

Argus

Zählt die Angriffe auf Ihre Server und bewahrt den Verlauf als Diagramme auf, ohne Dauerdienst und ohne Datenbank

Handbuch

Version	1.0.0-14
Commit	`9622e76`
Commit-Datum	3. November 2026
Lizenz	MIT

Offline-Handbuch, identisch mit den Anleitungen des Repositorys in der angegebenen Version und beim angegebenen Commit. Maßgeblich ist der Text des Repositorys.

Inhaltsverzeichnis

Überblick **1**
- Installation in zwei Schritten . . . 1
- Die drei Ansichten . . . 1
- Eine Verbindung pro Host, kein erneuter Versuch . . . 2
- Konfiguration . . . 2
- Prüfen, ob es funktioniert . . . 2
- Dokumentation . . . 2
- Credits . . . 3
- Lizenz . . . 3

Argus auf dem Server installieren **4**
- Was Sie erhalten . . . 4
- Voraussetzungen . . . 4
- Installation . . . 4
- Jetzt ausprobieren . . . 4
- Eine Einstellung ändern . . . 5
- Entfernen . . . 5

Die Diagramme auf den Arbeitsplatzrechner holen und lesen **6**
- Was Sie erhalten . . . 6
- Voraussetzungen . . . 6
- Die Server deklarieren . . . 6
- Kopieren . . . 6
- Eine Verbindung, kein erneuter Versuch . . . 7
- Die Diagramme lesen . . . 7

Diagramme: Zeitfenster, Aufteilung, Stunde, Serien **8**
- Zeitfenster . . . 8
- Ein langes Zeitfenster aufteilen . . . 8
- Die Stunde des Tages . . . 8
- Serien . . . 9
- Die Zahlen statt des Bildes lesen . . . 9
- Zeitscheiben um 00 Uhr (`T00`) . . . 9
- Diagrammsprache . . . 9

Fehlerbehebung **10**
- Die Prüfung ausführen . . . 10
- Was jede Zeile bedeutet . . . 10
- Einen Sammler von Hand ausführen . . . 10
- Häufige Ursachen . . . 10

Überblick

Kein Dauerdienst, keine Datenbank, geeignet für Maschinen mit weniger als 1 GB RAM.

Argus zählt die Angriffe gegen Ihre Server, SSH von selbst und, wenn sie installiert sind, die Sperren von Fail2Ban und CrowdSec, und bewahrt den Verlauf als Diagramme auf. Ein Cron-Job läuft jede Nacht, schreibt reine Textdateien und zeichnet die Diagramme. Zwischen zwei Nächten läuft nichts.

Argus speichert oder zeigt nie die IP-Adresse eines Angreifers, nur Anzahlen pro Stunde und pro Tag. Ein **Angriff** ist eine Quell-IP, die innerhalb eines Tages eine Mindestzahl fehlgeschlagener Authentifizierungsversuche erreicht (standardmäßig 5), damit ein falsch getipptes Passwort nicht zählt.

Grafana ist eine kontinuierliche Ansicht einer Infrastruktur: ein Dienst, der ständig läuft und live abgefragt werden kann. Argus ist eine periodische Momentaufnahme Ihrer Sicherheitshistorie: ein Bild pro Nacht, gelesen, wann Sie wollen. Grafana kann auch nach Woche oder Jahr aggregieren, zum Preis eines Dauerdienstes, einer Zeitreihendatenbank und eines zu bauenden Dashboards; Argus hat keines der drei, weshalb es auf einen Server mit 1 GB passt.

Installation in zwei Schritten

Wenn Sie ein Programm normalerweise auf dem Computer installieren, an dem Sie arbeiten, ist es hier umgekehrt. Das Paket kommt auf den **Server**, die angegriffene Maschine. Ihr eigener Computer, der Arbeitsplatzrechner, installiert nichts aus dem Paket und empfängt nur die Bilder.

1. **Auf dem Server** (der angegriffenen Maschine) installieren Sie das Paket. Es zählt die Angriffe und zeichnet jede Nacht die Diagramme. Danach ist nichts zu starten.
2. **Auf Ihrem Arbeitsplatzrechner** (dem Computer, an dem Sie lesen) führen Sie `argus-fetch` aus. Es kopiert die Diagrammbilder von Ihren Servern auf Ihren Computer.

Wo jeder Teil liegt:

```
server.example.org (the server)          your desk
─────────────────────────────────        ──────────────────────────────
/opt/argus/        scripts               ~/.config/argus/hosts.conf
/etc/argus/        argus.conf                the list of your servers
/srv/argus/<year>/ data and images       ~/argus-backup/<server>/<year>/images/
/usr/bin/argus-chart                         the copied charts
/usr/bin/argus-fetch   ── copies images ──►
```

Schritt 1, auf dem Server (Debian oder Ubuntu):

```
sudo apt install ./argus_1.0.0-14_all.deb
```

Schritt 2, auf Ihrem Arbeitsplatzrechner. Tragen Sie Ihre Server in die Datei `~/.config/argus/hosts.conf` ein, einen pro Zeile, in der Form `<ssh alias>,<data directory>`, und führen Sie dann `argus-fetch` aus:

```
mkdir -p ~/.config/argus
printf 'server.example.org,/srv/argus/\n' > ~/.config/argus/hosts.conf
argus-fetch
```

`argus-fetch` wird vom selben Paket installiert. Auf einem Rechner, der keine Debian-Maschine ist, kopieren Sie das einzelne Skript `argus-fetch` aus diesem Repository; es braucht nur `bash`, `ssh` und `rsync`. Einzelheiten: `docs/install.md` und `docs/desk.md`.

Die drei Ansichten

`argus-chart` zeichnet ein Diagramm für das Zeitfenster, das Sie wählen. Führen Sie es auf dem Server aus. Jeder Befehl schreibt ein PNG in `/srv/argus/<year>/images/` (mit `--out DIR` schreiben Sie woandershin, was ein gewöhnlicher Benutzer braucht).

- `argus-chart daily` ist der Verlauf des Jahres, ein Punkt pro Tag.
- `argus-chart period` ist die Anzahl jeder Serie über ein Zeitfenster.
- `argus-chart hourly` ist die Anzahl pro Stunde des Tages über ein Zeitfenster, von 00 bis 23.

Zehn Zeitfenster zum Kopieren:

```
argus-chart period --day 2026-10-30                     # one day, one point per hour
argus-chart period --week 2026-W44                      # ISO week, Monday to Sunday
argus-chart period --month 2026-10                      # one calendar month
argus-chart period --quarter 2026-Q4                    # one quarter
argus-chart period --year 2025                          # one year
argus-chart period --from 2025-12-01 --to 2026-01-31    # a range over two years
argus-chart period --month 2026-10 --split week         # one PNG per week of the month
argus-chart period --week 2026-W44 --series ssh_direct  # one series only
argus-chart hourly --week 2026-W44                      # which hours are attacked
argus-chart hourly --month 2026-10 --series ssh_direct,ip_ban_sshd
```

Die Serien werden nebeneinander gezeichnet, nie addiert: SSH, jedes Fail2Ban-Jail und jedes CrowdSec-Szenario behalten ihre eigene Linie und Farbe. Einzelheiten: `docs/charts.md`.

Eine Verbindung pro Host, kein erneuter Versuch

`argus-fetch` öffnet **eine Verbindung pro Host** und **versucht nie erneut**. Viele Server sperren eine Adresse nach einigen fehlgeschlagenen Anmeldungen, sodass ein zweiter Versuch Sie aussperren könnte. Ein Host, der nicht antwortet, wird einmal gemeldet, die anderen Hosts werden trotzdem kopiert, und der Exit-Code ist 1. Beheben Sie die Ursache (Schlüssel, Alias, Firewall, ausgeschaltete Maschine), und führen Sie den Befehl dann von Hand erneut aus.

Konfiguration

Alles funktioniert mit den Standardwerten. Um einen zu ändern, bearbeiten Sie `/etc/argus/argus.conf` auf dem Server; die Datei wird von jedem Skript gelesen und enthält jeden Wert auskommentiert:

```
# /etc/argus/argus.conf
ARGUS_SSH_THRESHOLD=5          # failed attempts of one IP in one day that make an attack
ARGUS_LANG=en                  # chart language: en, fr, de or es
ARGUS_DATA_DIR="/srv/argus"    # where the data and the images are written
```

Die anderen Variablen (Protokollpfade, Bildgröße, Serienfarben) sind in `man argus` aufgeführt.

Prüfen, ob es funktioniert

```
sudo /opt/argus/argus-doctor.sh
```

Es sagt, ob jede Quelle (SSH, Fail2Ban, CrowdSec) gestern gesammelt wurde. Siehe `docs/troubleshooting.md`.

Dokumentation

- `docs/install.md`: Installation auf dem Server, Aufbau, Deinstallation
- `docs/desk.md`: die Diagramme auf den Arbeitsplatzrechner holen und lesen
- `docs/charts.md`: Zeitfenster, Aufteilung, Stunde, Serien, Zeitzone, `T00`-Zeitscheiben
- `docs/troubleshooting.md`: was `argus-doctor.sh` sagt und was zu tun ist
- Handbuchseiten: `man argus`, `man argus-chart`, `man argus-fetch` (Quellen in `man/en/`)

Credits

Argus ist das Ergebnis einer Zusammenarbeit zwischen einem Menschen und mehreren Sprachmodellen, wobei die Rollen so festgehalten sind, wie sie tatsächlich gespielt wurden. Die vollständige Liste steht in `CONTRIBUTORS.md`.

- **Ronan Davalan** – Architekt und Schiedsrichter: ursprüngliche Skripte (2024), Entscheidungen, Validierung und Tests.
- **Claude Code (Anthropic)** – Leitender Entwickler: Sammler, Diagrammrendering, `argus-doctor.sh`, Debian-Paket, Dokumentation.
- **Gemini (Google)** – Synthesizer und strategischer Co-Autor: Planung und Rahmung des Projektzwecks.
- **Gemini (Google), GLM-5.3-Flash Free und Gemini 4 Argon** – Grafiker: visuelle Identität des Projekts (Marke, Icon, Favicon), von Ronan Davalan am 2026-11-02 übernommen.
- **DeepSeek** – Begleiter im Feld: CrowdSec-Einrichtung auf einem echten Server, der zur Validierung von `collect-crowdsec.sh` diente.
- **DeepSeek Flash** – Inhalt der Website auf Englisch, danach die französische, deutsche und spanische Übersetzung der Dokumentation, der Handbuchseiten und der Website.
- **Muse Spark 1.3 Contributor** – Gestaltung der Website: Einbindung des Logos, des Favicons und des Diagrammbilds.
- **gd2:** Ronan Davalans verstorbener Bruder. Er brachte Ronan Git und dessen Gebrauch bei, beriet bei diesem Projekt und nahm die erste externe Änderung an dessen README vor (2024-08-07).

Lizenz

MIT – siehe `LICENSE`.

Argus auf dem Server installieren

Das Paket kommt auf den **Server**, die Maschine, deren Protokolle Argus liest. Sie installieren es nicht auf Ihrem Arbeitsplatzrechner: Der Arbeitsplatzrechner kopiert nur die Diagramme (siehe `desk.md`).

Was Sie erhalten

```
/opt/argus/
├── collect-ssh.sh         SSH attacks, from auth.log or journald
├── collect-fail2ban.sh    Fail2Ban bans, one series per jail (optional)
├── collect-crowdsec.sh    CrowdSec alerts, one series per scenario (optional)
├── chart-daily.sh         history of the year, one point per day
├── chart-period.sh        count over a window (day, week, month, quarter, year, range)
├── chart-hourly.sh        count per hour of the day over a window
├── chart-*.gp             the gnuplot drawing of each view
├── argus-lib.sh           code shared by the chart scripts
└── argus-doctor.sh        health check of the collection

/usr/bin/argus-chart       one command for the three views
/usr/bin/argus-fetch       copies the charts to a desk
/etc/argus/argus.conf      optional settings, every line commented out
/etc/cron.d/argus          the nightly jobs
/srv/argus/                data and charts, readable by everyone
└── 2026/
    ├── ssh_direct_2026.txt      one line per hour with an attack
    ├── ip_ban_sshd_2026.txt     one file per Fail2Ban jail, if present
    ├── .daily/                  daily totals, rebuilt by chart-daily.sh
    ├── .heartbeat/              daily proof that each collector ran
    └── images/                  the PNG charts
```

`/srv/argus/` enthält nur Anzahlen, nie eine IP-Adresse, ist also für jeden Benutzer lesbar: Sie kopieren die Diagramme ohne `sudo`.

Voraussetzungen

Ein Debian- oder Ubuntu-Server mit Cron. Das Paket hängt von `gawk` und `gnuplot-nox` ab; `apt` installiert sie. `rsync` und `openssh-client` werden empfohlen (sie dienen `argus-fetch`). Fail2Ban, CrowdSec und `jq` sind optional. Ein Server mit 1 GB RAM genügt: Nichts bleibt laufen.

Installation

Laden Sie `argus_1.0.0-14_all.deb` von der Release-Seite des Repositorys herunter und führen Sie dann auf dem Server aus:

```
sudo apt install ./argus_1.0.0-14_all.deb
```

Die Cron-Jobs beginnen in dieser Nacht: Sammlung um 00:05, Diagramme um 00:15, Gesundheitsprüfung um 00:20. Das erste Diagramm erscheint nach der ersten Nacht in `/srv/argus/2026/images/`.

Jetzt ausprobieren

Um die erste Nacht zu überspringen, führen Sie die Schritte von Hand auf einem Server aus, der bereits einen Protokollverlauf hat:

```
sudo /opt/argus/collect-ssh.sh
sudo /opt/argus/chart-daily.sh
ls /srv/argus/2026/images/
```

Zeichnen Sie dann eine Ansicht:

```
sudo argus-chart period --month 2026-10
```

Eine Einstellung ändern

`/etc/argus/argus.conf` ist eine Shell-Datei, die von jedem Skript gelesen wird. Entfernen Sie die Kommentarzeichen nur bei dem, was Sie brauchen:

```
# /etc/argus/argus.conf
ARGUS_SSH_THRESHOLD=10         # failed attempts of one IP in one day that make an attack
ARGUS_LANG=en                  # chart language: en, fr, de or es
ARGUS_IMG_WIDTH=3840           # image size in pixels
ARGUS_IMG_HEIGHT=2160
ARGUS_COULEUR_ssh_direct=orange   # colour of one series, any gnuplot colour name
```

Variablennamen verwenden Großbuchstaben und Unterstriche, nie Bindestriche. Die Serie `caddy-xmlrpc` wird daher durch `ARGUS_COULEUR_caddy_xmlrpc` gefärbt. Alle Variablen sind in `man argus` aufgeführt.

Entfernen

```
sudo apt remove argus     # removes the scripts, keeps /srv/argus and /etc/argus
sudo apt purge argus      # also removes /srv/argus and /etc/argus
```

Purge löscht auch Ihren Verlauf. Kopieren Sie ihn zuerst mit `argus-fetch` (siehe `desk.md`).

Die Diagramme auf den Arbeitsplatzrechner holen und lesen

Argus läuft auf Ihren Servern und zeichnet die Diagramme dort. `argus-fetch` kopiert die Bilder auf den Computer, an dem Sie arbeiten. Vom Server wird nichts gesendet: Sie holen die Bilder, wann Sie wollen.

Was Sie erhalten

```
~/.config/argus/hosts.conf             the servers to copy, one per line
~/argus-backup/
└── server.example.org/                one folder per ssh alias
    └── 2026/
        └── images/
            ├── 2026-11-02_argus_4k.png
            └── 2026-11-02_argus_period_week-2026-W44.png
```

Voraussetzungen

`bash`, `ssh` und `rsync` auf dem Arbeitsplatzrechner. Das Paket installiert `argus-fetch` in `/usr/bin`; auf einem anderen System kopieren Sie die eine Datei `argus-fetch` aus dem Repository in einen Ordner Ihres `PATH`. Ihr `ssh` muss sich bereits mit einem Schlüssel beim Server anmelden, ohne Passwortabfrage: `argus-fetch` fragt nie danach.

Die Server deklarieren

Ein Server pro Zeile, `<ssh alias>,<data directory>`. Der Alias ist ein `Host`-Name aus `~/.ssh/config` (oder `user@host`); das Verzeichnis ist `ARGUS_DATA_DIR` auf diesem Server, standardmäßig `/srv/argus/`.

```
mkdir -p ~/.config/argus
printf 'server.example.org,/srv/argus/\nbackup.example.org,/srv/argus/\n' > ~/.config/argus/hosts.conf
cat ~/.config/argus/hosts.conf
```

Leere Zeilen und Zeilen, die mit `#` beginnen, werden ignoriert. Das Repository liefert `hosts.conf.example`.

Kopieren

```
argus-fetch
```

Für jeden Server öffnet es **eine** Verbindung, kopiert die PNG-Dateien aus `<directory>/<year>/images/` und schließt sie. Eine Datei, die bereits auf Ihrem Arbeitsplatzrechner liegt, wird nie überschrieben, und nichts wird gelöscht. Führen Sie es so oft aus, wie Sie wollen: Nur neue Bilder werden kopiert.

Um nur einen Server zu kopieren oder die Kopien anderswo abzulegen:

```
argus-fetch --only server.example.org
argus-fetch --dest ~/Documents/argus
```

Eine Verbindung, kein erneuter Versuch

Wenn ein Server nicht antwortet, meldet `argus-fetch` dies einmal auf der Fehlerausgabe, fährt mit den anderen Servern fort und endet mit dem Exit-Code 1. Es versucht nie erneut, weil viele Server eine Adresse nach einigen fehlgeschlagenen Anmeldungen sperren. Finden Sie die Ursache (Schlüssel, Alias, Firewall, ausgeschalteter Server), und führen Sie den Befehl dann selbst erneut aus.

Die Diagramme lesen

Öffnen Sie die Bilder mit einem beliebigen Betrachter:

```
xdg-open ~/argus-backup/server.example.org/2026/images/
```

Ein Diagramm zeigt eine Linie pro Serie. Bei einem Zeitfenster von höchstens 31 Punkten wird die genaue Anzahl an jedem Punkt geschrieben. Eine Ansicht, die es noch nicht gibt (eine andere Woche, ein Monat pro Stunde), wird auf dem Server gezeichnet, als root, damit das Bild im Bilderordner landet:

```
ssh server.example.org
sudo argus-chart period --week 2026-W44
```

Das nächste `argus-fetch` kopiert das neue Bild mit den anderen. Siehe `charts.md` für die Zeitfenster, die Sie anfordern können.

Diagramme: Zeitfenster, Aufteilung, Stunde, Serien

`argus-chart` hat drei Ansichten. Führen Sie es auf dem Server aus, als root, um in `/srv/argus/<year>/images/` zu schreiben, oder als gewöhnlicher Benutzer mit `--out DIR`.

```
argus-chart daily  [YEAR]              one point per day, the whole year
argus-chart period [window] [options]  one line per series over a window
argus-chart hourly [window] [options]  24 positions, 00 to 23, per series
```

Jede Datei heißt `<today>_argus_<view>_<window>.png`, zum Beispiel `2026-11-02_argus_period_week-2026-W44.png`.

Zeitfenster

`period` und `hourly` nehmen dieselben Zeitfenster. Ohne eines verwenden sie das laufende Jahr.

Option	Zeitfenster	Beispiel
`--day YYYY-MM-DD`	ein Tag	`--day 2026-10-30`
`--week YYYY-Www`	ISO-Woche, Montag bis Sonntag	`--week 2026-W44`
`--month YYYY-MM`	Kalendermonat	`--month 2026-10`
`--quarter YYYY-Qn`	Quartal, `n` von 1 bis 4	`--quarter 2026-Q4`
`--year YYYY`	Kalenderjahr	`--year 2025`
`--from D --to D`	Zeitraum, beide Tage eingeschlossen	`--from 2025-12-01 --to 2026-01-31`

Wochen folgen ISO 8601: Woche 1 des Jahres 2027 beginnt am Montag, 2027-01-04, und 2026 hat eine Woche 53. Ein Zeitfenster, das zwei Jahre umfasst, liest die Daten beider.

```
argus-chart period --day 2026-10-30 --out ~/argus-out
argus-chart period --from 2025-12-01 --to 2026-01-31 --out ~/argus-out
```

Ein langes Zeitfenster aufteilen

`--split` zeichnet ein Diagramm pro Unterzeitraum statt eines einzigen langen Diagramms:

```
argus-chart period --month 2026-10 --split week --out ~/argus-out
argus-chart period --year 2026 --split month --out ~/argus-out
```

`--split week` eignet sich für einen Monat oder ein Quartal, `--split month` für ein Quartal oder ein Jahr. Der erste Befehl schreibt eine Datei pro ISO-Woche, die Oktober berührt, jede auf das Zeitfenster zugeschnitten, benannt `…_month-2026-10_week-2026-W41.png`.

Die Stunde des Tages

`hourly` addiert für jede Serie die Angriffe, die zu jeder Stunde im Zeitfenster gesehen wurden, und zeichnet 24 Positionen. Es zeigt, zu welchen Stunden des Tages Sie angegriffen werden, nicht an welchen Tagen.

```
argus-chart hourly --week 2026-W44 --out ~/argus-out
```

Die Stunde ist die **lokale Serverzeit**, wie die Sammler sie schreiben. Es ist die Stunde, zu der der Angriff in den Protokollen gesehen wurde, nicht die Stunde seines Beginns. Der Titel sagt „local server

time“. Eine Zeitumstellung fügt an einem Tag eine Stunde hinzu oder entfernt sie; über eine Woche oder mehr zeigt sich der Effekt nicht.

Serien

Eine Serie ist eine Linie: `ssh_direct` für SSH, `ip_ban_<jail>` für jedes Fail2Ban-Jail, `ip_ban_<scenario>` für jedes CrowdSec-Szenario. Der Name ist der Dateiname ohne das Jahr, also ist `ssh_direct_2026.txt` die Serie `ssh_direct`.

Die Serien werden übereinandergelegt, nie addiert: Argus erfindet keine Punktzahl aus verschiedenen Werkzeugen. Jede Serie behält dieselbe Farbe von Jahr zu Jahr (legen Sie sie mit `ARGUS_COULEUR_<series>` fest, sonst stammt sie aus einem Hash des Namens).

```
argus-chart period --week 2026-W44 --list-series
argus-chart period --week 2026-W44 --series ssh_direct
argus-chart hourly --month 2026-10 --series ssh_direct,ip_ban_sshd --out ~/argus-out
```

Ein unbekannter Name in `--series` stoppt den Befehl mit dem Exit-Code 2 und listet die verfügbaren Namen auf.

Die Zahlen statt des Bildes lesen

`--print-data` gibt die Tabelle hinter dem Diagramm auf der Standardausgabe aus (tabgetrennt, Kopfzeile beginnend mit `#`) und zeichnet nichts:

```
argus-chart period --week 2026-W44 --print-data
argus-chart hourly --day 2026-10-30 --print-data
```

Zeitscheiben um 00 Uhr (`T00`)

Eine Datenzeile ist `<count> <date>T<hour>`, zum Beispiel `492 2026-10-30T14`. Dateien von vor der stündlichen Sammlung enthalten eine Zeile pro Tag, alle als `T00` geschrieben. Eine Serie, die nur aus `T00`-Zeitscheiben besteht, hat keine Stundeninformation, daher lässt `hourly` sie aus, statt einen Balken um Mitternacht zu zeichnen. Es gibt die Meldung `series 'legacy' excluded: all its slices are at hour 00 (daily data, no hourly depth)` auf der Fehlerausgabe aus und schreibt `excluded series: no hourly data: legacy` in den Titel des Diagramms. `period` und `daily` zeichnen sie weiterhin als Tagespunkte.

Diagrammsprache

`ARGUS_LANG` legt die Titel und die Achsen fest: `en` (Standard), `fr`, `de` oder `es`.

```
ARGUS_LANG=de argus-chart period --week 2026-W44 --out ~/argus-out
```

Fehlerbehebung

Ein Diagramm ohne Angriff kann einen ruhigen Tag oder einen Sammler bedeuten, der angehalten wurde. Die Datendateien können beide nicht unterscheiden, weil ein Tag ohne Angriff keine Zeile schreibt. `argus-doctor.sh` kann es: Jeder Sammler schreibt eine Zeile pro Tag in `/srv/argus/<year>/.heartbeat/<source>.txt`, `<date> <number of events>`, auch wenn die Zahl 0 ist.

Die Prüfung ausführen

```
sudo /opt/argus/argus-doctor.sh
```

Der Cron-Job führt sie jede Nacht um 00:20 aus und hängt die Ausgabe an `/var/log/argus.log` an. Der Exit-Code ist 0, wenn nichts zu melden ist, sonst 1. Ein gesunder Server gibt aus:

```
== Source availability ==

== Heartbeats (2026) ==
  ssh : ok
    -> up to date, yesterday: 12 event(s)
  fail2ban : absent
  crowdsec : absent

Nothing to report.
```

Was jede Zeile bedeutet

`<source> : ok` oder `absent` sagt, ob die Quelle jetzt gelesen werden kann: `auth.log` oder `journald` für `ssh`, `fail2ban-client` und sein Protokoll für `fail2ban`, `cscli` und `jq` für `crowdsec`. `absent` für Fail2Ban oder CrowdSec ist normal, wenn Sie sie nicht betreiben.

Zeile unter der Quelle	Bedeutung	Was zu tun ist
`up to date, yesterday: N event(s)`	gestern gesammelt, N Ereignisse (0 ist ein ruhiger Tag)	nichts
`last confirmed on DATE (no entry for yesterday)`	der Sammler lief nicht oder scheiterte seit DATE	sehen Sie in `/var/log/argus.log` nach, führen Sie den Sammler von Hand aus
`never collected`	keine Lebenszeichen-Datei, obwohl die Quelle lesbar ist	führen Sie den Sammler von Hand aus, prüfen Sie `/etc/cron.d/argus`

Zeilen, die eine Aktion erfordern, werden unter `TO CHECK` auf der Fehlerausgabe wiederholt.

Einen Sammler von Hand ausführen

```
sudo /opt/argus/collect-ssh.sh
sudo /opt/argus/argus-doctor.sh
tail -n 20 /var/log/argus.log
```

Häufige Ursachen

- **Kein Bild nach der ersten Nacht.** Prüfen Sie, ob `/etc/cron.d/argus` existiert und Cron läuft (`systemctl status cron`). Führen Sie `sudo /opt/argus/chart-daily.sh` aus und lesen Sie seine Meldung.

- **`chart-daily.sh: no data file for 2026 in /srv/argus/2026 — nothing to plot.`** Kein Sammler hat in diesem Jahr eine Datei geschrieben. Ein Server ohne jeden Angriff schreibt keine. Führen Sie `sudo /opt/argus/collect-ssh.sh` aus, um gestern zu sammeln.
- **SSH zeigt jeden Tag 0 Ereignisse.** `auth.log` fehlt und `journald` enthält die Protokolle unter einem anderen Unit-Namen. Setzen Sie `ARGUS_SSHD_UNIT="sshd"` in `/etc/argus/argus.conf` (der Standard ist `ssh`).
- **Weniger SSH-Angriffe als Fail2Ban-Sperren.** Argus zählt eine IP erst nach `ARGUS_SSH_THRESHOLD` fehlgeschlagenen Versuchen an einem Tag (standardmäßig 5), und Fail2Ban kann früher sperren. Senken Sie den Schwellenwert zum Vergleichen.
- **`argus-chart: unknown view.`** Die Ansichten sind `period`, `hourly` und `daily`.
- **`unknown series.`** Listen Sie die Namen mit `argus-chart period --list-series` auf.
- **`argus-fetch` meldet einen Host.** Der Server antwortete beim ersten Versuch nicht, und `argus-fetch` versucht nicht erneut. Prüfen Sie Alias, Schlüssel und Firewall, und führen Sie es dann erneut aus. Siehe `desk.md`.
- **Zugriff verweigert beim Schreiben eines Bildes.** `/srv/argus` gehört root: Verwenden Sie `sudo` oder `--out DIR` in Ihrem Home-Verzeichnis.