Cloudflare ACE Training Handbook

This page outlines all labs and assignments. Please make use of this page if you happen to be faster or slower than the training speed.

> 💡 **Learning Objective:**
> After completing the training, you can implement **Cloudflare application services** for your customers, on a POC or a production project.
> To ensure that, **please make sure to complete all the labs and assignments!**

🔌 Table of Contents

Prerequisite

▼ Click to view

Day 1. Implementing Cloudflare

☝ CNAME Setup Onboarding Labs

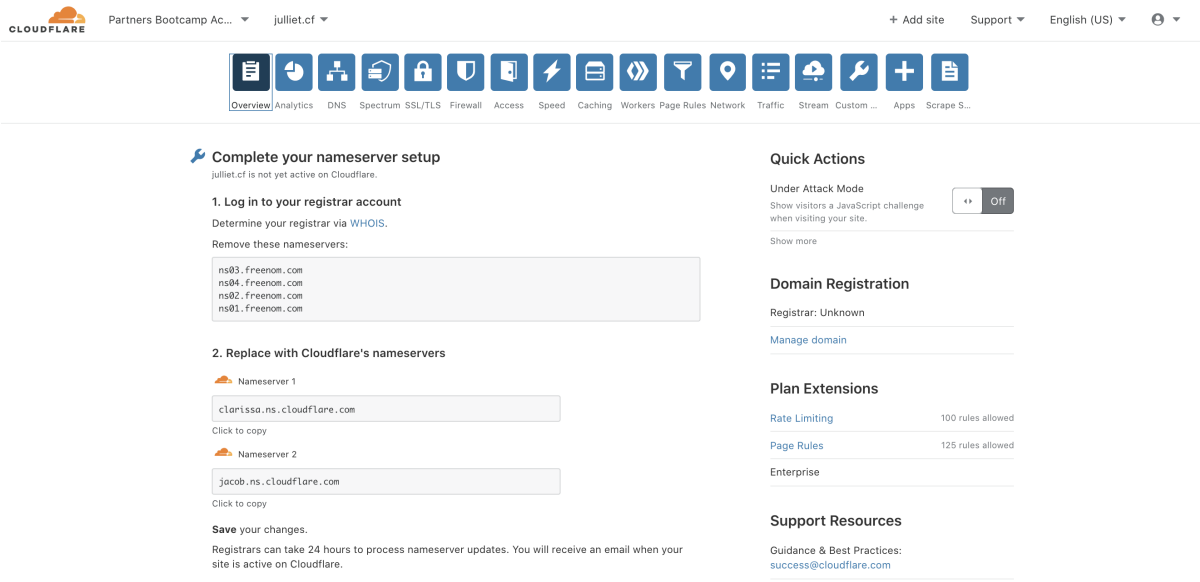
▼ A. Get your domain

In this guide, we will use free registrar service at freenom.com. But do feel free to use your own choice of registrar for this step.

1. Go to freenom.com and create your account.
2. Get a free domain at `services - Register new domain`
3. Go to Cloudflare web dashboard.
4. Access `Partners Demo (Bootcamp) Account`
5. Click `Add a site` and register your new domain.

> 💡 Add the root domain `yourdomain.cf`, not the FQDN `test.yourdomain.cf`

6. Select Enterprise Plan.
7. Finish the guide.

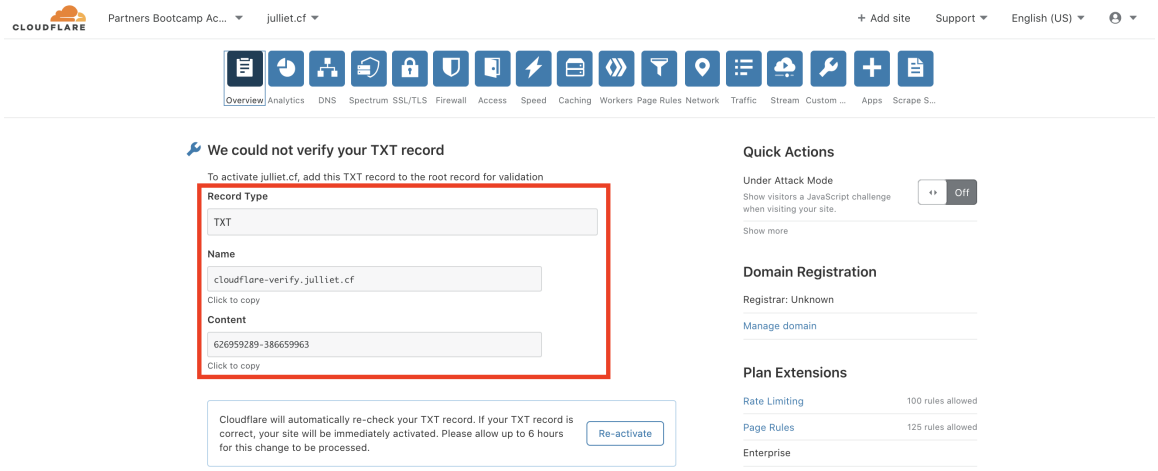


This is what you would be seeing after the steps.

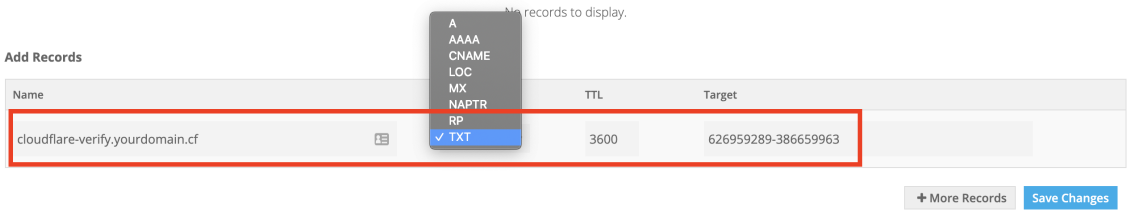
▼ B. Account activation on `CNAME setup`

> 💡 We are following the CNAME setup to learn about customer's testing scenario.
> You can also use Cloudflare as your authoritative DNS following full setup.

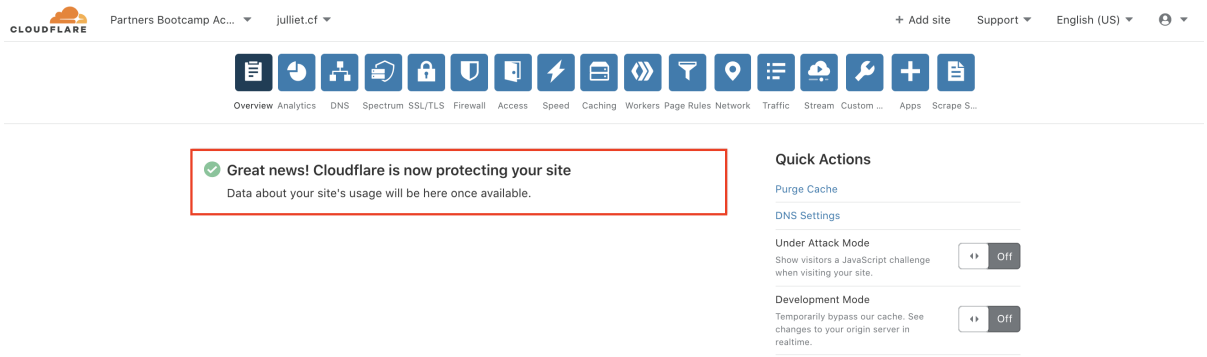
1. Go to Cloudflare dashboard - Overview.
2. Find `Advanced Options -- Convert to CNAME DNS Setup` at the bottom of the screen.
3. Read the warning and click `Convert`.



4. Find TXT record for the zone validation, then go to Freenom dashboard.
5. At Freenom, access `My domains - Manage Domain - Manage Freenom DNS` and add TXT record you were given.



6. Confirm the TXT record propagation at `https://dnschecker.org`. Then confirm Cloudflare account validation.

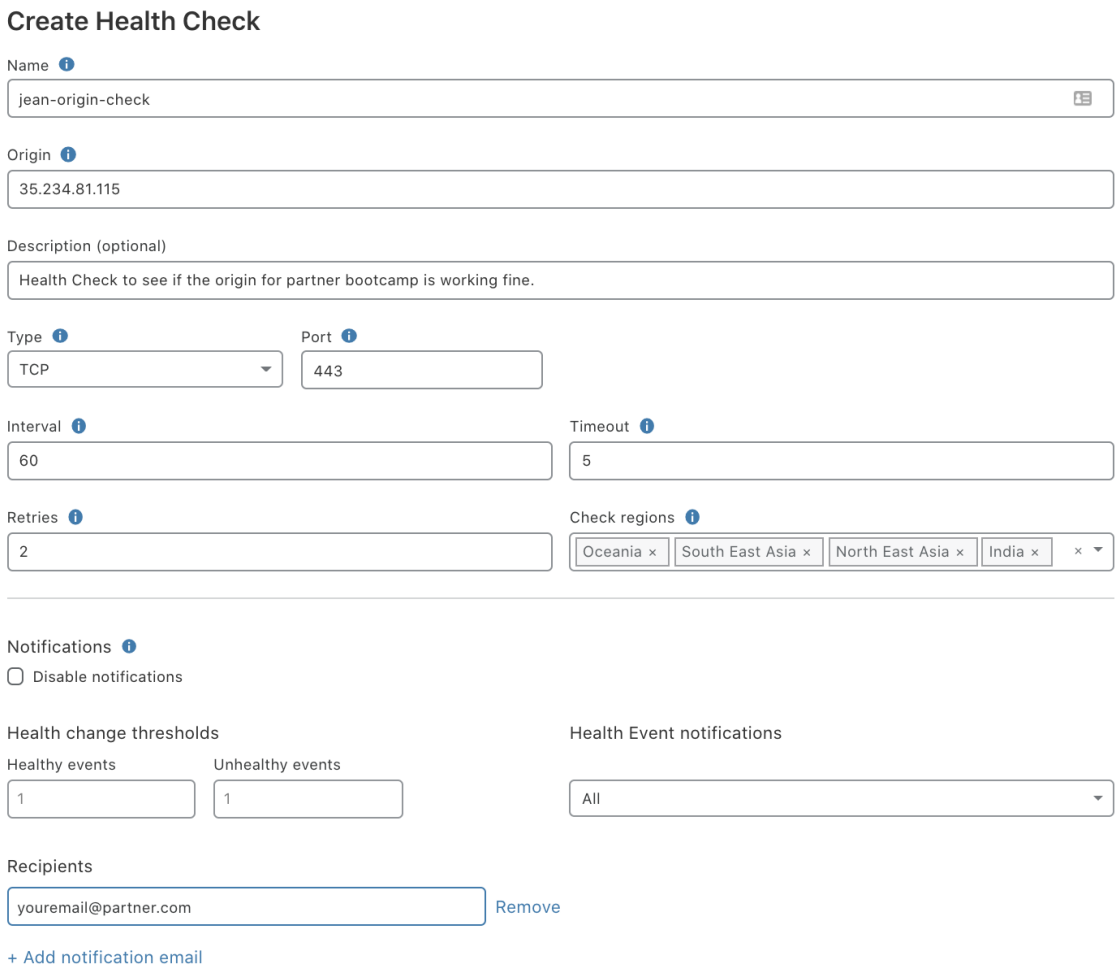


Congratulations, account activation success!

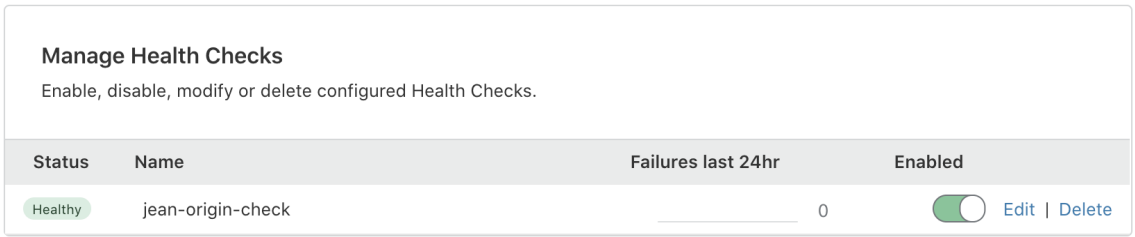
▼ C. Health checks — CF ↔ Origin

Always better advised to set up Cloudflare to origin health check to ensure the origin responds to Cloudflare correctly before pushing traffic through Cloudflare proxy.

1. Go to Cloudflare dashboard.
2. Access Traffic - Health Checks.
3. Configure health checks. Today's origin: **35.234.81.115**.



- You should always proceed to next steps after confirming your health check is successful.

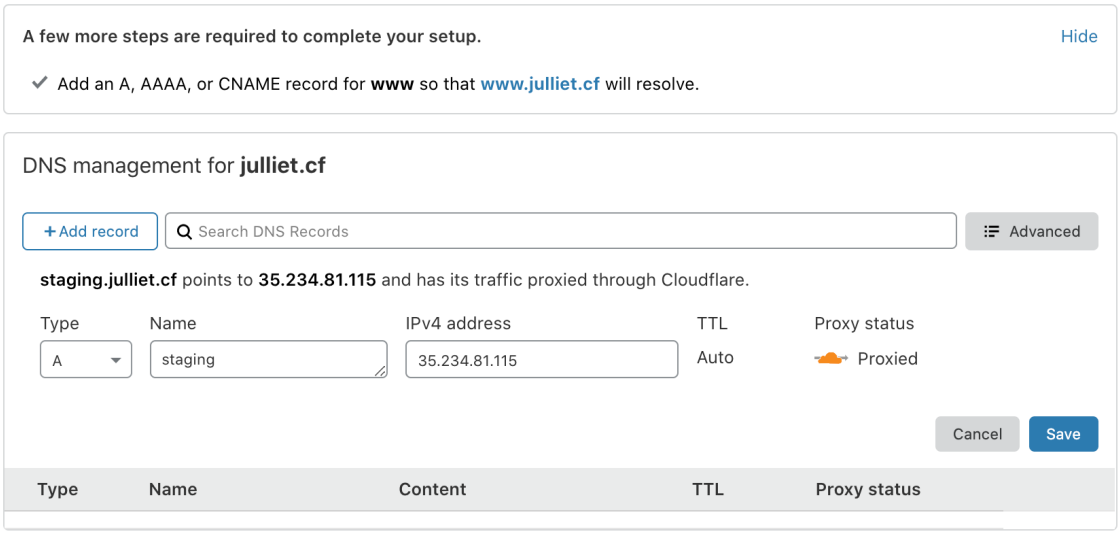


Like this.

▼ D. Activate Cloudflare for staging host first.

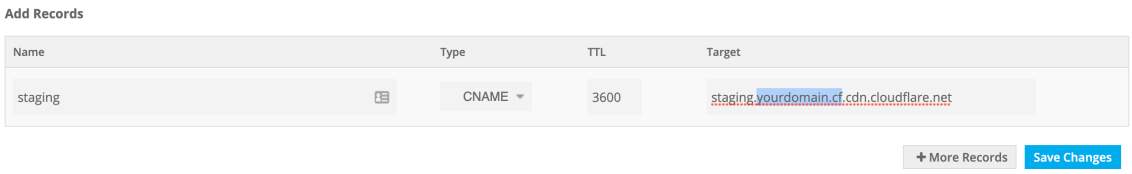
1. Go to Cloudflare dashboard - DNS.
2. At Cloudflare DNS, add a DNS record as following:

```
Type: A
Name: staging
IPv4 address: 35.234.81.115
Proxy status: on (orange-clouded)
```



3. Go to Freenom DNS control panel.
4. At Freenom DNS, add a DNS record as following:

```
Type: CNAME
Name: staging
Value: staging.yourdomain.com.cdn.cloudflare.net
TTL: 300
```



5. Confirm the new DNS record propagation at https://dnschecker.org.
6. Confirm if your site is accessible at browser and/or terminal.

```
$ curl -svo /dev/null/ http://staging.yourdomain.com 2>&1 | grep 'HTTP'

HTTP/2 200 OK
```

Staging implementation complete. Please test the site to see if the site works as expected.

▼ E. Activate Cloudflare for the production host.

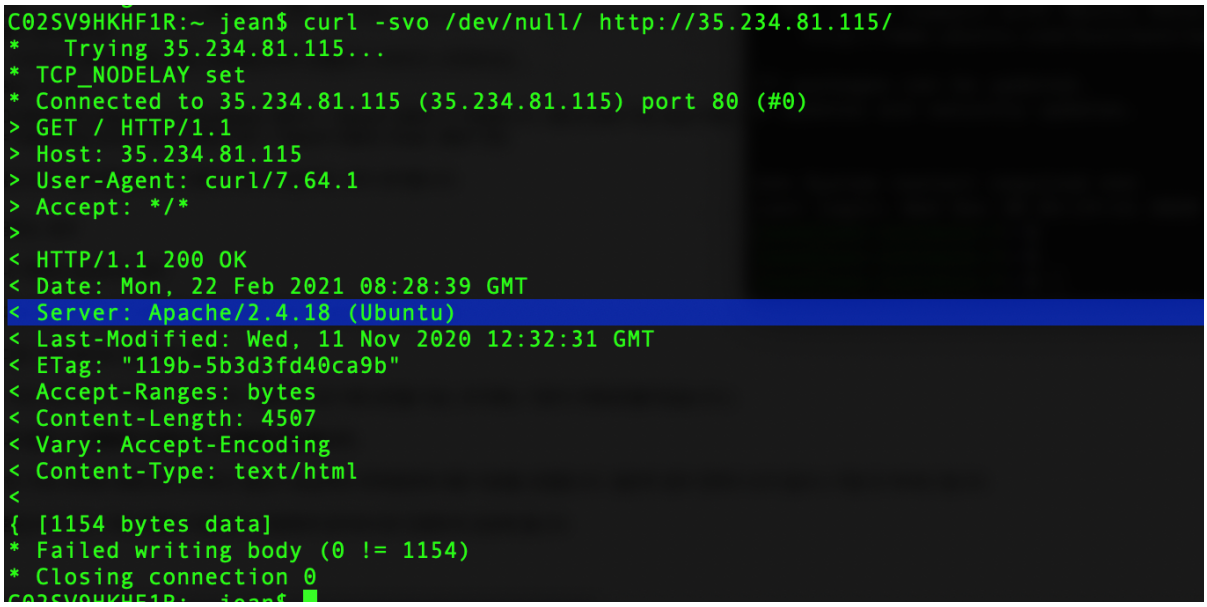
Activate Cloudflare for the `www` host. You can refer to the step d1-d6 if you are not sure how to.

▼ F. Confirm Cloudflare is enabled.

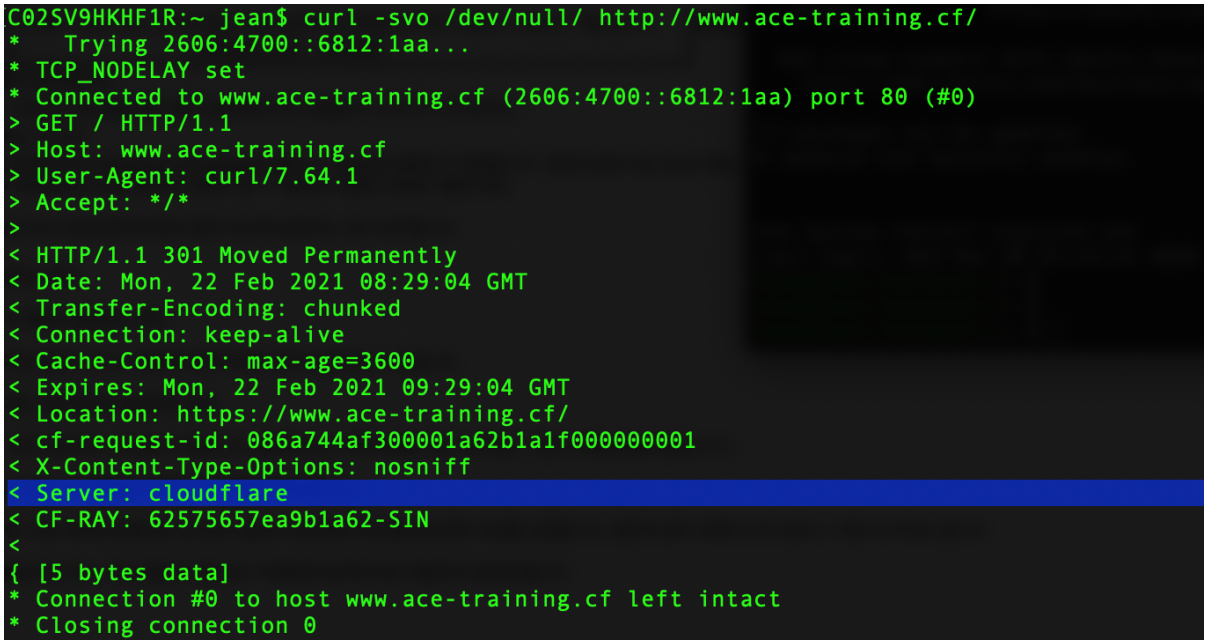
- Use your terminal to send below two requests, and compare the difference in HTTP response headers.

```
curl -svo /dev/null/ http://35.234.81.115/

curl -svo /dev/null/ http://staging.yourdomain.com/

curl -svo /dev/null/ https://www.yourdomain.com/
```

- Did you find the difference in response headers? Think about why.
- Are you able to connect to HTTPS to both sites? Think of a reason about why you can or can't.



Send curl to the origin.



Send curl to Cloudflare onboarded domain.

✌️ DNS, SSL, Onboarding Check Lab

▼ DNS Lab

Performance comparison between customer's current DNS and Cloudflare DNS.

Let's learn why we would like to recommend Cloudflare DNS to our customers.

- Go to DNS Speed Test Tool
- Try with non-Cloudflare domain. e.g. your customer domain

Email Share

DNS Speed Test

The DNS hosting speed tool will give you valuable DNS performance information for each level in the DNS tree to assist with performance evaluations and performance troubleshooting.

Enter a host name or domain name:

freenom.com Go »

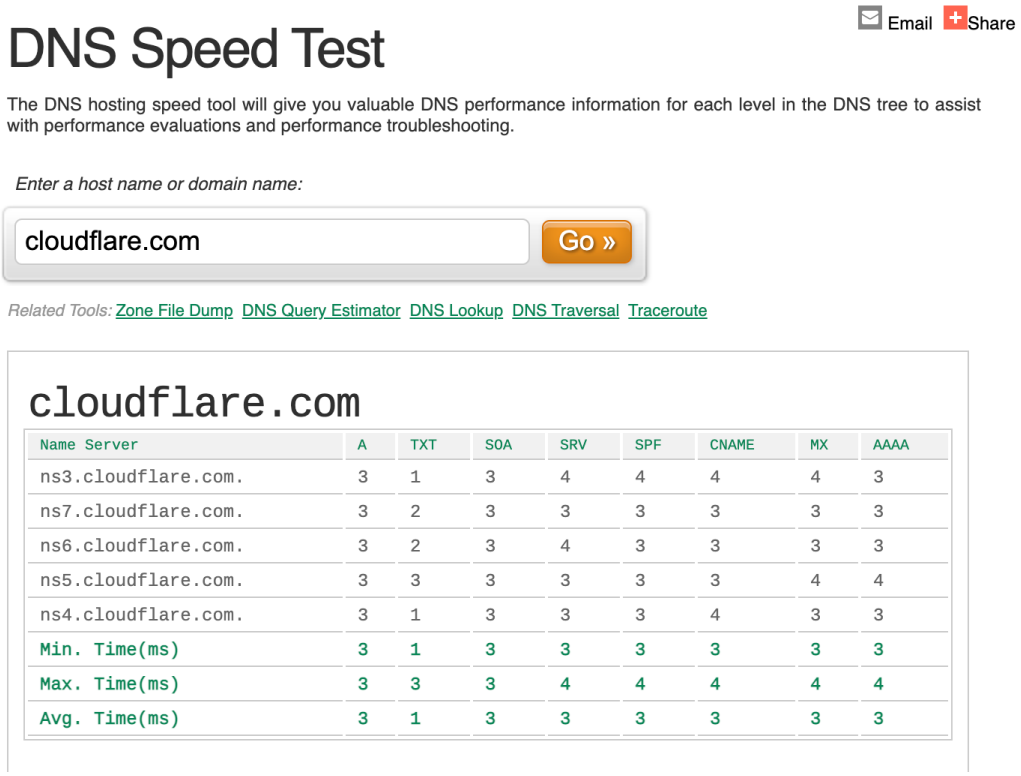
Related Tools: Zone File Dump DNS Query Estimator DNS Lookup DNS Traversal Traceroute

freenom.com

Name Server	A	TXT	SOA	SRV	SPF	CNAME	MX	AAAA
ns03.freenom.com.	83	83	83	83	83	83	83	83
ns01.freenom.com.	68	69	69	68	68	67	68	72
ns04.freenom.com.	83	83	83	83	83	83	83	83
ns02.freenom.com.	69	69	68	67	68	68	68	68
Min. Time(ms)	68	69	68	67	68	67	68	68
Max. Time(ms)	83	83	83	83	83	83	83	83
Avg. Time(ms)	75	76	75	75	75	75	75	76

Example: DNS speed test to freenom.com.

- Try with cloudflare.com



Example: same to cloudflare.com.

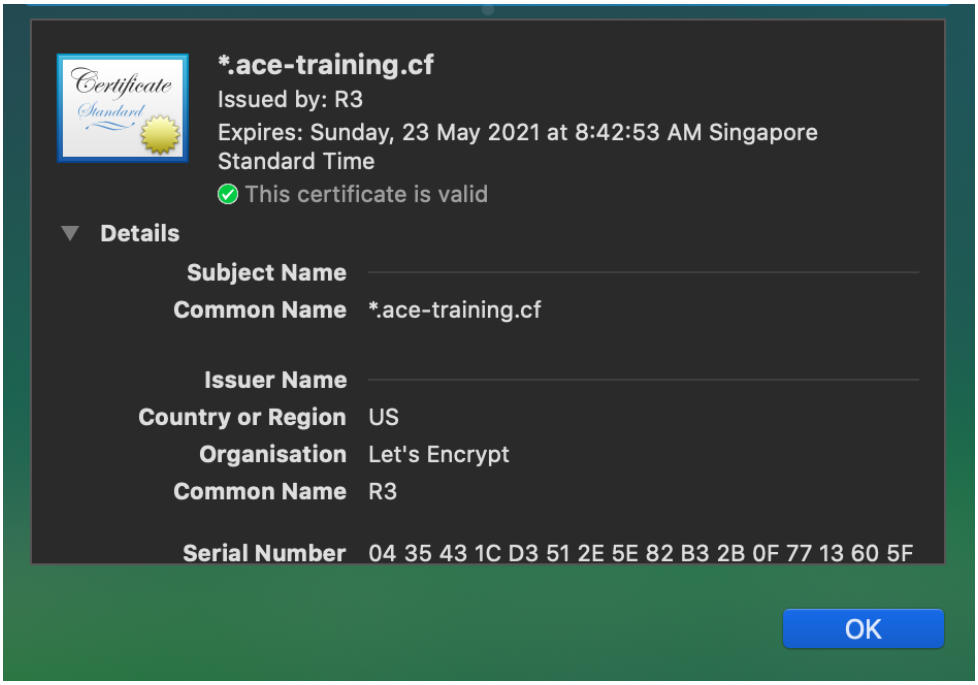
> 💡 **Would you like to test more?**
> You may want to add a record at Freenom DNS (or your choice of any authoritative DNS) then measure its propagation time vs add a record at Cloudflare DNS (you need a full setup zone for this) then measure its propagation time. You can measure it at dnschecker.org.

▼ SSL Lab

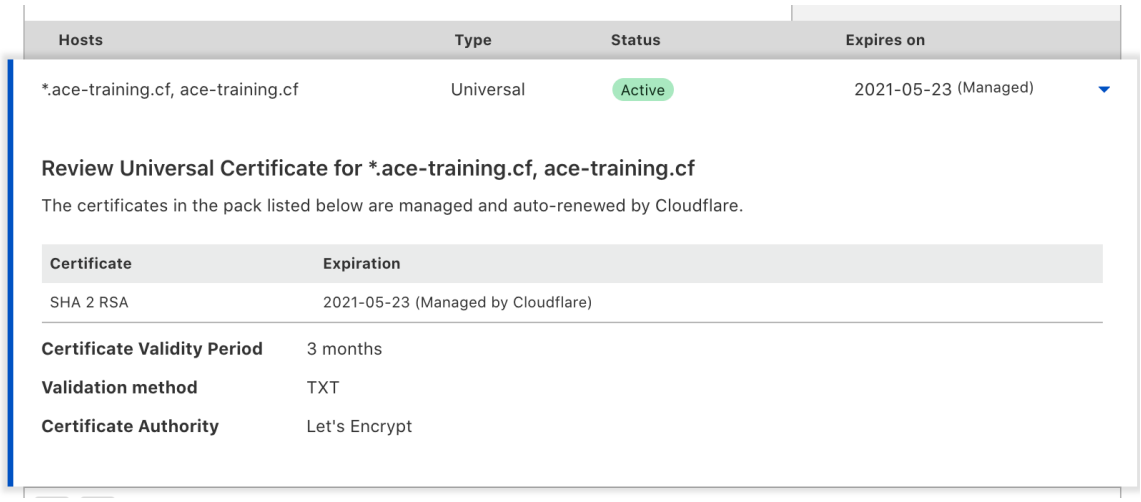
Labs — Easy SSL deployment and easy SSL redirection. Cloudflare Certificate is easy to issue and maintain!

A. Already-available SSL without your action

1. At your browser, connect to `https://www.yourdomain.cf/` and see the certificate information.



Confirm HTTPS is already available without your action. See the certificate information.



Learn how to verify which certificate is shown in the browser.

B. Try the following commonly used SSL setting.

- Automatically redirect `http://` requests to `https://`
- Order an `Advanced Certificate` with your preferred custom hostnames, validity period, certificate authority.
- Upload your own certificate in the dashboard.

▼ Onboarding Checks

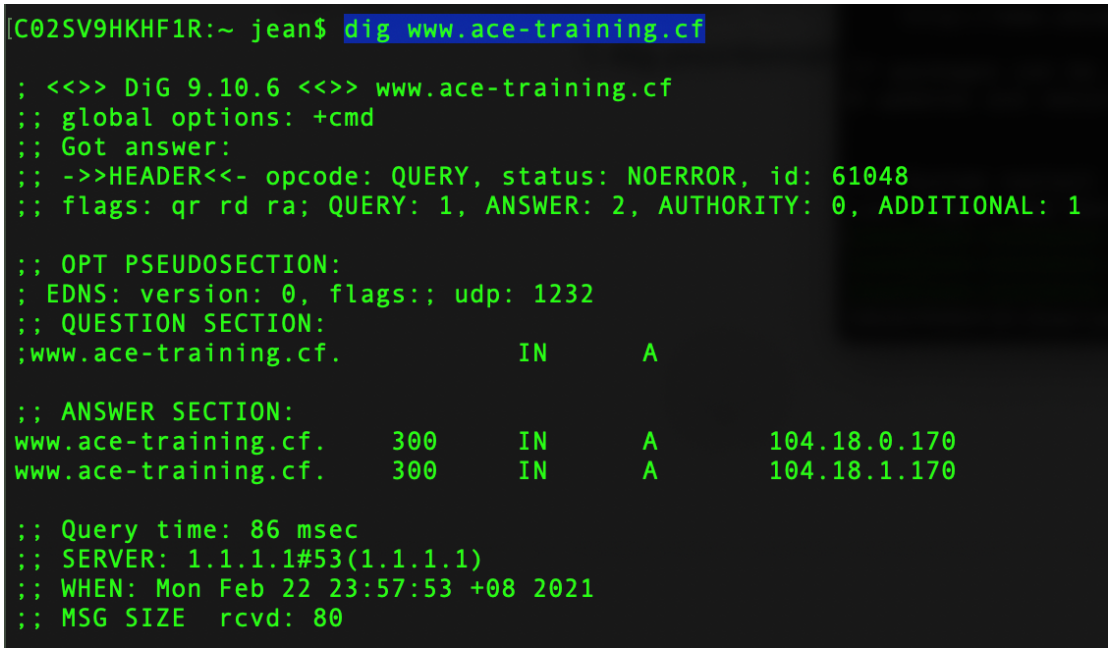
Let's have some fun with basic commands you can use for Cloudflare.

▼ dig

Dig is command line tool similar to nslookup that is used to run DNS queries and check DNS records for a given domain/website.

- Try it with your domain.

```
$ dig yourdomain.cf
```

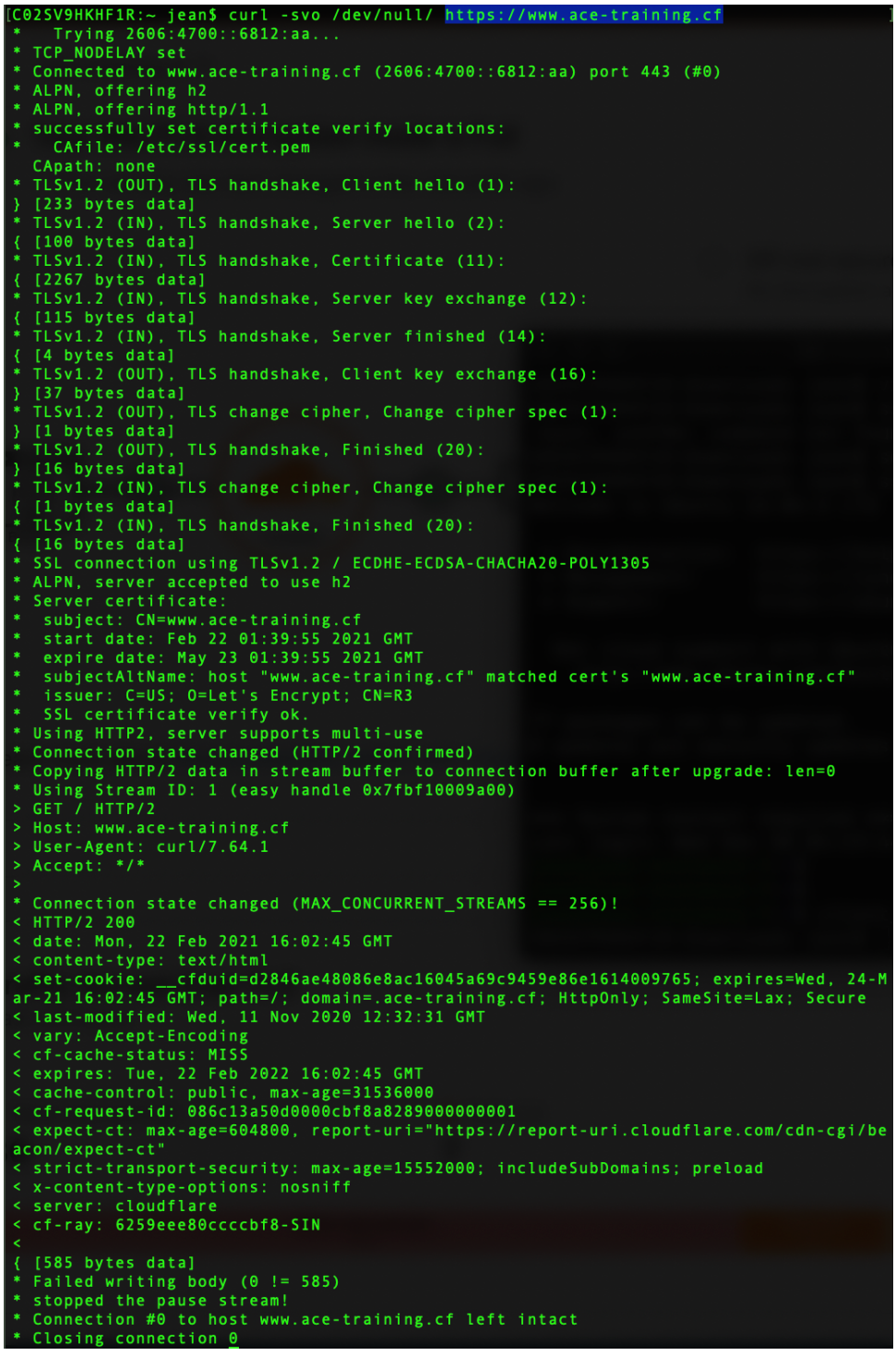


▼ curl

cURL is a command line tool used to transport data using the URL syntax.

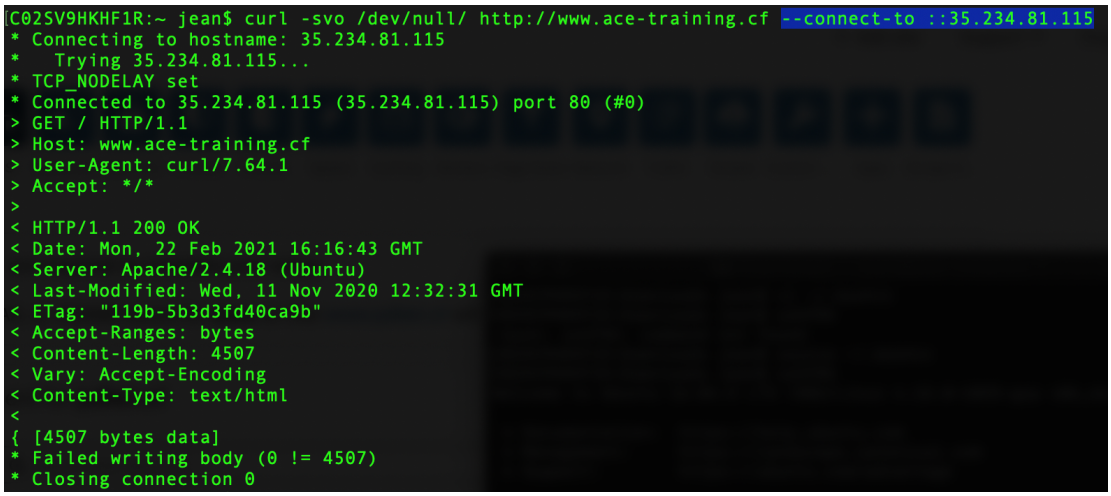
- Try it with your domain.

```
$ curl -svo /dev/null/ https://www.yourdomain.cf/
```



- Try this `curl` and see the difference.

```
$ curl -svo /dev/null/ http://www.yourdomain.cf/ --connect-to ::35.234.81.115
```



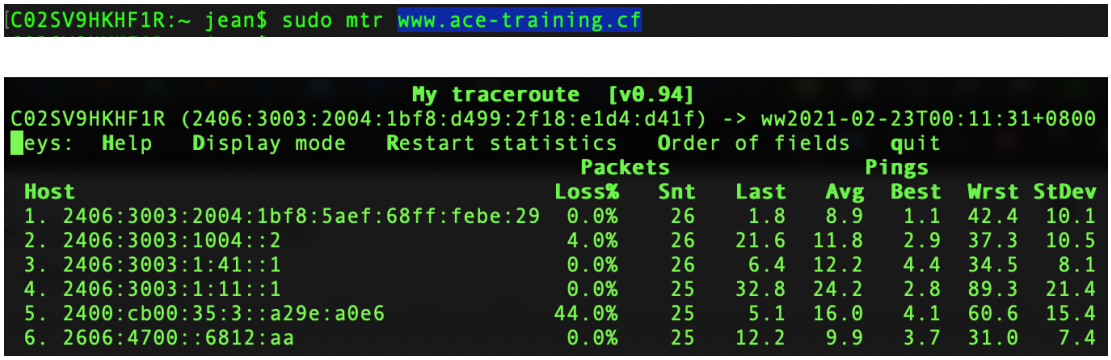
This option will check the origin response directly.

▼ mtr

MTR/Traceroute is Network based command line tools used to measure performance/latency on a particular path to a given host/destination.

- Try it with your domain.

```
$ sudo mtr www.yourdomain.cf
```



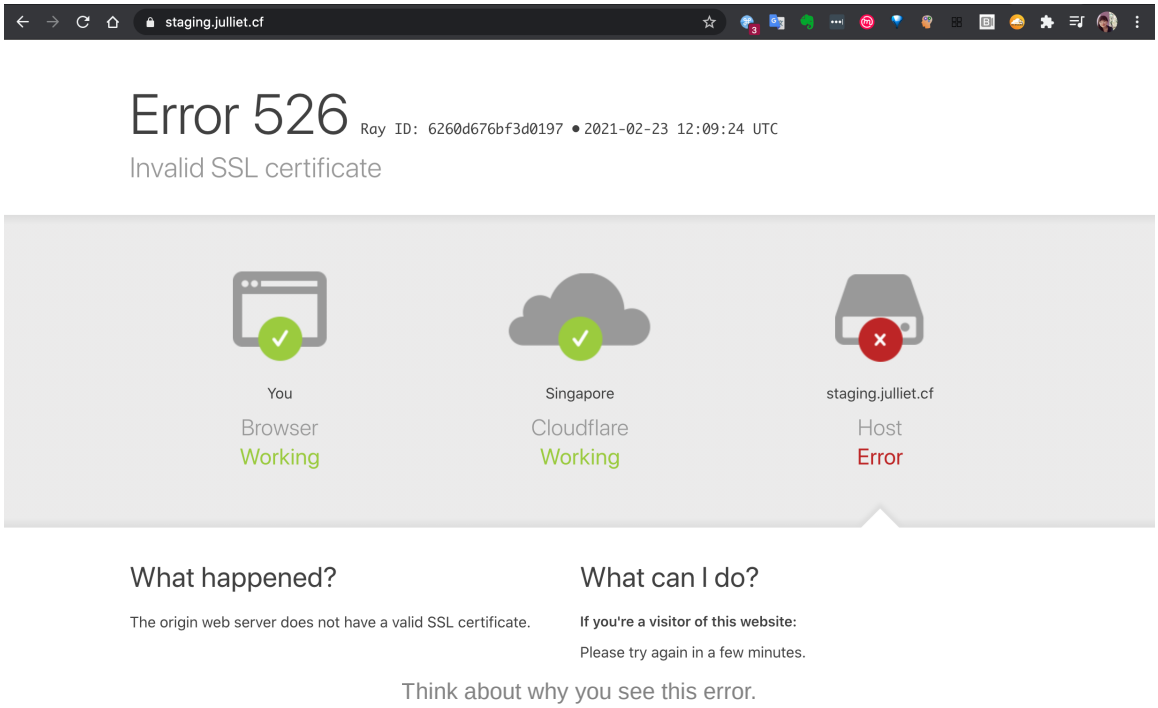
Day 2. Optimizing Cloudflare

☝ Onboarding Best Practice — Labs

▼ Custom Error Pages

Configure example custom error pages. Let's see why we need "Custom Error Pages" for enterprise customers.

1. At Cloudflare dashboard, go to `TLS/SSL - Overview` and select `Strict (SSL only origin pull)`
2. At the browser, visit your website: `https://www.yourdomain.cf/`



3. At the browser, access `http://www.ace-training.cf/error.html`
4. At Cloudflare dashboard, visit `Custom Pages - 500 Class Errors`, and try publishing the page: `http://www.ace-training.cf/error.html`
5. Give Cloudflare some time to provision, then visit your website again: `https://www.yourdomain.cf/` and confirm the difference.
6. Once you're finished with testing, please roll back the SSL setting to `full`.

> 💡 Why configuring custom error pages is a must?
> When something happens, what do you think the customer wants to show - their branded page or Cloudflare branded error page?

▼ Configure Alerts

Configure necessary alerts to your email address. Get alerted by email in the event of: Origin server failure, DDoS attack

1. At Cloudflare dashboard, go to `Account Home - Notification`.
2. Try setting `HTTP DDoS Attack Alert`, `Layer 3/4 DDoS Attack Alert` and `Passive Origin Monitoring` to your work email.
3. Once alert is set, you will get alerted on HTTP DDoS events, and origin health (even if no active health check) based on limited set of passive error codes. (e.g. 521)

> 💡 Note:
> - Alert only works after you have added the notifications;
> - Layer 3/4 DDoS Attack Alerts is currently available for Magic Transit, Spectrum customers only;
> - Customizing alerting threshold is not supported yet

▼ Is the Origin Correctly Secured?

In this lab we will scan the origin server and understand the implementation best practice. You should be permitted to scan the origin server when you run this for the customer.

1. Try access https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap
2. Enter the test origin address `35.234.81.115` and run a `light scan`. Check the result.
3. If you have, check your own test origin server or a customer's origin server.
4. Do you think this origin is opening the web port to ANY? Were you able to confirm?
5. Even if the origin is set like this, if it's behind Cloudflare, is it immune to DDoS and security threats?

Found 4 open ports (1 host)

35.234.81.115

› 115.81.234.35.bc.googleusercontent.com

Port Number	State	Service Name	Service Product	Service Version	Service Extra Info
22	open	ssh	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Ubuntu Linux; protocol 2.0
80	open	http	Apache httpd	2.4.18	(Ubuntu)
81	open	http	Apache httpd	2.4.46	(Unix)
443	open	https	Apache httpd	2.4.18	(Ubuntu)
3306	closed	mysql			
3389	closed	ms-wbt-server			
5000	closed	upnp			
8080	closed	http			
8443	closed	https-alt			

What should you advise to the owner of this server?

✌ Security Labs

▼ WAF

Let's do a quick pentest before and after WAF configuration, check the logs

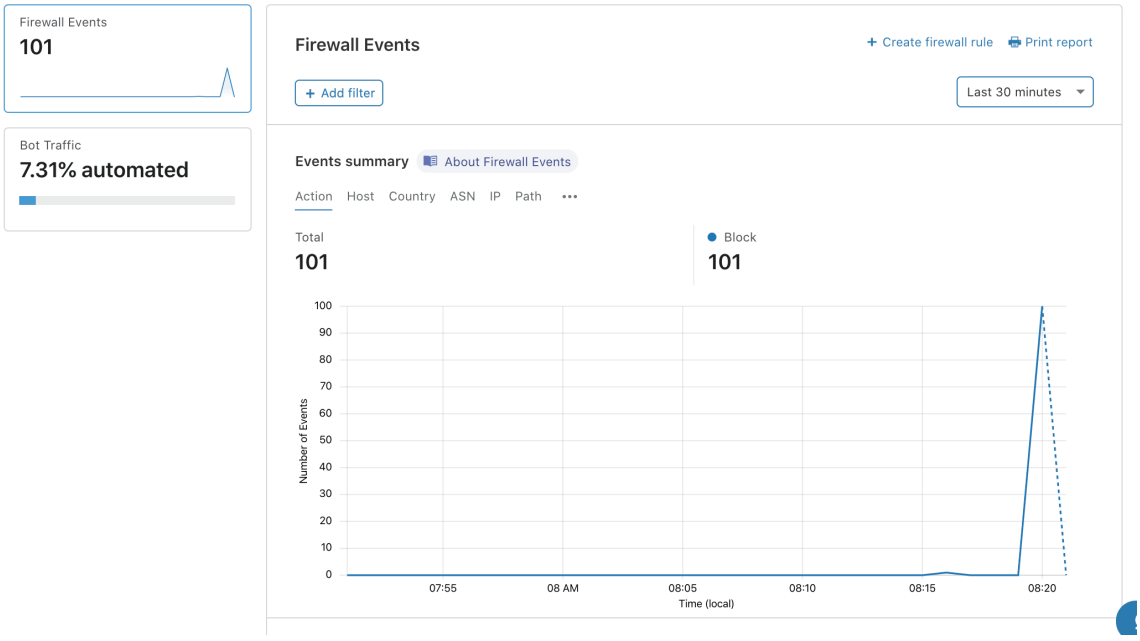
1. Access Cloudflare dashboard - `Firewall - Managed Rules`. Confirm WAF is `OFF`.
2. Access `https://www.yourdomain.cf/file.php?cmd=echo(shell_exec(%22ls%20/etc/var%22))`

```
$ curl -svo /dev/null/ "https://www.yourdomain.cf/file.php?cmd=echo(shell_exec(%22ls%20/etc/var%22))"
```

3. Turn the WAF `on`.
4. Re-try the exploit.
5. (Optional) Try many times

```
$ for i in {1..100}; do curl -svo /dev/null/ -H "exploit: true" "https://www.yourdomain.cf/file.ph
p?cmd=echo(shell_exec(%22ls%20/etc/var%22))" 2>&1 | grep "< HTTP"; done;
```

6. Find the blocked logs at Cloudflare Firewall dashboard.



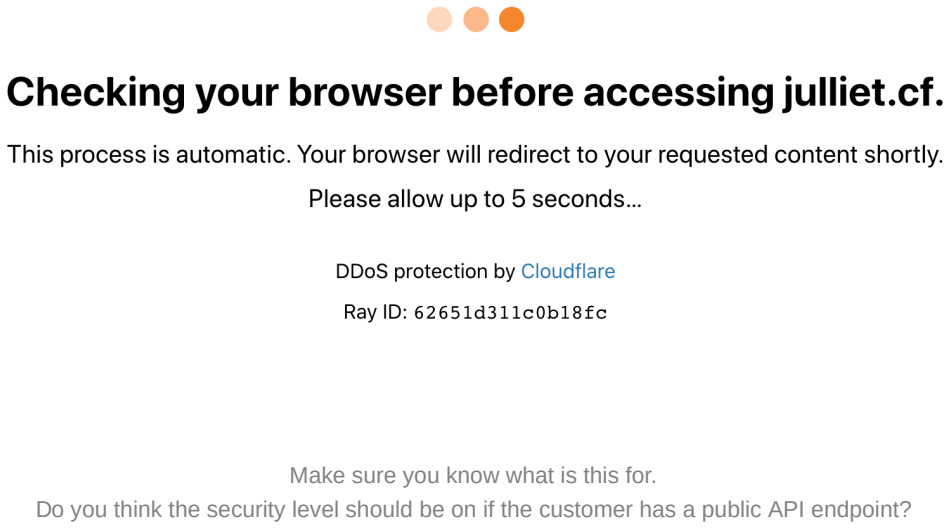
Check the detail of the event.

▼ Security Level

Let's understand the Security Level, JS Challenge everyone with "I'm Under Attack Mode"

1. At Cloudflare dashboard, adjust your test domain's security level to `I'm Under Attack Mode`.
2. At your browser, try access the domain and check the result and status codes.

3. At your terminal, try access the domain and check the result and status codes.
4. After the exercise, `turn off the IUAM` (change it to medium/high) so the next exercise won't be disturbed.



▼ Rate Limiting

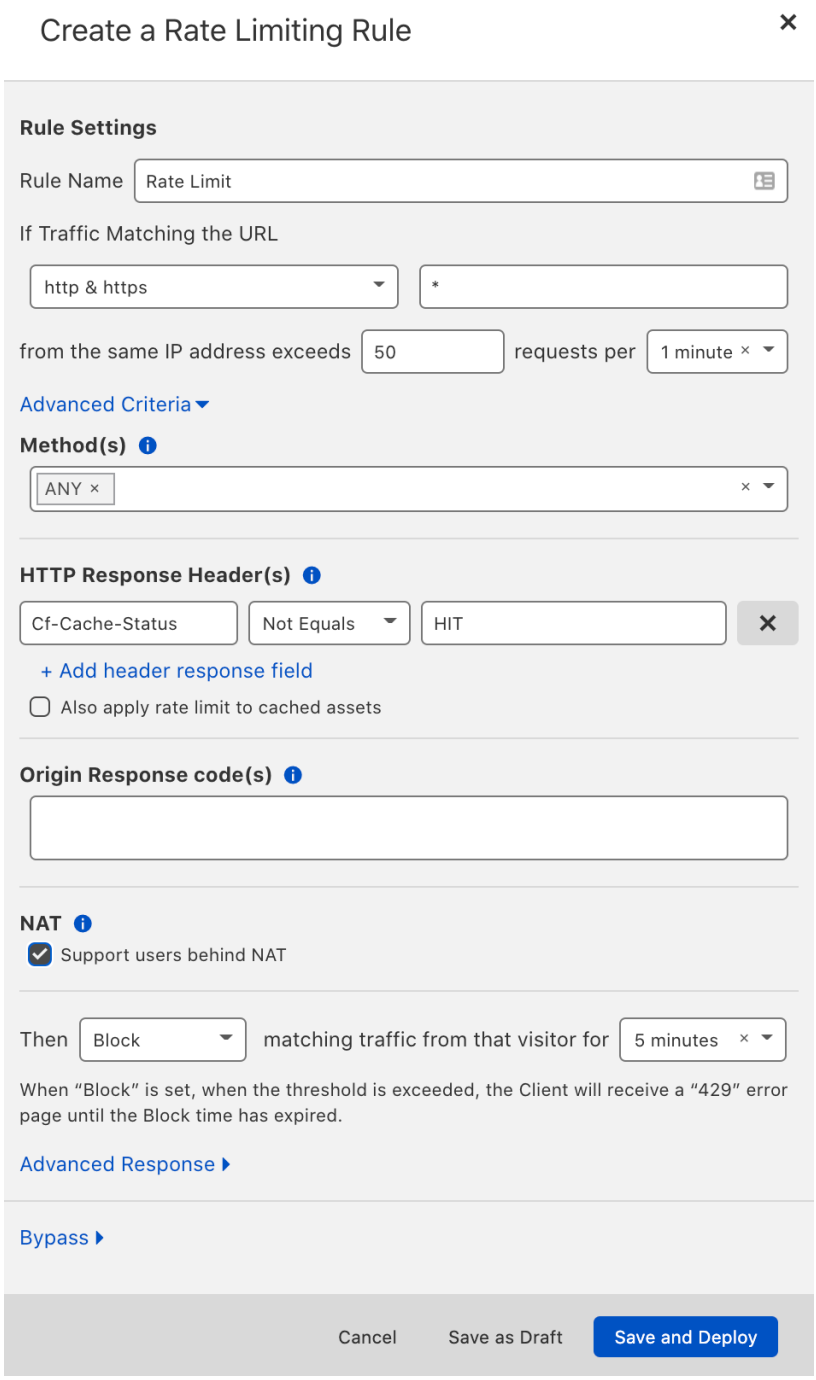
Rate Limiting is a must add-on for enterprise clients who are worried about DDoS attack.

We will do a quick test before and after Rate Limiting configuration, check the logs

- At your terminal, run this command to send 200 requests to the site:

```
for i in {1..200}; do curl -svo /dev/null/ -H "requestflood: true" "https://www.yourdomain.cf/" 2>
&1 | grep "< HTTP"; done;
```

- Confirm your requests are served with status code `200`.
- At Cloudflare dashboard, create a Rate Limiting rule.



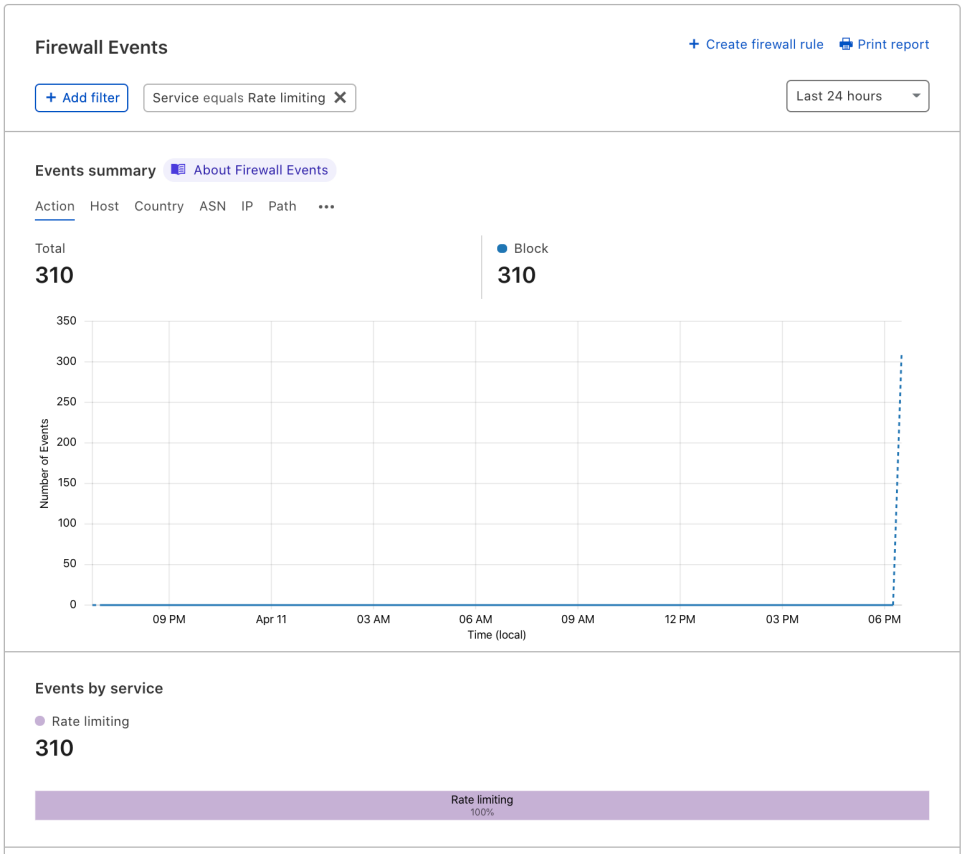
- Run the same command again.

```
for i in {1..200}; do curl -svo /dev/null/ -H "requestflood: true" "https://www.yourdomain.cf/" 2>
&1 | grep "< HTTP"; done;
```

- See what happens to your flood requests.

```
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 200
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
< HTTP/2 429
```

- At Cloudflare dashboard, check the logs created just now.



▼ Firewall Rules

Using Firewall Rules, you can flexibly customize your organization's security rules to meet the needs. Let's test with below examples.

1. Try set a rule to only allow one client IP `1.2.3.4` when people access `http(s)://yourtestdomain.cf/admin.html`.

2. Try set a rule to give `JS challenge` to everyone when the request to `http(s)://yourtestdomain.cf/*` is `NOT` coming from your country.

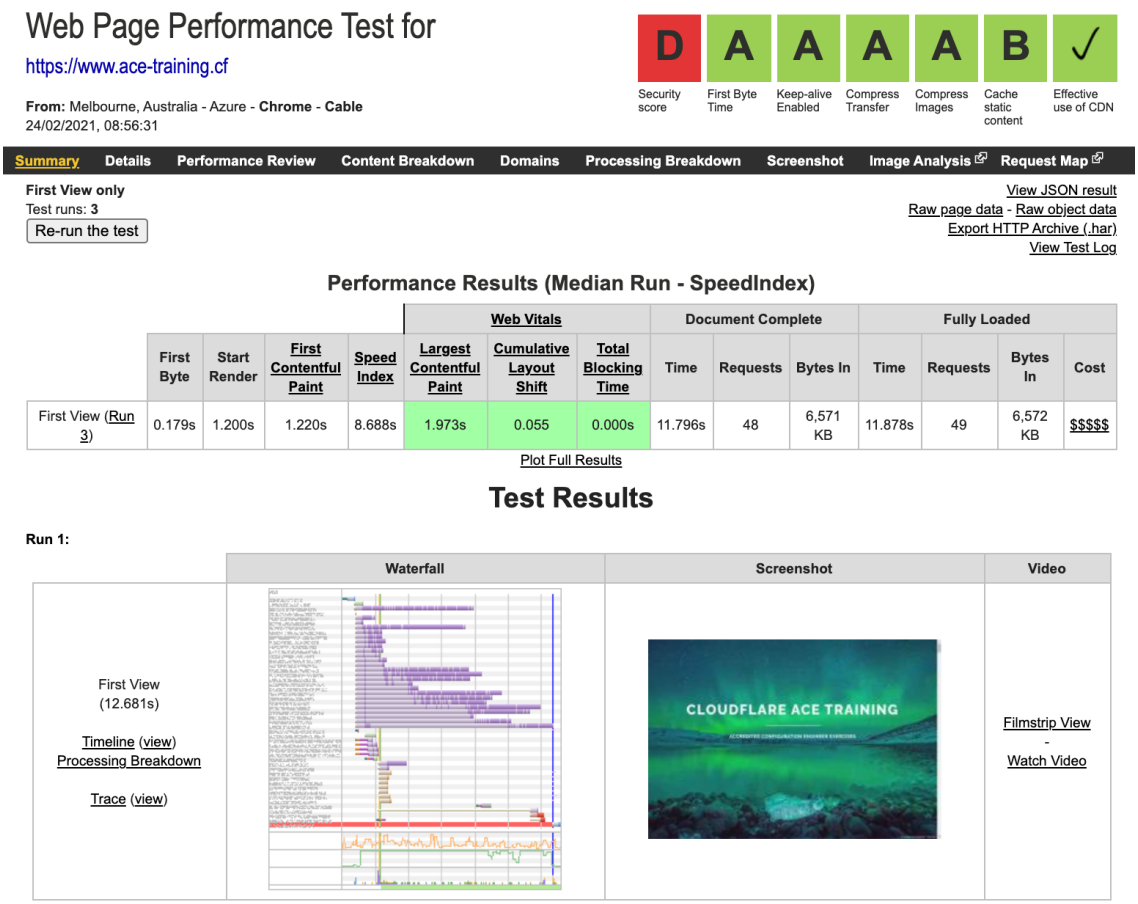
Try to create the rules

🤟 Performance Labs

▼ Synthetic Performance Test

Learn how to run synthetic performance tests, and think about how you can make your Cloudflare site faster than you see.

1. Access `https://webpagetest.org`
2. Run a test to `https://www.yourdomain.cf/` (choose a node you want; e.g. Singapore EC2)
3. Open another tab with the same URL webpagetest.org, run another test to the sample site — `https://optimized.ace-training.cf/`
   This is the same page proxying to the same origin. Use the same location with above (e.g. Singapore EC2)
4. Compare two results. Content is same. Is the result similar or different? Let's think about why.



Web Page Performance Test for
https://www.ace-training.cf

From: Melbourne, Australia - Azure - Chrome - Cable
24/02/2021, 08:56:31

D	A	A	A	A	B	✓
Security score	First Byte Time	Keep-alive Enabled	Compress Transfer	Compress Images	Cache static content	Effective use of CDN

Summary | Details | Performance Review | Content Breakdown | Domains | Processing Breakdown | Screenshot | Image Analysis | Request Map

First View only
Test runs: 3
Re-run the test

View JSON result
Raw page data - Raw object data
Export HTTP Archive (.har)
View Test Log

Performance Results (Median Run - SpeedIndex)

					Web Vitals			Document Complete			Fully Loaded			
	First Byte	Start Render	First Contentful Paint	Speed Index	Largest Contentful Paint	Cumulative Layout Shift	Total Blocking Time	Time	Requests	Bytes In	Time	Requests	Bytes In	Cost
First View (Run 3)	0.179s	1.200s	1.220s	8.688s	1.973s	0.055	0.000s	11.796s	48	6,571 KB	11.878s	49	6,572 KB	$$$$$

Plot Full Results

Test Results

Run 1:

	Waterfall	Screenshot	Video
First View (12.681s) Timeline (view) Processing Breakdown Trace (view)		CLOUDFLARE ACE TRAINING	Filmstrip View - Watch Video

Think about why the difference between this and that

> 💡 **Challenge:** Make your domain as fast as `optimized.ace-training.cf` too!

▼ Granular Settings

Understand how you can customize Cloudflare cache settings. Try creating a caching rule for all `HTML pages` under the domain.

- At the Edge:
  - If `status code == 200(OK)`, cache `1 minute`
  - If `status code == 403(Forbidden)` or `404(Not Found)`, cache `10 minutes`
- At client browser: Recommend cache for `30 seconds`

> 💡 You can make rules at `Page Rules`

🤝 Optimization Summary

▼ Click to view

Optimization (Fine-tuning) Checklist

Aa Category		Checklist
Onboarding	☐	Set up health checks
Untitled	☐	Set up necessary notification email
Untitled	☐	Use custom error pages
Untitled	☐	Consider Cloudflare dashboard 2FA or SSO
Untitled	☐	Origin to allow-list Cloudflare IPs
Untitled	☐	Review CF headers/cookies, restore the originating IP if needed.
Untitled	☐	Enable CF Logpush (or Logpull)
Security	☐	Avoid HTTP, redirect/rewrite to HTTPS
Untitled	☐	Hide origin IP/port
Untitled	☐	Turn on WAF
Untitled	☐	Use Security Level at Med or High, IUAM if needed.
Untitled	☐	Set Rate Limiting Rules
Untitled	☐	Get bots visibility and control them
Untitled	☐	Deploy their security needs at Cloudflare Firewall Rules
Performance	☐	Cache as much as possible
Untitled	☐	Maximise use of optimization features
Untitled	☐	Use Brotli compression
Untitled	☐	Use Argo Smart Routing
Untitled	☐	Use newer TLS and better technologies
Untitled	☐	Keep the customer's staging subdomain so you can always use it for origin compatibility test vs. CF optimization feature

Day 3. Troubleshooting Cloudflare

🛠️ Troubleshooting Labs

▼ Turn on the Log

Cloudflare logs is enterprise only, and it has all the necessary information you need for 99% of troubleshooting. While Cloudflare recommends `Logpush` over Logpull (remember this on customer project), we will be using Logpull for this lab because not everyone has access to cloud-based storage.

- Follow this doc https://developers.cloudflare.com/logs/logpull-api/enabling-log-retention to enable Log retention. You can use Postman or Terminal.

Confirm "flag": true, "success": true

▼ Use curl to compare responses

Use cURL resolve override to compare the behaviour between `response-coming-via-Cloudflare` vs `response-directly-from-origin`.

1. ```
   curl -svo /dev/null/ "http://www.yourdomain.cf"
   ```
2. ```
   curl -svo /dev/null/ "http://www.yourdomain.cf" --resolve www.yourdomain.cf:80:35.234.81.115
   ```
3. Think about in what situation you can make use of these two commands.

▼ Use cdn-cgi page

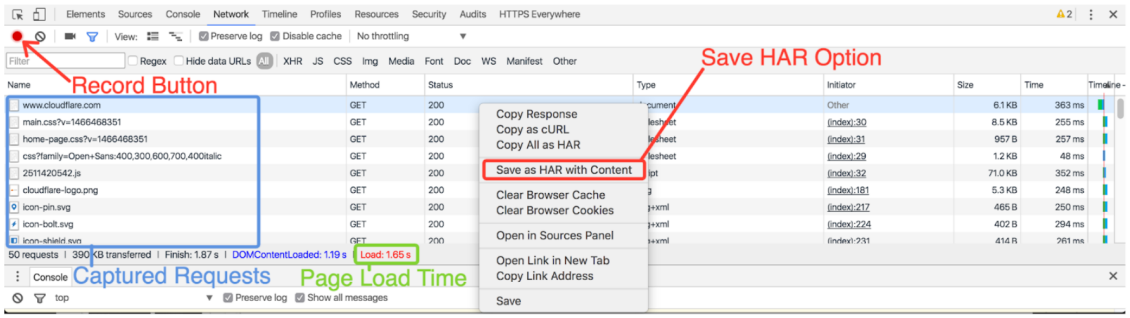
When a host is on Cloudflare there's a way to find metadata easily.

1. At Cloudflare dashboard, **grey-cloud** `staging.yourdomain.cf`
2. At the browser, visit `http://www.yourdomain.cf/cdn-cgi/trace/`
3. At another tab of the browser, visit `http://staging.yourdomain.cf/cdn-cgi/trace/`

▼ Get HAR file

Generate `HAR` file to show the status code and a page you see. If the error is harder to replicate, it will help the Cloudflare support team to understand what you are seeing, or what your customer is seeing.

1. At your browser, open developers tool first, access `http://www.yourdomain.cf/`
2. Right-click the mouse and find "Save as HAR with Content". Save it in your local.

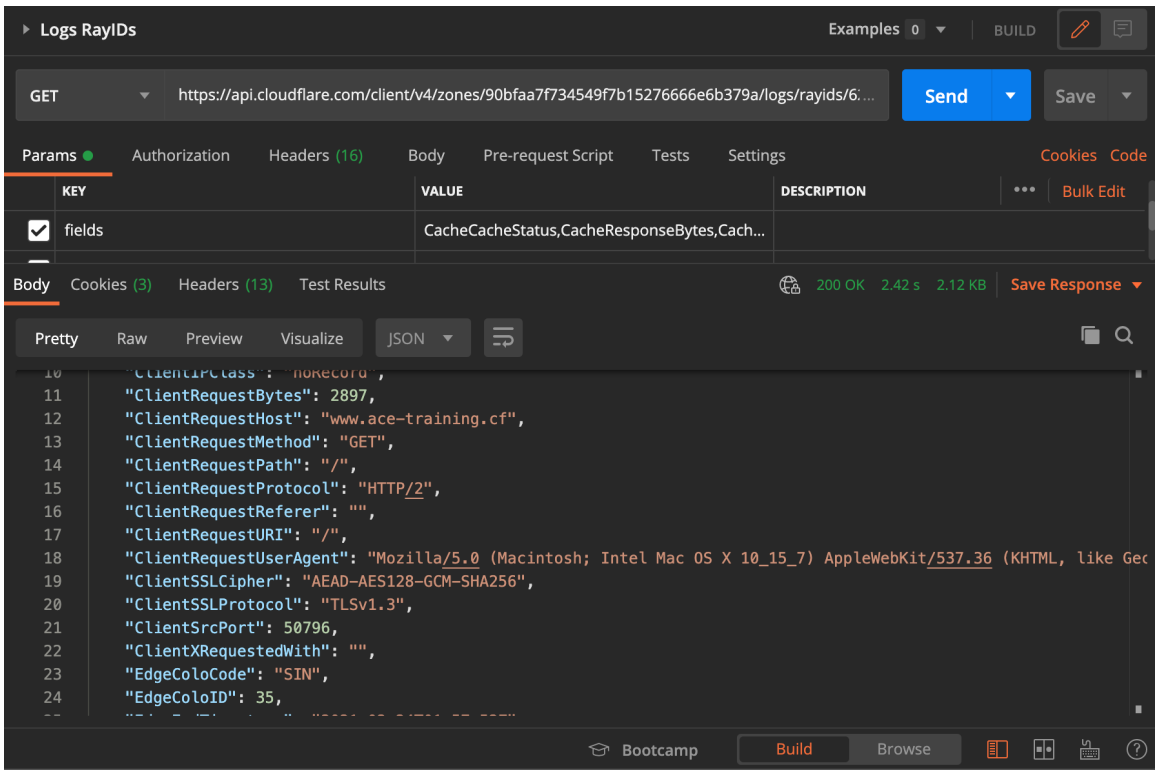


3. Open Google HAR Analyzer, open the HAR file you have just saved.

▼ Retrieve Logs with RayID

`RayID` is Cloudflare's identifier of a request. Use RayID to retrieve detailed information of a request.

1. rayId: Find one RayID you would like to inspect
2. zoneName: `yourdomain.cf`
3. Guidance and example: here
4. Hint: Start from a readymade query
5. Log fields and its meaning: https://developers.cloudflare.com/logs/log-fields

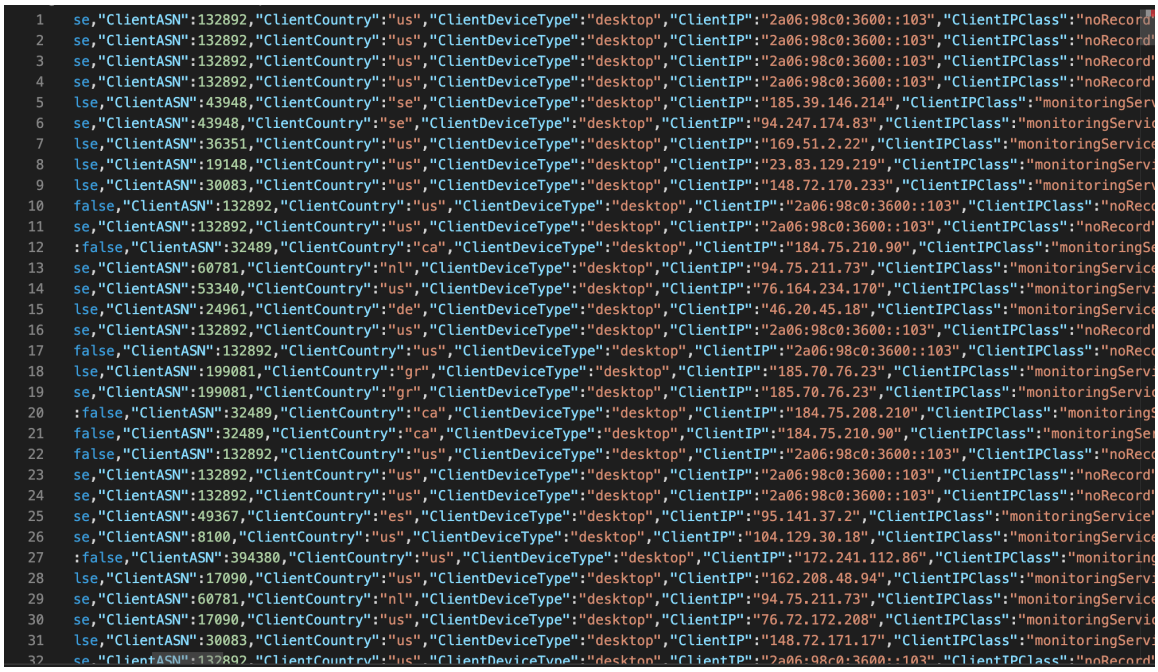


Easier and quicker with POSTMAN.

▼ Get All Logs for the Last 1 Hour

Try to use timestamp to download all logs of a Cloudflare ENT zone within specific time range.

1. zoneName: `yourdomain.cf`
2. time_start: Use this format `2021-02-25T03:00:00Z`
3. time_end: Use this format `2021-02-25T04:00:00Z`
4. Guidance and example: here
5. Hint: Start from a readymade query
6. Log fields and its meaning: https://developers.cloudflare.com/logs/log-fields

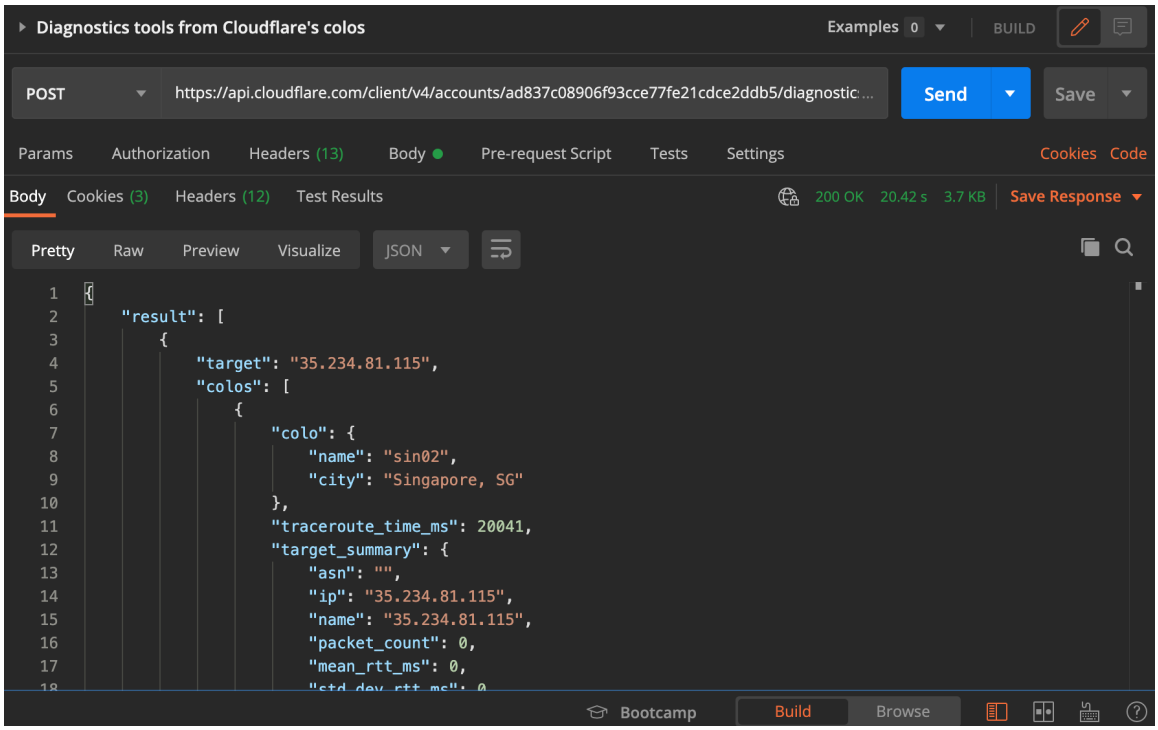


Easier and quicker with POSTMAN.

▼ Traceroute from Cloudflare colo

If the feature is enabled, you can use API to run traceroute from specific Cloudflare data center to the origin server.

1. Access https://api.cloudflare.com/#diagnostics-properties
2. Try running a diagnostics to: `35.234.81.115` from: `SIN02`.
3. Hint: Account ID can be found in dashboard overview or at the address line.



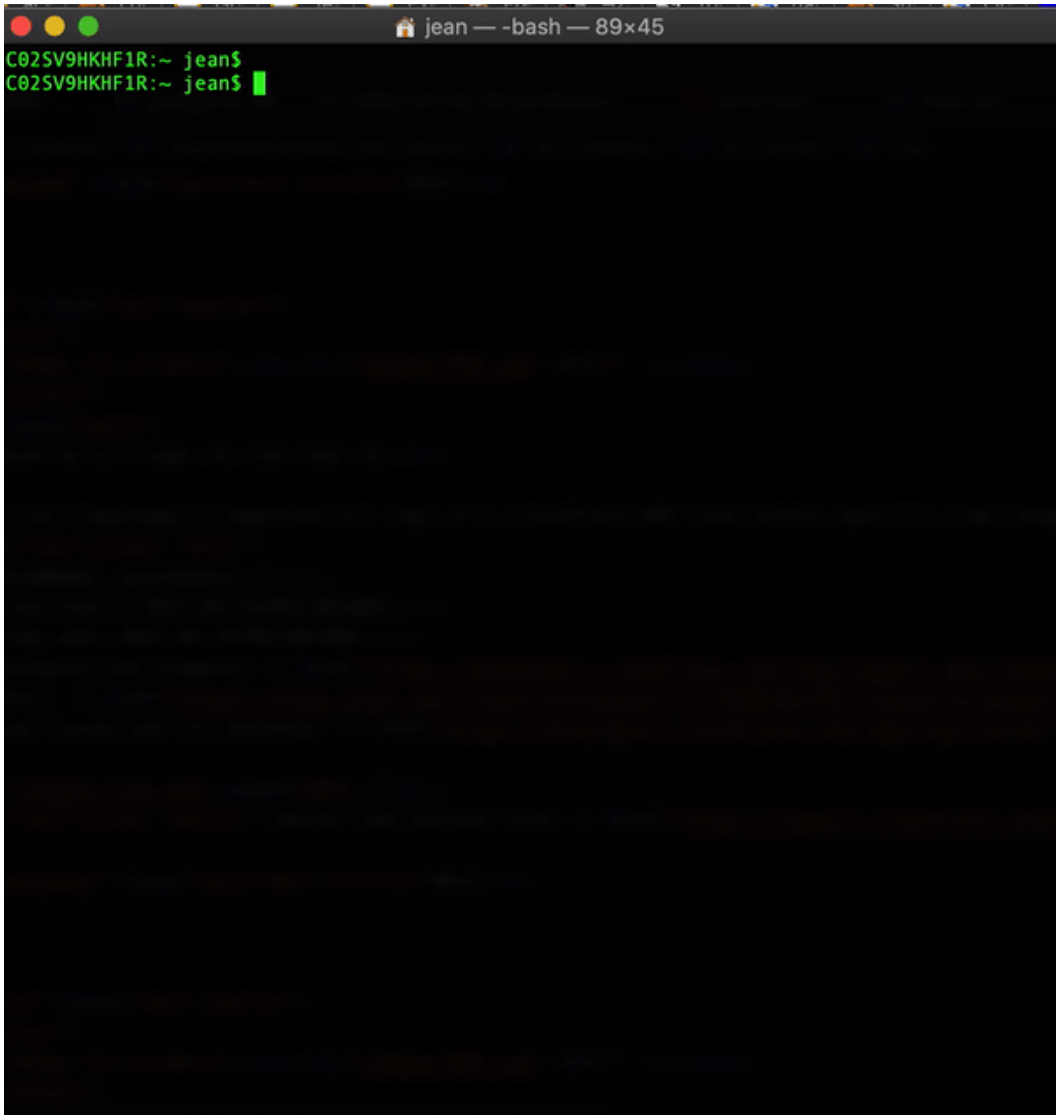
Easier and quicker with POSTMAN.

▼ Play more with curl

Directly send request to origin, repeat cURL 50 times to confirm intermittent error, send specific headers, etc.

```
for i in {1..50}; do curl -svo /dev/null/ "https://www.cloudflare.com?x=${i}" 2>&1 | grep -Ei "< HTTP|<
Date|< CF-Cache-Status|< CF-RAY|< Server"; printf "\n\n"; done;
```

```
curl -o /dev/null -D- -k -s -v -w '%{url_effective} CODE:%{http_code} \n -- DNS:%{time_namelookup} \n -
- Connect:%{time_connect} \n -- TTFB:%{time_starttransfer} \n -- Time_Pretransfer:%{time_pretransfer}
 \n -- Time_Redirect:%{time_redirect} \n -- Time_Start_Transfer:%{time_starttransfer} \n -- TOTAL Tim
e:%{time_total}\n -- Size_download:%{size_download} \n' "https://cloudflare.com"
```



💥 Troubleshooting Summary

▼ Click to view

- **Initial t/s investigation checkpoints:**
  1. Health checks
  2. CF-Origin response codes cross check (cURL)
  3. Confirm logs of the corresponding RayID
  4. Change logs (audit logs) of the problematic time
  5. Check `cloudflarestatus.com`
  6. Save cdn-cgi and HAR
- **Still can’t find the root cause? Send SOS to the below contact:**

1. Customer issue: `entsupport@cloudflare.com`
2. Partner issue: `partnersupport@cloudflare.com`
3. 💡 IMPORTANT: Share the initial t/s result. It will save time!
4. 💡 IMPORTANT: Need to contact support from the right legitimate email.

Take the ACE Exam

Once you completed the training, take the ACE certification at the Cloudflare partner portal.

Successful candidates who passed ACE can take further steps and attend Accredited Services Architect coursework.

Take Home Assignments

Do you want to get hands-on yourself and ensure you are comfortable with Cloudflare implementation?

Please complete the below technical assignments. Please contact your partner SE (APAC: jean@cloudflare.com) if you have any questions!

▼ **Click to view the assignment**

Aa Assignment	Requirements	Reference	Verification
Onboarding	Implement Cloudflare so the following hosts are accessible via Cloudflare: `https://web.yourdomain.com/` `https://api.yourdomain.com/` `https://admin.yourdomain.com/`, and `ssh.yourdomain.com` You can use full setup or CNAME setup, as you like.		
Untitled	Protect the web services at `80/443`, and SSH service at `22`.		
Untitled	Make sure nmap test says the origin doesn't have `22/80/443` opened.		
Untitled	Make sure an email alert will be sent when the origin is not reachable from Cloudflare.		
Untitled	Make sure `web.yourdomain.com` has the following HA set up: All visitors will be routed to the primary origin. But once the primary origin is not reachable, it will fall back to the backup origin (`35.234.81.115`)		
Security	Any requests over HTTP needs to be redirected to HTTPS.		
Untitled	Make sure there's no path of HTTP traffic flows unencrypted.		
Untitled	Make sure you use Cloudflare's WAF and IP Intelligence.		

Assignment	Requirements	Reference	Verification
Untitled	Make sure you block anyone who sends more than 600 requests in a minute. Blocking time is 5 minutes.		
Untitled	Site Rule: `admin.yourdomain.com` should NOT allow any requests without the following request header 'admin: true'		
Untitled	Site Rule: `admin.yourdomain.com` should NOT allow any external access other than my own IP		
Untitled	Site Rule: `api.yourdomain.com` should NOT use Cloudflare's WAF and IP intelligence.		
Untitled	Site Rule: Anyone who accesses `web.yourdomain.com/country.html` from anywhere but your country or residence, should firstly pass JS Challenge.		
Performance	Check the current cache TTL and change it to 7 days.		
Untitled	Cache the front page for 1 minute.		
Untitled	Optimize the content as much as possible. Compress the images and codes.		
Untitled	What other settings do you need to enable to make the site faster? Find and enable them. (Hint: Refer to optimization training)		
API and Troubleshooting	Set the WAF in "Detection-only" mode.		
Untitled	Set up Logpush for HTTP Request, and Spectrum Events.		
Untitled			