System overview

In this article

Learn more about GitHub Enterprise Server's system internals, functionality, and security.

About GitHub Enterprise Server

GitHub Enterprise Server is a self-hosted platform for software development within your enterprise. GitHub distributes GitHub Enterprise Server as a self-contained virtual appliance. After you provision a virtual machine and install the appliance, the instance runs a Linux operating system with a custom application stack. For more information, see "About GitHub Enterprise Server."

Storage architecture

GitHub Enterprise Server requires two storage volumes, one mounted to the *root filesystem* path (`/`) and the other to the *user filesystem* path (`/data/user`). This architecture simplifies the upgrade, rollback, and recovery procedures by separating the running software environment from persistent application data.

The root filesystem is included in the distributed machine image. It contains the base operating system and the GitHub Enterprise Server application environment. The root filesystem should be treated as ephemeral. Any data on the root filesystem will be replaced when upgrading to future GitHub Enterprise Server releases.

The root storage volume is split into two equally-sized partitions. One of the partitions will be mounted as the root filesystem (`/`). The other partition is only mounted during upgrades and rollbacks of upgrades as `/mnt/upgrade` , to facilitate easier rollbacks if necessary. For example, if a 200GB root volume is allocated, there will be 100GB allocated to the root filesystem and 100GB reserved for the upgrades and rollbacks.

The root filesystem contains files that store the following information. This list is not exhaustive.

- Custom certificate authority (CA) certificates (in `/usr/local/share/ca-certificates*`)
- Custom networking configurations
- Custom firewall configurations
- The replication state

The user filesystem contains files that store following configuration and data. This list is

not exhaustive.

- Git repositories
- Databases
- Search indexes
- Content published on GitHub Pages sites
- Large files from Git Large File Storage
- Pre-receive hook environments

Deployment topologies

You can deploy GitHub Enterprise Server in a variety of topologies, such as a high availability pair. For more information, see "About GitHub Enterprise Server."

Data retention and datacenter redundancy

Warning: Before using GitHub Enterprise Server in a production environment, we strongly recommend you set up backups and a disaster recovery plan.

GitHub Enterprise Server includes support for online and incremental backups with GitHub Enterprise Server Backup Utilities. You can take incremental snapshots over a secure network link (the SSH administrative port) over long distances for off-site or geographically dispersed storage. You can restore snapshots over the network into a newly provisioned instance at time of recovery in case of disaster at the primary datacenter.

In addition to network backups, both AWS (EBS) and VMware disk snapshots of the user storage volumes are supported while the instance is offline or in maintenance mode. Regular volume snapshots can be used as a low-cost, low-complexity alternative to network backups with GitHub Enterprise Server Backup Utilities if your service level requirements allow for regular offline maintenance.

For more information, see "Configuring backups on your instance."

Security

GitHub Enterprise Server runs on your infrastructure and is governed by access and security controls that you define, such as firewalls, network policies, IAM, monitoring, and VPNs. GitHub Enterprise Server is suitable for use by enterprises that are subject to regulatory compliance, which helps to avoid issues that arise from software development platforms in the public cloud.

GitHub Enterprise Server also includes additional security features.

- Operating system, software, and patches
- Network security
- Application security
- External services and support access
- Encrypted communication
- Users and access permissions
- Authentication
- Audit and access logging

Operating system, software, and patches

GitHub Enterprise Server runs a customized Linux operating system with only the necessary applications and services. GitHub distributes patches for the instance's core operating system as part of its standard product release cycle. Patches address functionality, stability, and non-critical security issues for GitHub Enterprise Server. GitHub also provides critical security patches as needed outside of the regular release cycle.

GitHub Enterprise Server is provided as an appliance, and many of the operating system packages are modified compared to the usual Debian distribution. We do not support modifying the underlying operating system for this reason (including operating system upgrades), which is aligned with the GitHub Enterprise Server license and support agreement, under section 11.3 Exclusions.

Currently, the base operating system for GitHub Enterprise Server is Debian 10 (Buster), which receives support under the Debian Long Term Support program.

Regular patch updates are released on the GitHub Enterprise Server releases page, and the release notes page provides more information. These patches typically contain upstream vendor and project security patches after they've been tested and quality approved by our engineering team. There can be a slight time delay from when the upstream update is released to when it's tested and bundled in an upcoming GitHub Enterprise Server patch release.

Network security

GitHub Enterprise Server's internal firewall restricts network access to the instance's services. Only services necessary for the appliance to function are available over the network. For more information, see "Network ports."

Application security

GitHub's application security team focuses full-time on vulnerability assessment, penetration testing, and code review for GitHub products, including GitHub Enterprise Server. GitHub also contracts with outside security firms to provide point-in-time security assessments of GitHub products.

External services and support access

GitHub Enterprise Server can operate without any egress access from your network to outside services. You can optionally enable integration with external services for email delivery, external monitoring, and log forwarding. For more information, see "Configuring email for notifications," "Setting up external monitoring," and "Log forwarding."

You can manually collect and send troubleshooting data to GitHub Support. For more information, see "Providing data to GitHub Support."

Encrypted communication

GitHub designs GitHub Enterprise Server to run behind your corporate firewall. To secure communication over the wire, we encourage you to enable Transport Layer Security (TLS). GitHub Enterprise Server supports 2048-bit and higher commercial TLS certificates for HTTPS traffic. For more information, see "Configuring TLS."

By default, the instance also offers Secure Shell (SSH) access for both repository access using Git and administrative purposes. For more information, see "About SSH" and "Accessing the administrative shell (SSH)."

If you configure SAML authentication for your GitHub Enterprise Server instance, you can enable encrypted assertions between the instance and your SAML IdP. For more

information, see "Using SAML for enterprise IAM."

Users and access permissions

GitHub Enterprise Server provides three types of accounts.

- The `admin` Linux user account has controlled access to the underlying operating system, including direct filesystem and database access. A small set of trusted administrators should have access to this account, which they can access over SSH. For more information, see "Accessing the administrative shell (SSH)."
- User accounts in the instance's web application have full access to their own data and any data that other users or organizations explicitly grant.
- Site administrators in the instance's web application are user accounts that can manage high-level web application and instance settings, user and organization account settings, and repository data.

For more information about GitHub Enterprise Server's user permissions, see "Access permissions on GitHub."

Authentication

GitHub Enterprise Server provides four authentication methods.

- SSH public key authentication provides both repository access using Git and administrative shell access. For more information, see "About SSH" and "Accessing the administrative shell (SSH)."
- Username and password authentication with HTTP cookies provides web application access and session management, with optional two-factor authentication (2FA). For more information, see "Configuring built-in authentication."
- External LDAP, SAML, or CAS authentication using an LDAP service, SAML Identity Provider (IdP), or other compatible service provides access to the web application. For more information, see "Using SAML for enterprise IAM."
- OAuth and personal access tokens provide access to Git repository data and APIs for both external clients and services. For more information, see "Managing your personal access tokens."

Audit and access logging

GitHub Enterprise Server stores both traditional operating system and application logs. The application also writes detailed auditing and security logs, which GitHub Enterprise Server stores permanently. You can forward both types of logs in real time to multiple destinations via the `syslog-ng` protocol. For more information, see "About the audit log for your enterprise" and "Log forwarding."

Access and audit logs include information like the following.

Access logs

- Full web server logs for both browser and API access
- Full logs for access to repository data over Git, HTTPS, and SSH protocols
- Administrative access logs over HTTPS and SSH

Audit logs

- User logins, password resets, 2FA requests, email setting changes, and changes to authorized applications and APIs
- Site administrator actions, such as unlocking user accounts and repositories

- Repository push events, access grants, transfers, and renames
- Organization membership changes, including team creation and destruction

Open source dependencies for GitHub Enterprise Server

You can see a complete list of dependencies in your instance's version of GitHub Enterprise Server, as well as each project's license, at `http(s)://HOSTNAME/site/credits`.

Tarballs with a full list of dependencies and associated metadata are available on your instance.

- For dependencies common to all platforms, at `/usr/local/share/enterprise/dependencies-<GHE version>-base.tar.gz`
- For dependencies specific to a platform, at `/usr/local/share/enterprise/dependencies-<GHE version>-<platform>.tar.gz`

Tarballs are also available, with a full list of dependencies and metadata, at `https://enterprise.github.com/releases/<version>/download.html`.

Further reading

- "Setting up a trial of GitHub Enterprise Server"
- "Setting up a GitHub Enterprise Server instance"