Common error codes

- TCP connection failed
  - Cause
  - Solution
- HTTP timeout occurred
  - Cause
  - Solution
- Response code mismatch error
  - Cause
  - Solution
  - Alternate cause
  - Solution
- Response body mismatch error
  - Cause
  - Solution
- TLS untrusted certificate error
  - Cause
  - Solution
- TLS name mismatch error
  - Cause
  - Solution
- TLS protocol error
  - Cause
  - Solution
- TLS unrecognized name error
  - Cause
  - Solution
- No route to host error
  - Cause

    - Solution
- Exceeded quota error
    - Cause
    - Solution
- TCP Timeout
    - Cause
    - Solution
- TLS Handshake Failure
    - Cause
    - Solution
- Network Unreachable
    - Cause
    - Solution
- HTTP Invalid Response
    - Cause
    - Solution
- DNS Unknown Host
    - Cause
    - Solution
- Connection Reset by Peer
    - Cause
    - Solution
- Monitor Config Error
    - Cause
    - Solution
- DNS Internal
    - Cause
    - Solution
- Load Balancing Not Enabled
    - Cause
    - Solution
- Validation failed error
    - Cause
    - Solution

- Object referenced by other objects
  - Cause
  - Solution
- Other Failure
  - Cause
  - Solution

The Cloudflare Load Balancing API adds global health to each pool and endpoint. It also gives you a view into what our network sees at a wider level. Cloudflare uses a quorum system to determine pool and endpoint health status. The quorum is taken from PoPs responsible for running health monitor requests in a region, and the majority result is used.

When troubleshooting failures, use the Cloudflare API for programmatic access to Cloudflare Load Balancing. The Health Monitor Events and Load Balancer Monitors routes are excellent tools for accessing load balancing event logs and reconfiguring Cloudflare monitors.

You can get a per-data center breakdown of the health of your endpoints from the Cloudflare API from the List Health Monitor Events command:

```
GET user/load_balancing_analytics/events
```

If a health monitor request fails, the breakdown will include the reason.

Common troubleshooting causes and solutions are listed below.

TCP connection failed

Cause

Our health monitor requests failed to establish a TCP connection to your endpoint.

Solution

This typically occurs when there is a network failure between Cloudflare and your endpoint, and/or a firewall refused to allow our connection. Ensure your network and firewall configurations are not interfering with load balancing traffic.

HTTP timeout occurred

Cause

The endpoint failed to return an HTTP response within the timeout configured. This happens if you have the timeout set to a low number — 1 or 2 seconds, for instance.

Solution

We recommend increasing the HTTP response timeout to allow the endpoint to respond.

Response code mismatch error

Cause

Cloudflare receives an HTTP status code that does not match the values defined in the `expected_codes` property of your Cloudflare monitor configuration.

Solution

Response codes must match the `expected_codes`. Use the List Monitors API command to confirm the values are correct.

Alternate cause

You may also see this issue if you have a monitor configured to use HTTP connections and your endpoint is redirecting to HTTPS. In this case, the response code will often be 301, 302, or 303.

Solution

Either change your Cloudflare monitor configuration to use HTTPS, or set the value of `follow_redirect` to `true` so that we can resolve the correct status code.

Response body mismatch error

Cause

The response body returns from your endpoint and does not include the (case-insensitive) value of `expected_body` configured in your monitor.

Note that we only read the first 10 KB of the response. If you return a larger response, and the expected_body is not in the first 10 KB, the health monitor request will fail.

Solution

Ensure the expected_body is in the first 10 KB of the response body.

TLS untrusted certificate error

Cause

The certificate is not trusted by a public Certificate Authority (CA).

Solution

If you're using a self-signed certificate, we recommend either using a publicly trusted certificate or setting the `allow_insecure` property on your monitor to `true`.

TLS name mismatch error

Cause

Our health monitor (client) was not able to match a name on the server certificate to the hostname of the request.

Solution

Use the List Monitors command to confirm that the `header` value set in the Cloudflare monitor is correct and the Update Monitors command to make any necessary changes.

TLS protocol error

Cause

This error can occur if you’re using an older version of TLS or your endpoint is not configured for HTTPS.

Solution

Ensure that your endpoint supports TLS 1.0 or greater and is configured for HTTPS.

TLS unrecognized name error

Cause

The server did not recognize the name provided by the client. When a host header is set, we set this as the ServerName in the initial TLS handshake. If not set, we will not provide a ServerName, which can cause this error.

Solution

Set the host header in your monitor object.

No route to host error

Cause

The IP address cannot be reached from our network. Common causes are ISP or hosting provider network issues (e.g. BGP level), or that the IP does not exist.

Solution

Make sure IP is accurate, and if it is check if there is an ISP or hosting provider network issue.

Exceeded quota error

Cause

You will receive this error if you attempt to create more objects (monitors, pools, or endpoints) than are included in your plan.

If using the dashboard, you will not be able to create additional objects.

If you're using the **Cloudflare API**, you will receive an error message.

Solution

- Enterprise customers who need to create more objects (load balancers, pools, endpoints, or monitors) should reach out to their account team to discuss this issue.
- Self-service customers can upgrade their Load Balancing subscription with more endpoints to increase load balancing capacity.

TCP Timeout

Cause

Data transmission was not acknowledged and retransmit of data did not succeed.

Solution

Confirm whether the SYN-ACK for the handshake takes place at your endpoint and contact Cloudflare Support.

TLS Handshake Failure

Cause

Indicates that the browser's connection to the web server is not secure.

Solution

Change wifi networks, connect to a wired network, or verify the network connection is stable.

Network Unreachable

Cause

Cloudflare cannot connect to the endpoint due to network unavailability. This is usually caused by a network issue or incorrect IP.

Solution

Check either the IP entered for the endpoint in Cloudflare's Load Balancer configuration or the IP returned via DNS for the endpoint hostname.

HTTP Invalid Response

Cause

Usually caused by an HTTP 502 error or bad gateway.

Solution

Ensure the endpoint responds to requests and that no applications have crashed or are under high load.

DNS Unknown Host

Cause

The endpoint hostname does not exist.

Solution

Confirm the endpoint resolves to an IP address.

Connection Reset by Peer

Cause

A network error occurred while the client received data from the endpoint.

Solution

Confirm whether the endpoint is experiencing a high amount of traffic or an error.

Monitor Config Error

Cause

There was a configuration error in the monitor and no checks are run against the pool endpoints.

Solution

Review your monitor configuration to ensure it matches an expected request to your endpoint.

DNS Internal

Cause

The endpoint's hostname resolves to an internal or orange-clouded IP address. No checks are run against the pool endpoints.

Solution

Cloudflare does not allow use of an endpoint hostname that is proxied by Cloudflare.

Load Balancing Not Enabled

Cause

Load Balancing is not enabled for your account or zone.

Solution

For Enterprise customers, reach out to your Cloudflare Account Team. Free, Pro, and Business customers should Enable Load Balancing.

Validation failed error

Cause

You will receive an error if you try to set the host header value while configuring a load balancer endpoint.

Solution

Cloudflare now restricts configured endpoint host headers to fully qualified domain names (FQDNs) that are immediate subdomains of a zone associated with the account. For example, this host header would be the same zone as the load balancer itself, but pools may be used across multiple Load balancers.

Object referenced by other objects

Cause

You will receive this error when you attempt to delete a pool that is referenced by a load balancer geo steering region, or by a pool set.

Solution

For a geo steering reference, remove the pool from the load balancer's geo steering configuration. If your load balancer no longer uses geo steering, you will need to re-enable geo steering and then remove the pool.

For a pool set reference, remove the pool from every pool set that references it, including any `overrides.pool_weights` and `overrides.fallback_pool` entries.

Other Failure

Cause

If the failure cannot be classified as any other type of failure mentioned above.

Solution

Contact Cloudflare Support.

□□□ #2
□ □□□ □□□ 2026-11-01 02:50:51 UTC
□ □□□ □□□ 2026-11-01 02:50:52 UTC