About system logs

In this article

To help administrators understand activity and errors, GitHub Enterprise Server stores system logs.

About system logs for GitHub Enterprise Server

To trace, review, and troubleshoot activity and exceptions on your GitHub Enterprise Server instance, you can review system logs. Your instance stores the following two types of system logs.

- Plain text log files on disk, stored by syslog or specific services
- Binary log files, stored by journald

By default, GitHub Enterprise Server rotates system logs automatically every 24 hours and retains rotated logs for seven days. System logs include system-level events, application logs, and data about Git events. Because log files are written often and can be large in size, you may prefer to extract and parse log entries on a host separate from your GitHub Enterprise Server instance.

People with administrative SSH access to a GitHub Enterprise Server instance can access and read system logs. For more information, see "Accessing the administrative shell (SSH)."

You can forward system logs and audit logs to an external system for analysis or longer retention. For more information see "Log forwarding" and "Streaming the audit log for your enterprise."

In addition to reviewing your system logs, you can monitor activity on your instance in other ways. For example, you can review audit logs and push logs, or configure global webhooks. For more information, see "Monitoring activity in your enterprise."

Note: The following lists of logs are not intended to be comprehensive.

System log files

GitHub Enterprise Server writes several categories of system logs to the instance's disk in plain text. People with administrative SSH access to the instance can parse these files using Linux command-line tools such as `cat`, `tail`, `head`, `less`, and `more`.

- Log files for databases
- Log files for the GitHub application
- Log files for the HTTP server

- Log files for instance configuration
- Log files for the Management Console
- Log files for search
- Log files for storage
- Log files for webhooks
- Log files for system services

Log files for databases

The following log files record events from database services on your instance.

Path	Description
`/var/log/mysql/mysql.log`	Records events related to the instance's MySQL database.
`/var/log/mysql/mysql.err`	Records errors related to the instance's MySQL database.

Log files for the GitHub application

The following log files record events from the GitHub application on your instance.

Path	Description
`/var/log/github/audit.log`	Records user, repository, and system events for activity in the GitHub application on your instance. You can filter entries in the log using the `github_audit` keyword.
`/var/log/github/exceptions.log`	Records exceptions that the GitHub application encounters.
`/var/log/github/gitauth.log`	Records Git authentication requests using HTTPS or SSH. The `babeld` service processes all Git authentication requests and activity.
`/var/log/github/production.log`	Records internal events for the GitHub application. For requests to the website, includes the controller action that responded. May contain entries with different structures, depending on the origin of the job or request.

Log files for the HTTP server

The following log files record events from the instance's HTTP server.

Path	Description
`/var/log/nginx/error.log*`	Records errors for web requests.
`/var/log/nginx/gist.log`	Records HTTP requests related to gists. For more information, see "Creating gists."
	Records errors related to HTTP requests for

`/var/log/nginx/gist.error.log`	gists.
`/var/log/nginx/github.log`	Records HTTP requests to the GitHub application.
`/var/log/nginx/github.error.log`	Records errors associated with HTTP requests.
`/var/log/nginx/pages.log`	Records HTTP requests associated with GitHub Pages. For more information, see "About GitHub Pages."
`/var/log/nginx/pages.error.log`	Records errors related to HTTP requests for GitHub Pages.

Log files for the Management Console

The following log files contain events from your instance's Management Console. For more information, see "About the Management Console."

Path	Description
`/var/log/enterprise-manage/audit.log`	Records activity in the instance's Management Console.
`/var/log/enterprise-manage/unicorn.log`	Records HTTP and HTTPS operations that administrators perform in the Management Console using the web UI or REST API.

Log files for instance configuration

The following log files contain events related to the configuration of your instance.

Path	Description
`/data/user/common/ghe-config.log`	Records events associated with each configuration run. If a configuration run fails, output to the log stops. This log also records information about migrations that run during the process of upgrading an instance's software. For more information, see "Command-line utilities."

Log files for search

The following log files contain events from services that provide search functionality for your instance.

Path	Description
`/var/log/elasticsearch/github-enterprise.log`	Records events associated with the Elasticsearch service, which your instance uses to provide search services.

Log files for webhooks

The following log files contain events from the service that delivers webhook payloads for your instance. For more information, see "About webhooks."

Path	Description
`/var/log/hookshot/resqued.log`	Records webhook deliveries and failures from your instance.
`/var/log/hookshot/unicorn.log`	Records webhook events that are triggered on your instance.

Log files for system services

The following logs contain events from system services on your instance.

Path	Description
`/var/log/coredumps.log`	Records information about system processes that terminate unexpectedly.
`/var/log/boot.log`	Records information about the instance's boot process.
`/var/log/chrony/`	This directory contains logs related to Network Time Protocol (NTP) synchronization and the instance's system clock. For more information, see "Configuring time synchronization."
`/var/log/haproxy.log`	Records all web and API requests to the instance. For HTTP connections, entries include the URL that the client requested, as well as the HTTP method for the request.
`/var/log/ssh-console-audit.log`	Records commands that administrators run using the administrative shell (SSH). For more information, see "Accessing the administrative shell (SSH)."
`/var/log/mail-replies/metroplex.log`	Records information about mail that your instance receives. For more information, see "Configuring email for notifications."

System logs in the systemd journal

Several GitHub Enterprise Server services, such as the `babeld` service, are containerized. GitHub Enterprise Server writes system logs for these services to the systemd journal in a binary format.

People with administrative SSH access to the instance can parse these logs using the `journalctl` command. For more information, see journalctl(1) in the online Linux manual pages.

To view logs in the systemd journal, run the following command, replacing SERVICE-NAME with a service name from the following list of logs.

```
journalctl -t SERVICE-NAME
```

Journal logs for the GitHub application

The following logs record events from the GitHub application on your instance.

Service name	Description
`github-resqued`	Records events related to background jobs. If the job involves built-in or external authentication, this log includes information about the request. If the instance uses LDAP authentication and LDAP Sync is enabled, events for LDAP Sync appear in this log. For more information, see "Using LDAP."
`github-unicorn`	Records HTTP and HTTPS operations that users perform in the instance's web UI or via the APIs. If the operation involves built-in or external authentication, this log includes information about the request. If debug logging is enabled for LDAP or SAML authentication, the debug-level information for authenticated requests appear in this log. For more information, see "Using LDAP" or "Troubleshooting SAML authentication."

Journal logs for Git

The following logs contain events related to Git activity on your instance.

Service name	Description
`babeld`	Records events for all Git activity on the instance, including authentication to access the repository.
`codeload`	Records events for activity related to the generation or retrieval of code archives for repositories on the instance.
`gpgverify`	Records events related to commit signature verification. For more information, see "About commit signature verification."

Journal logs for storage

The following logs contain events from services that store or retrieve data on your instance.

Service name	Description
`alambic`	Records events related to the storage and retrieval of files, such as Git LFS objects, avatar images, file attachments from comments in the web UI, and release archives.

About system logs in support bundles

If you generate a support bundle, the file includes system logs. For more information, see "Providing data to GitHub Support."