ARES
Server Guardian

ARES SUITE

ARES Server Guardian

Changes

Detects attacks on your servers and blocks them at the firewall.

VERSION	PRODUCTION	DATE
1.6.0	guardian.server1.nacino.net	19 November 2026
AUTHOR	DEMO	CLASSIFICATION
Alfredo Nacino	guardian-demo.nacino.net	Internal

Contents

01 Version 1.6.0 (2026-11-19)

02 Version 1.5.1 (2026-11-07)

03 Version 1.5.0 (2026-11-07)

04 Version 1.4.1 (2026-11-07)

05 Version 1.4.0 (2026-11-07)

06 Version 1.3.2 (2026-11-05)

07 Version 1.3.1 (2026-10-14)

08 Version 1.3.0 (2026-10-14)

09 Version 1.2.1 (2026-10-14)

10 Version 1.2.0 (2026-10-14)

11 Version 1.1.4 (2026-10-14)

12 Version 1.1.3 (2026-10-14)

13 Version 1.1.2 (2026-10-14)

14 Version 1.1.1 (2026-10-14)

15 Version 1.1.0 (2026-10-14)

16 Version 1.0.0 (2026-10-14)

All notable changes to ARES Server Guardian. Format: Keep a Changelog, versions: SemVer.

1. Version 1.6.0 (2026-11-19)

1.1 Added

- Agent mode: `[server] web = false` runs every monitor and the ARES Central link without the web app. An agent has no dashboard, API, users or open port, and is managed from ARES Central.
- `deploy/install-agent.sh`: writes an agent configuration (firewall backend detected, the server's own addresses and the installing SSH client whitelisted), joins ARES Central with a one-time code and waits for the link. Options `--read-only`, `--convert` (full install to agent) and `--rejoin`.
- `scripts/install-remote.sh`: installs or upgrades ARES on the servers named on the command line only, as an agent, standalone or behind Apache. With `--central` it creates each new server's join code on ARES Central over SSH.
- `deploy/uninstall.sh`: removes a full install or an agent, its firewall rules and, unless `--keep-data`, its configuration and data.
- `ares-guardian status`: version, mode, service, firewall backend and the ARES Central link.
- `GET /healthz` for health checks, and `PORT`, `HOST` and `DATA_DIR` from the environment.
- ARES Suite packaging: manifest, brand, Demo (preproduction) deployment, documents and presentation.

1.2 Changed

- `scripts/deploy-remote.sh` knows the `agent` mode; an agent counts as healthy when its link to ARES Central is connected.
- ARES Central is told whether a server is an agent or a full install.
- On an agent, `backup restore` checks the service instead of a port.

2. Version 1.5.1 (2026-11-07)

2.1 Added

- Logs page: activity, security events, web attacks, alerts, firewall, AI runs and the application log, as a table, raw lines or JSON, with search, dates, live follow and downloads.
- Each attack opens with all its fields; an address can be traced across every log, with a built-in analysis that uses no AI.
- ARES Central can receive each attack.
- Help: a "How to use ARES" section, linked from About.

2.2 Changed

- AI analysis runs through Claude Code on a Claude plan. The Anthropic API option is removed, and ARES stores no Claude credential.

3. Version 1.5.0 (2026-11-07)

3.1 Added

- Log retention of 1, 2, 3 or 6 months, set under Settings.
- Backups, scheduled or on demand, restored from the console.
- AI analysis: risk score, findings and charts, with cost analysis per query and scheduled email reports with a PDF.
- Attack rates by type per second, minute and hour in reports.
- More web application firewall signatures.

4. Version 1.4.1 (2026-11-07)

4.1 Fixed

- Web logins: a 200 response is no longer counted as a failed login.

5. Version 1.4.0 (2026-11-07)

5.1 Added

- Web application firewall: classifies requests from the access logs, shows the attacked applications per site, and adds blocking rules per site and path.
- Anti-DDoS rate-limit presets; HTTP and connection floods also add a temporary rate limit.
- Permanent ban for an address banned 3 times.
- Brute-force guard: one failed login limits that address on the web ports and the port it failed on.
- Allowed and denied DNS names for dynamic addresses, re-resolved every 5 minutes.
- Log forwarding as JSON over HTTPS, HTTP, TLS, TCP or UDP.

6. Version 1.3.2 (2026-11-05)

6.1 Added

- Help and About buttons in the top bar, help on the sign-in page, and `scripts/new-server.sh`.

7. Version 1.3.1 (2026-10-14)

7.1 Fixed

- `deploy-apache.sh` counts ARES's allowed-address refusal as a working site.

8. Version 1.3.0 (2026-10-14)

8.1 Added

- Link to ARES Central over mutual TLS 1.3: the server reports health, alerts, attackers and firewall rules, and runs Ed25519-signed firewall commands.
- Console commands `central join`, `central status` and `central leave`; `[central]` settings in `ares.toml`.
- The `ares-guardian` console command.

9. Version 1.2.1 (2026-10-14)

9.1 Fixed

- Apache `vhost_combined` access logs are parsed.

10. Version 1.2.0 (2026-10-14)

10.1 Added

- Standalone HTTPS deployment for servers without a usable web server.

11. Version 1.1.4 (2026-10-14)

11.1 Fixed

- `install.sh` installs `python3-venv` when it is missing and rebuilds a broken virtual environment.

12. Version 1.1.3 (2026-10-14)

12.1 Changed

- Installs under the `ares-guardian` paths; the command line uses the live configuration.

13. Version 1.1.2 (2026-10-14)

13.1 Fixed

- `install.sh` no longer asks for an admin when there is no terminal.

14. Version 1.1.1 (2026-10-14)

14.1 Added

- In-app help, About, the user guide and Apache deployment.

15. Version 1.1.0 (2026-10-14)

15.1 Added

- Allowed-address restriction for the web app, with DNS names re-resolved on a schedule.
- Emailed one-time remote access links that open only the user's own account.
- SMTP settings with a test email.

16. Version 1.0.0 (2026-10-14)

16.1 Added

- First release: detection of SSH and web login brute force, HTTP floods, web scans, port scans, connection and SYN floods; automatic bans through nftables, iptables or ufw; health monitoring; alerts and reports; users with mandatory 2FA; web dashboard and REST API.