

01-guacamole.md

kstack: book: Centerpoint Home
Lab chapter: Utilities page: Apache
Guacamole tags: [guacamole,
remote-desktop, rdp, vnc, ssh,
authentik, postgres]

Overview

Apache Guacamole is a clientless remote desktop gateway. It provides browser-based access to RDP, VNC, SSH, and Telnet sessions with no client software required. Authentication is via Authentik OpenID Connect (native Guacamole extension — not Traefik ForwardAuth). The stack is three containers: the web application, the `guacd` native protocol daemon, and PostgreSQL 15 for connection and user data.

Access

Type	URL	Auth
External	<code>https://guac.jeeves5454.ddns.net</code>	Authentik OIDC + GeoBlock + CrowdSec
Internal	<code>https://guac.home.local</code>	Authentik OIDC (Step-CA TLS)

Guacamole uses its built-in `openid` extension with `EXTENSION_PRIORITY=openid` to handle the Authentik OIDC flow directly. Traefik does not apply `authentik-auth@docker` ForwardAuth.

Containers

Container	Image	Role
guacamole	guacamole/guacamole:latest	Web application (Tomcat/Java)
guacd	guacamole/guacd:latest	Native protocol daemon (RDP/VNC/SSH)
guacamole_db	postgres:15-alpine	PostgreSQL database

guacamole (application)

Runtime: Apache Tomcat / Java. WEBAPP_CONTEXT=R00T serves the app at / rather than /guacamole.

Key environment variables:

Variable	Value / Notes
GUACD_HOSTNAME	guacd
POSTGRESQL_HOSTNAME	postgres (internal alias for guacamole_db)
POSTGRESQL_DATABASE	guacamole_db
POSTGRESQL_USER	guacamole_user
POSTGRESQL_PASSWORD	REDACTED
WEBAPP_CONTEXT	R00T
EXTENSION_PRIORITY	openid
OPENID_ISSUER	https://auth.jeevesconsults.ca/application/o/guacamole/
OPENID_CLIENT_ID	A1l7KFyrugknbc8jtFjPxm520XkcNVjGMfTFtJMt
OPENID_CLIENT_SECRET	REDACTED
OPENID_REDIRECT_URI	https://guac.jeeves5454.ddns.net/
OPENID_AUTHORIZATION_ENDPOINT	https://auth.jeevesconsults.ca/application/o/authorize/
OPENID_JWKS_ENDPOINT	https://auth.jeevesconsults.ca/application/o/guacamole/jwks/
OPENID_SCOPE	openid email profile
OPENID_USERNAME_CLAIM_TYPE	preferred_username

No bind mounts — app state is stored in PostgreSQL.

guacd

The native protocol daemon that handles the actual RDP, VNC, SSH, and Telnet protocol sessions. Guacamole app proxies all protocol traffic through guacd.

Bind mounts:

Host Path	Container Path	Purpose
/home/jeeves/docker/guacamole/drive	/drive	Virtual drive for file transfer
/home/jeeves/docker/guacamole/record	/record	Session recordings

guacamole_db (PostgreSQL 15)

Image: postgres:15-alpine

Variable	Value
POSTGRES_DB	guacamole_db
POSTGRES_USER	guacamole_user
POSTGRES_PASSWORD	REDACTED
PGDATA	/var/lib/postgresql/data/guacamole

Bind mounts:

Host Path	Container Path	Purpose
/home/jeeves/docker/guacamole/db-data	/var/lib/postgresql/data	Database files
/home/jeeves/docker/guacamole/init	/docker-entrypoint-initdb.d	Init SQL scripts

Traefik Labels

```
traefik.http.routers.guacamole-external.rule: Host(`guac.jeeves5454.ddns.net`)
traefik.http.routers.guacamole-external.entrypoints: websecure
traefik.http.routers.guacamole-external.tls.certresolver: letsencrypt
traefik.http.routers.guacamole-external.middlewares: plex-geoblock@file,crowdsec-bouncer@file
traefik.http.routers.guacamole-external.service: guac-svc

traefik.http.routers.guacamole-internal.rule: Host(`guac.home.local`)
traefik.http.routers.guacamole-internal.entrypoints: websecure
traefik.http.routers.guacamole-internal.tls.certresolver: step-ca
```

```
traefik.http.routers.guacamole-internal.service: guac-svc
```

```
traefik.http.services.guac-svc.loadbalancer.server.port: 8080
```

```
traefik.docker.network: traefik-net
```

Notes / Gotchas

- `EXTENSION_PRIORITY=openid` means Guacamole's OpenID extension takes precedence over any local user database. If Authentik is down, Guacamole login is unavailable — there is no local admin fallback while OpenID is primary.
- `OPENID_REDIRECT_URI` must exactly match the redirect URI registered in Authentik. It points to the **external** domain (`guac.jeeves5454.ddns.net`) even when accessing internally — Authentik sends the browser there after authentication.
- `WEBAPP_CONTEXT=ROOT` removes the `/guacamole` path prefix. The app responds directly at `/`. Without this, Traefik would need to strip the prefix or all URLs would be `/guacamole/...`.
- Session recordings are stored in the `record` bind mount. Manage disk usage if many long sessions are recorded.
- The `init` bind mount contains the SQL schema initialisation scripts for the database. These run once on first start. Do not remove them if the container has not yet initialised.

Last Updated: 2026-06-17

Revision #2

Created 2026-06-17 04:46:00 UTC by Admin

Updated 2026-06-17 04:46:00 UTC by Admin