`/var/log/github/audit.log`	Audited user, repository and system events.
`/var/log/github/resqued.log`	Details about background jobs.
`/var/log/github/unicorn.log`	API and web interface traffic.
`/var/log/github/exceptions.log`	Application-level errors.
`/var/log/haproxy.log`	All IP traffic reaching the appliance.

`/var/log/hookshot/resqued.log`	Webhook delivery and failures.
`/var/log/github/auth.log`	Authentication requests, whether through built in, LDAP, CAS or SAML methods.
`/var/log/github/gitauth.log`	All Git authentication requests.

Git activity and authentication requests are processed by the `babeld` service.

Several GitHub Enterprise Server services, such as the `babeld` service, are containerized. Containerized logs are written to the `systemd journal`, and can be queried at any time using the `journalctl` command.

Audited system events

All entries from the `audit.log` file use and can be filtered with the `github_audit` keyword.

For example, this entry shows that a new repository was created.

```
Oct 26 01:42:08 github-ent github_audit: {:created_at=>1351215728326, :actor_ip=>"1
```

This example shows that commits were pushed to a repository.

```
Oct 26 02:19:31 github-ent github_audit: { "pid":22860, "ppid":22859, "program":"re
```

Support bundles

The support bundle includes system logs and all audit information is logged to the `audit.log` file in the `github-logs` directory. For more information, see "Providing data to GitHub Support."

Further reading

- Linux man page for the `journalctl` command