acl-log

- Examples

The command shows a list of recent ACL security events:

1. Failures to authenticate their connections with `AUTH` or `HELLO`.
2. Commands denied because against the current ACL rules.
3. Commands denied because accessing keys not allowed in the current ACL rules.
4. Commands denied because accessing Pub/Sub channels not allowed in the current ACL rules.
5. Commands denied because accessing a database not allowed in the current ACL rules.
6. TLS clients failing automatic authentication via certificate field because no matching user exists.

The optional argument specifies how many entries to show. By default up to ten failures are returned. The special `RESET` argument clears the log. Entries are displayed starting from the most recent.

Examples

```
127.0.0.1:6379> AUTH someuser wrongpassword
(error) WRONGPASS invalid username-password pair
> ACL LOG 1
1)  1) "count"
    2) (integer) 1
    3) "reason"
    4) "auth"
    5) "context"
    6) "toplevel"
    7) "object"
    8) "AUTH"
    9) "username"
   10) "someuser"
   11) "age-seconds"
```

```
   12) "8.038"
   13) "client-info"
   14) "id=3 addr=127.0.0.1:57275 laddr=127.0.0.1:6379 fd=8 name= age=16 idle=0 flags=N db=0
sub=0 psub=0 ssub=0 multi=-1 qbuf=48 qbuf-free=16842 argv-mem=25 multi-mem=0 rbs=1024 rbp=0
obl=0 oll=0 omem=0 tot-mem=18737 events=r cmd=auth user=default redir=-1 resp=2"
   15) "entry-id"
   16) (integer) 0
   17) "timestamp-created"
   18) (integer) 1675361492408
   19) "timestamp-last-updated"
   20) (integer) 1675361492408
```

Each log entry is composed of the following fields:

1. `count`: The number of security events detected within a 60 second period that are represented by this entry.
2. `reason`: The reason that the security events were logged. One of the following:
   - `command`: the user has no permission to run the command.
   - `key`: the user has no permission to access one of the keys used by the command.
   - `channel`: the user has no permission to access one of the Pub/Sub channels used by the command.
   - `database`: the user has no permission to access one of the databases referenced by the command.
   - `auth`: authentication failed for the connection.
   - `tls-cert`: automatic authentication from a TLS certificate failed because no matching user exists.
3. `context`: The context that the security events were detected in. Either `toplevel`, `multi`, `lua`, `script`, or `module`.
4. `object`: The resource that the user had insufficient permissions to access. The value depends on `reason`:
   - `command`: the command name.
   - `key`: the key pattern.
   - `channel`: the Pub/Sub channel.
   - `database`: the database id, or the command name when the command implicitly accesses every database (such as `FLUSHALL`).
   - `auth`: the literal string `AUTH`.
   - `tls-cert`: the certificate that did not match any existing user.
5. `username`: The username that executed the command that caused the security events or the username that had a failed authentication attempt.
6. `age-seconds`: Age of the log entry in seconds.
7. `client-info`: Displays the client info of a client which caused one of the security events.
8. `entry-id`: The sequence number of the entry (starting at 0) since the server process started. Can also be used to check if items were “lost”, if they fell between periods.
9. `timestamp-created`: A UNIX timestamp in `milliseconds` at the time the entry was first created.

10. `timestamp-last-updated`: A UNIX timestamp in `milliseconds` at the time the entry was last updated.

□□□ #1
□ □□□ □□□ 2026-10-31 15:09:25 UTC
□ □□□ □□□ 2026-10-31 15:09:25 UTC