

Name: Nayan Rajani

Organization: Blazeclan Technologies

E-mail: nayan.rajani@blazeclan.com

Assignment: ACE+

1.

Create a simple website, running on 2 origin web servers (Pending)

OCT application team would like to use Cloudflare for 2 applications:

web.<domain.com>

app.<domain.com>

endpoint returns all HTTP request headers in the body of http response?





Are both the sub domain to be pointing to same origin web servers? Or should web point to one server and app point to another one? Do we need to configure staging for each domain? Should health check be added?

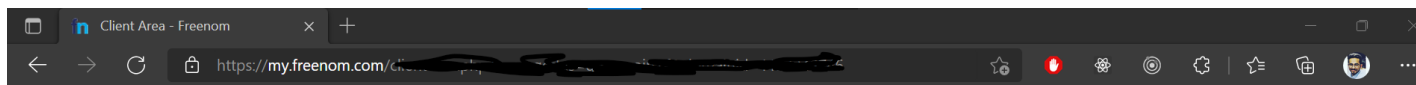
2. DNS/SSL

2.A Deploy a ECDSA origin cert on the origin and secure the communication between Cloudflare and the origin using SSL Full (Strict) mode

DNS Configurations!!

DNS

DNS management for greencoin.cf					
+ Add record		<input type="text" value="Search DNS Records"/>			Advanced
Type	Name	Content	Proxy status	TTL	
A	app	35.234.81.115	 Proxied	Auto	Edit ▶
A	staging	35.234.81.115	 Proxied	Auto	Edit ▶
A	web	35.234.81.115	 Proxied	Auto	Edit ▶
A	www	35.234.81.115	 Proxied	Auto	Edit ▶



[« Back to domain details](#)

Modify Records

Name	Type	TTL	Target	
APP	CNAME	300	app.greencoin.cf.cdn.cloudflare.net	Delete
STAGING	CNAME	300	staging.greencoin.cf.cdn.cloudflare.net	Delete
WEB	CNAME	300	web.greencoin.cf.cdn.cloudflare.net	Delete
WWW	CNAME	300	www.greencoin.cf.cdn.cloudflare.net	Delete
CLOUDFLARE-VERIFY	TXT	300	316332963-495648367	Delete

[Save Changes](#)

Add Records

1. Configuring the origin using SSL Full (Strict) mode
Path: Dashboard -> SSL/TLS Overview -> Change

Overview | SSL/TLS | greencoin.cf

Cloudflare Blazeclan - Partner Dem... greencoin.cf

SSL/TLS Overview

✓ Your SSL/TLS encryption mode is Full

Browser → Cloudflare → Origin Server

- ☐ Off (not secure) ⓘ
No encryption applied
- ☐ Flexible
Encrypts traffic between the browser and Cloudflare
- ☒ **Full**
Encrypts end-to-end, using a self signed certificate on the server
- ☐ Full (strict)
Encrypts end-to-end, but requires a trusted CA or Cloudflare Origin CA certificate on the server
- ☐ Strict (SSL-Only Origin Pull)
Same as Full (strict), but ensures that the request to the origin is always encrypted

[Help](#)

2. Deploy a ECDSA origin cert on the origin
Path: Dashboard -> Origin Server -> Origin Certificate -> Create Certificate

SSL/TLS

Origin Server

Origin Certificates

Generate a free TLS certificate signed by Cloudflare to install on your origin server.

Origin Certificates are only valid for encryption between Cloudflare and your origin server.

Create Certificate

Hosts	Expires On		
*.greencoin.cf, greencoin.cf (2 hosts)	Mar 7, 2022	Download	Revoke

[Help ▶](#)

- After this Copy your Certificate and Private key in any format, I have chosen PEM format, then click on ok.

3. Install Origin CA certificate on origin server?

- <https://developers.cloudflare.com/ssl/origin-configuration/origin-ca>

2.B Describe the difference between SSL mode Flexible, Full and Full (strict)

- CloudFlare provides free CDN and also it provides free SSL. When adding SSL there will be five options like i) off ii) Flexible iii) Full iv) Full (Strict) v) Strict (SSL-only Origin Pull)

I. Flexible:

- There will be certificates between User and CloudFlare. No Certificates Between CloudFlare and Server.
- Edge to origin not encrypted
- Self-signed certificates are not supported



II. Full:

- There will be certificates between User and CloudFlare. There will be Certificates Between Cloudflare and Server
- Edge to origin certificates can be self-signed



III. Full (strict)-> Recommended

- f. Encrypts end-to-end
- g. Requires a trusted CA or Cloudflare Origin CA certificate
- h. Strong certificates between User and CloudFlare. Strong Certificates Between CloudFlare and Server.



2.C Bonus (1 point): deploy a custom vanity NS server on your zone

<https://support.cloudflare.com/hc/en-us/articles/200169006-Setting-up-Custom-Nameservers-at-Cloudflare>

3. Firewall

3 A. Enable both the Cloudflare Managed Rulesets and the OWASP ruleset on the entire zone. Set OWASP threshold to low, with PL4 Paranoia level

Wait for this!! Upgrade is in progress

3.B. Create a Firewall Rule to block request to `app.greencoin.cf/admin` from any IP in Singapore, unless that request contains a cookie: `"cf_bypass=true"`

Firewall Rules | Firewall | greenco... x NayanRajani-BlazeclanTechnolo... x ACE+ Exam Guide_Nov2021v5.p... x +

https://dash.cloudflare.com/.../greencoin.cf/firewall/firewall-rules...

CLOUDFLARE Blazeclan - Partner Dem... greencoin.cf

Add site Support English (US)

Firewall Rules

[← Back to rules list](#)

Edit Firewall Rule

Rule name
Give your rule a descriptive name

When incoming requests match...

Field	Operator	Value	
URI Path	contains	app.greencoin.cf/admin/*	And X
And			
Country	equals	Singapore	And X
And			
Cookie	does not equal	cf_bypass=true	And Or X

Expression Preview [Edit expression](#)

```
(http.request.uri.path contains "app.greencoin.cf/admin/*" and ip.geoip.country eq "SG" and http.cookie ne "cf_bypass=true")
```

Then... [About Firewall Actions](#)

Choose an action
 [Test rule](#)

[Help](#)

3.C. Create a Firewall Rule to allow requests going to the app.greencoin.cf/admin to bypass WAF Managed Rulesets and Rate Limiting

Firewall Rules | Firewall | greenco... x NayanRajani-BlazeclanTechnolo... x ACE+ Exam Guide_Nov2021v5.p... x +

https://dash.cloudflare.com/.../greencoin.cf/firewall/firewall-rules...

CLOUDFLARE Blazeclan - Partner Dem... greencoin.cf

Add site Support English (US)

Firewall

Firewall Rules

[← Back to rules list](#)

Edit Firewall Rule

Rule name
Give your rule a descriptive name

When incoming requests match...

Field	Operator	Value	
URI Path	contains	app.greencoin.cf/admin/*	And Or

Expression Preview [Edit expression](#)

```
(http.request.uri.path contains "app.greencoin.cf/admin/*")
```

Then... [About Firewall Actions](#)

Choose an action [Choose a feature](#)

[Test rule](#)

[Help](#)

4. Performance (30 points)

4.A. Ensure that all static html pages are cached at Cloudflare edge for 1 day

How to identify all static pages?

The screenshot shows the Cloudflare dashboard interface. At the top, there's a navigation bar with the Cloudflare logo and the text 'Blazeclan - Partner Dem...'. Below this, there's a breadcrumb trail: 'Page Rules' > 'Transform Rules'. The main heading is 'Rules' with a sub-heading 'Page Rules'. A link to '← Back' is visible. The title of the configuration is 'Edit Page Rule for greencoin.cf'. A note states: 'If the URL matches: By using the asterisk (*) character, you can create dynamic patterns that can match many URLs, rather than just one. All URLs are case insensitive. [Learn more](#)'. The input field for the URL pattern contains '*.greencoin.cf/static/*.html'. Below this, a section titled 'Then the settings are:' contains two rows of settings. The first row has 'Cache Level' set to 'Cache Everything'. The second row has 'Edge Cache TTL' set to 'a day'. There are 'X' icons to remove each setting. A '+ Add a Setting' button is below these. At the bottom are 'Cancel' and 'Save' buttons. A 'Help' button is in the bottom right corner.

Page Rules | Rules | greencoin.cf

https://dash.cloudflare.com/greencoin.cf/rules/form

Cloudflare

Blazeclan - Partner Dem... greencoin.cf

Add site Support English (US)

Page Rules Transform Rules Settings

Rules

Page Rules

[← Back](#)

Edit Page Rule for greencoin.cf

If the URL matches: By using the asterisk (*) character, you can create dynamic patterns that can match many URLs, rather than just one. All URLs are case insensitive. [Learn more](#)

Then the settings are:

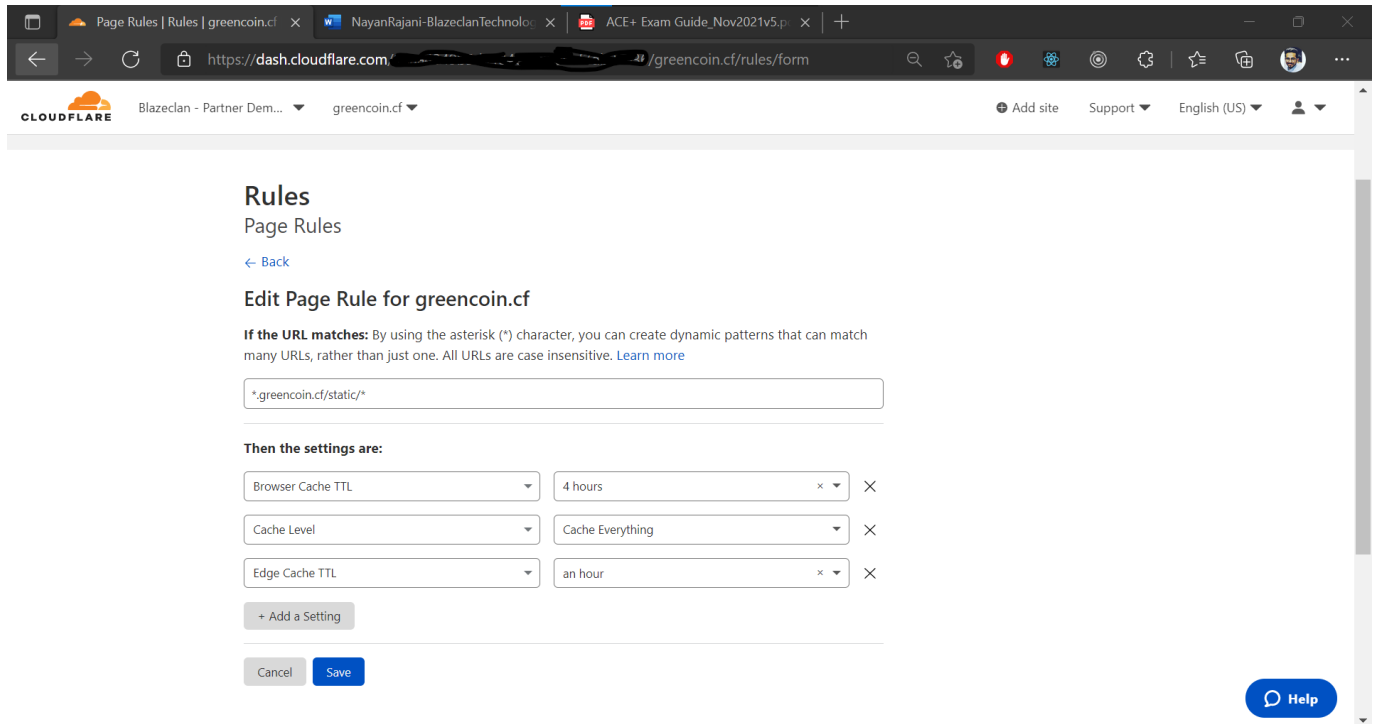
Cache Level	Cache Everything	X
Edge Cache TTL	a day	X

[+ Add a Setting](#)

[Cancel](#) [Save](#)

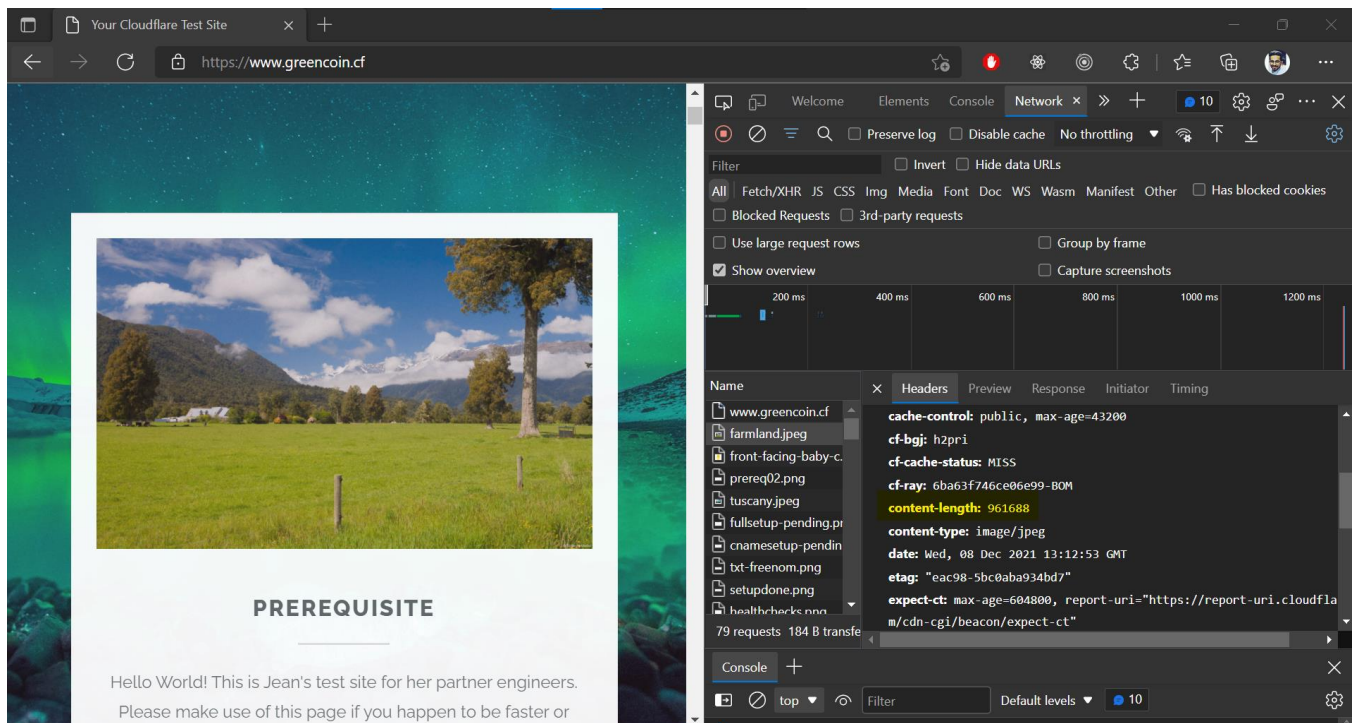
[Help](#)

4.B. Ensure that all static files under /static directory should be cached at Cloudflare edge for 1 hour and in browser for 4 hours



4.C. Turn on webp conversion for pictures on Cloudflare and do a size comparison of both version of the picture, with and without webp

Before WebP-> Content-length: 961688



After WEBP->

Cloudflare Optimization | Speed | greencoin.cf

Polish

Improve image load time by optimizing images hosted on your domain. Optionally, the WebP image codec can be used with supported clients for additional performance benefits.

Note: Purge cache to have your change take effect immediately.

This setting was last changed 2 hours ago

WebP

Auto Minify

Reduce the file size of source code on your website.

JavaScript

CSS

Help

greencoin.cf

DAY 3 START
TURN ON THE LOG

Network

Filter

Has blocked cookies

Blocked Requests

3rd-party requests

200 ms 400 ms 600 ms 800 ms 1000 ms 1200 ms

Name

www.greencoin.cf

farmland.jpeg

front-facing-baby-chick_1f42

prereq02.png

tuscany.jpeg

fullsetup-pending.png

80 requests 264 B transferred

Headers

cf-bj: img:85,h2pri

cf-cache-status: HIT

cf-polished: degrade=85, origSize=961688

cf-ray: 6ba66934ea622e46-BOM

content-length: 566176

content-type: image/jpeg

date: Wed, 01 Dec 2021 13:41:23 GMT

Console

What's New

Highlights from the Chrome 96 update

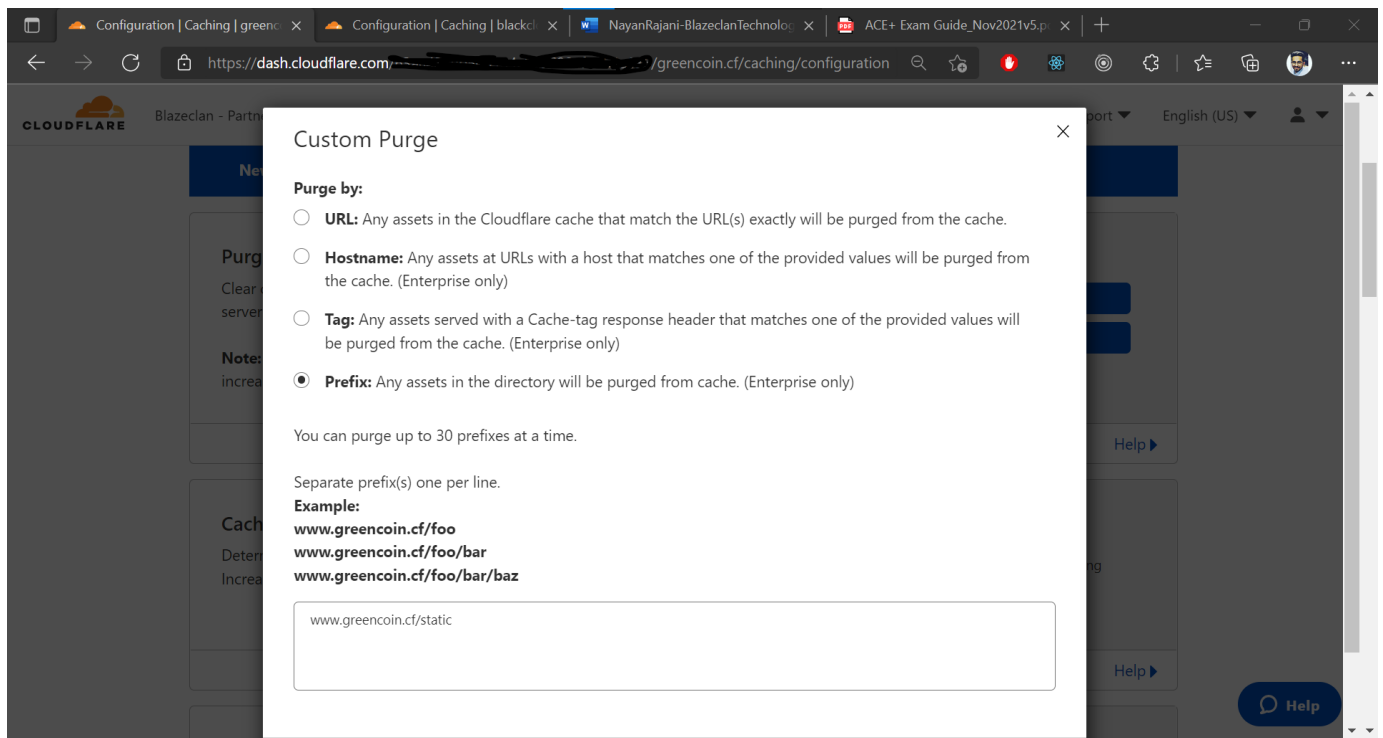
New preview feature: CSS Overview panel

Use the CSS overview panel to identify CSS improvements on your page.

Enable emulating prefers-contrast media and auto dark mode

Emulate the user preference on using a different contrast

4.D. Show the steps to purge all cache under the folder app.greencoin.cf/static



4.E.

need to create site? One page rule? same cache HIT?

5. User Administration & Log Analytics (5 points)

User Administration:

A. Show the screenshot where you can check which account member changed any Cloudflare configuration

Audit Log

Nov 7, 2021 → Dec 7, 2021 [Download CSV](#)

User: Domain:

Date	Action	User	Domain
Dec 7, 2021	Crypto change setting	uday.gidge@blazeclan.com	extensia.cf
Dec 7, 2021	Deployed	Cloudflare	extensia.cf
Dec 7, 2021	Ordered	Cloudflare	extensia.cf
Dec 7, 2021	Set custom error page	nayan.rajani@blazeclan.com	greencoin.cf

[Help](#)

B. Show the screenshot where you personalize any block and error pages for your domain

Custom Pages

Personalize the error and challenge pages that Cloudflare presents to your visitors.

IP/Country Block

Customize the error page shown to your visitors when they visit from a blocked IP address or country.

[Custom Pages](#)

WAF Block

Customize the error page presented to your visitors when they trigger a Web Application Firewall rule.

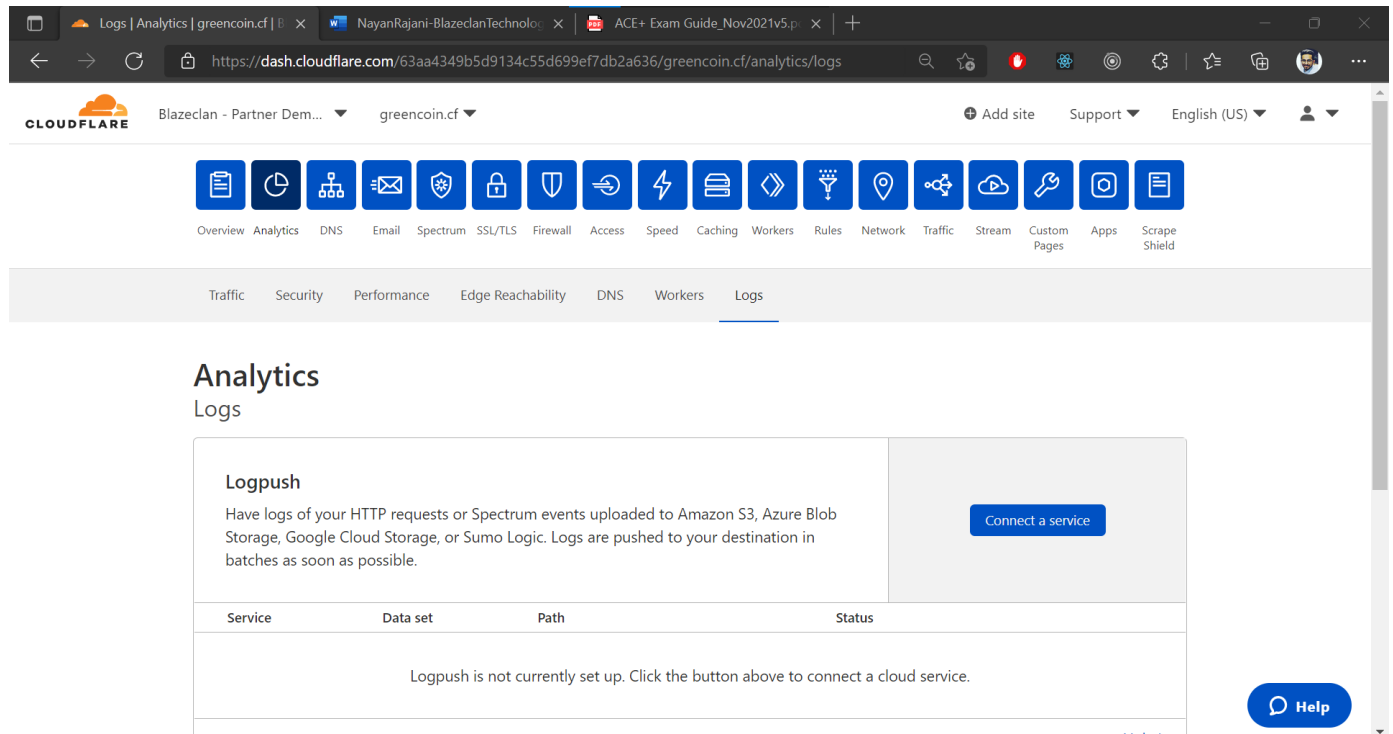
[Custom Pages](#)

[API](#) [Help](#)

[Help](#)

Logs and Analytics

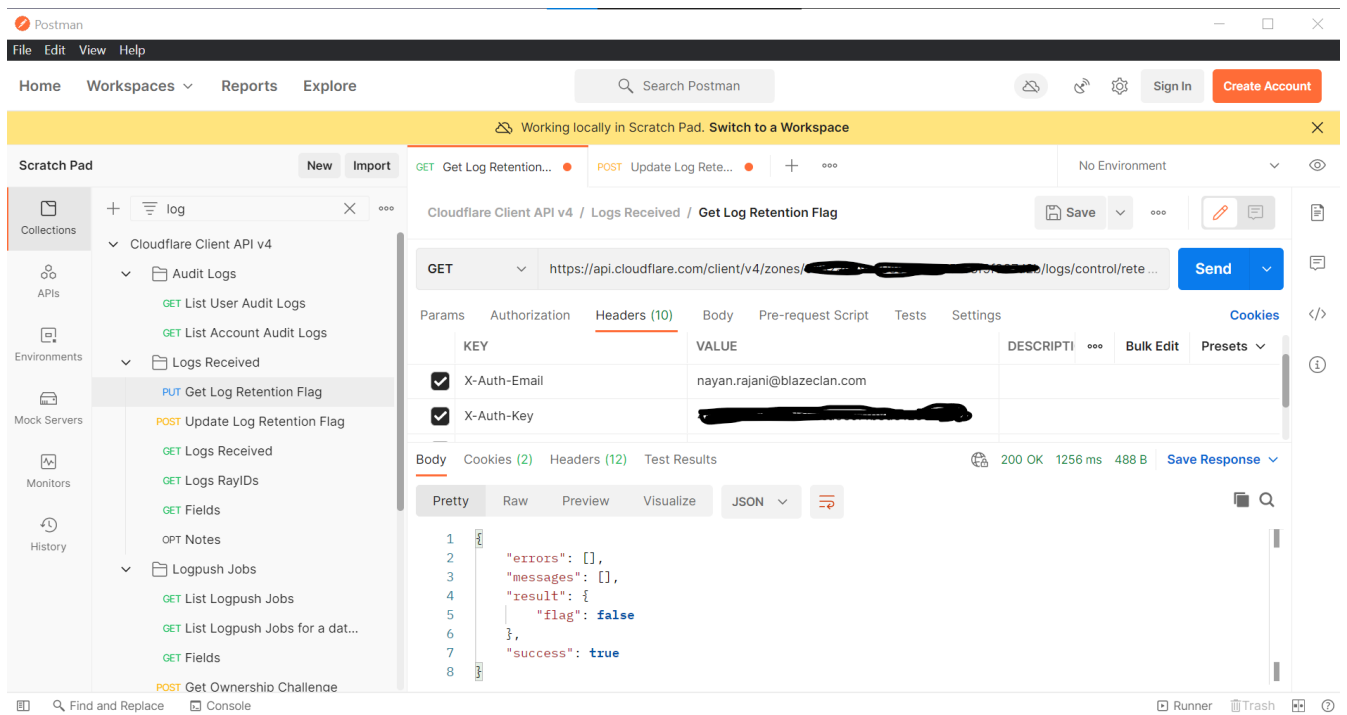
C. Show the screenshot to set up Logpush jobs to any Logpush target for HTTP requests, Audit Log and Firewall events



D. Show the screenshot of Postman or curl to run API call and output to turn on Logpull for your zone.

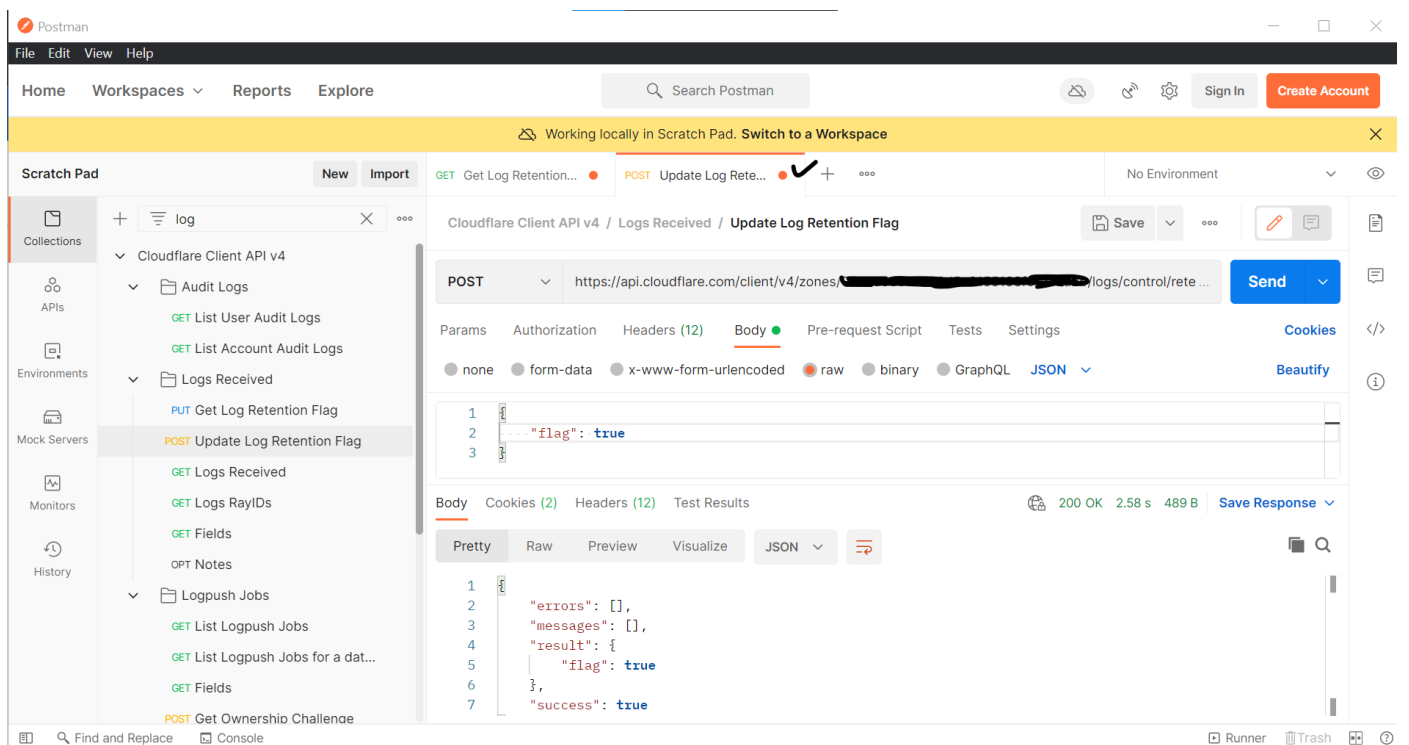
GET- <https://api.cloudflare.com/client/v4/zones/<ZONEID>/logs/control/retention/flag>

Header- Email and API token (Global)



POST- <https://api.cloudflare.com/client/v4/zones/<ZONEID>/logs/control/retention/flag>

Body- {"flag": true}



E. Show the screenshot of Postman or curl to run API call to download your log for the previous 1 hour using Logpull, while redacting your authentication key

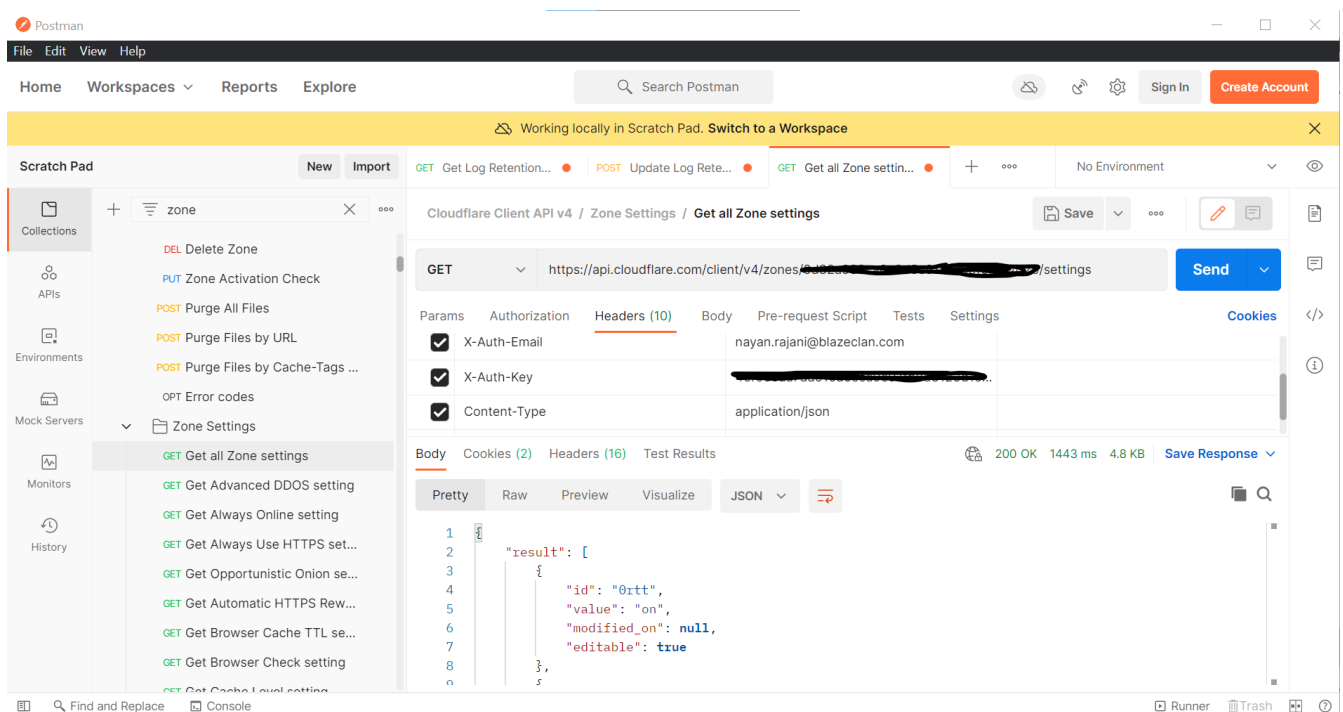
```

Command- curl -s -H "X-Auth-Email: nayan.rajani@blazeclan.com" -H "X-Auth-Key:
4ef065aa7da010a6eca9e97fb8d3123d1efbf"
"https://api.cloudflare.com/client/v4/zones/0d32a989ca0e8d5e9155163f9f937d2b/logs/received?start
=2021-12-04T14:17:06Z&end=2021-12-04T15:17:06Z&fields=$(curl -s -H "X-Auth-Email:
nayan.rajani@blazeclan.com" -H "X-Auth-Key: 4ef065aa7da010a6eca9e97fb8d3123d1efbf"
"https://api.cloudflare.com/client/v4/zones/0d32a989ca0e8d5e9155163f9f937d2b/logs/received/fields
" | jq '. | to_entries[] | .key' -r | paste -sd "," -)&timestamps=RFC3339"

```

6. Client API (15 points)

6. A. Using Postman, GET the JSON response of the zone settings of your zone



Response->

```

{"result":[{"id":"0rtt","value":"on","modified_on":null,"editable":true},{"id":"advanced_ddos","value":"on",
,"modified_on":null,"editable":false},{"id":"always_online","value":"on","modified_on":null,"editable"
:true},{"id":"always_use_https","value":"on","modified_on":"2021-12-
06T16:37:58.302853Z","editable":true},{"id":"automatic_https_rewrites","value":"off","modified_on":n
ull,"editable":true},{"id":"brotli","value":"on","modified_on":"2021-12-
07T04:19:11.732723Z","editable":true},{"id":"browser_cache_ttl","value":14400,"modified_on":null,"ed
itable":true},{"id":"browser_check","value":"on","modified_on":null,"editable":true},{"id":"cache_level"
,"value":"aggressive","modified_on":"2021-12-
07T07:31:33.874056Z","editable":true},{"id":"challenge_ttl","value":1800,"modified_on":null,"editable"
:true},{"id":"ciphers","value":[],"modified_on":null,"editable":true},{"id":"cname_flattening","value":"fla
tten_at_root","modified_on":null,"editable":true},{"id":"development_mode","value":"off","modified_o
n":null,"editable":true},{"id":"early_hints","value":"off","modified_on":null,"editable":true},{"id":"edge_

```

```

cache_ttl","value":7200,"modified_on":null,"editable":true},{
  "id":"email_obfuscation","value":"on","modified_on":null,"
  editable":true},{
  "id":"filter_logs_to_cloudflare","value":"off","modified_on":null,"
  editable":true},{
  "id":"hotlink_protection","modified_on":null,"value":"off","
  editable":true},{
  "id":"http2","value":"on","modified_on":null,"editable":true},
  {"id":"http3","value":"off","modified_on":null,"editable":true},
  {"id":"ip_geolocation","value":"on","modified_on":null,"
  editable":true},{
  "id":"ipv6","value":"on","modified_on":"2021-12-06T12:33:31.548757Z",
  "editable":true},{
  "id":"log_to_cloudflare","value":"on","modified_on":null,"
  editable":true},{
  "id":"max_upload","value":100,"modified_on":null,"editable":true},
  {"id":"min_tls_version","value":"1.0","modified_on":null,"
  editable":true},{
  "id":"minify","value":{"js":"on","css":"on","html":"on"},"
  modified_on":"2021-12-07T04:19:07.760373Z","editable":true},
  {"id":"mirage","value":"on","modified_on":"2021-12-07T04:19:37.882213Z",
  "editable":true},{
  "id":"mobile_redirect","value":{"status":"off","mobile_subdomain":null,
  "strip_uri":false},"modified_on":null,"editable":true},
  {"id":"opportunistic_encryption","value":"off","modified_on":null,
  "editable":true},
  {"id":"opportunistic_onion","value":"on","modified_on":null,"
  editable":true},
  {"id":"orange_to_orange","value":"off","modified_on":null,"
  editable":true},
  {"id":"origin_error_page_pass_thru","value":"off","modified_on":null,
  "editable":true},
  {"id":"polish","value":"lossy","modified_on":"2021-12-07T04:18:56.530269Z",
  "editable":true},
  {"id":"prefetch_preload","value":"off","modified_on":null,"
  editable":true},
  {"id":"privacy_pass","value":"on","modified_on":null,"
  editable":true},
  {"id":"proxy_read_timeout","value":"100","modified_on":null,"
  editable":true},
  {"id":"pseudo_ipv4","value":"off","modified_on":null,"
  editable":true},
  {"id":"response_buffering","value":"off","modified_on":null,"
  editable":true},
  {"id":"rocket_loader","value":"on","modified_on":"2021-12-07T04:19:34.891571Z",
  "editable":true},
  {"id":"security_header","modified_on":null,"value":{"strict_transport_security":{"enabled":false,
  "max_age":0,"include_subdomains":false,"preload":false,"nosniff":false}},
  "editable":true},
  {"id":"security_level","value":"medium","modified_on":null,"
  editable":true},
  {"id":"server_side_exclude","value":"on","modified_on":null,"
  editable":true},
  {"id":"sort_query_string_for_cache","value":"off","modified_on":null,
  "editable":true},
  {"id":"ssl","value":"full","modified_on":null,"certificate_status":"none",
  "validation_errors":[],"editable":true},
  {"id":"tls_1_2_only","value":"off","modified_on":null,"
  editable":true},
  {"id":"tls_1_3","value":"zrt","modified_on":null,"
  editable":true},
  {"id":"tls_client_auth","value":"off","modified_on":null,"
  editable":true},
  {"id":"true_client_ip_header","value":"off","modified_on":null,"
  editable":true},
  {"id":"visitor_ip","value":"on","modified_on":null,"
  editable":true},
  {"id":"waf","value":"on","modified_on":"2021-12-06T16:39:54.550518Z",
  "editable":true},
  {"id":"webp","value":"on","modified_on":"2021-12-07T04:18:59.859169Z",
  "editable":true},
  {"id":"websockets","value":"on","modified_on":null,"
  editable":true}],
  "success":true,"errors":[],"messages":[]}

```

6.B Create an API token that can be used to purge cache at your domain only, valid for 1 week and can be executed from a device coming from your network only

Click to go back (Alt+Left arrow), hold to see history

SupportEnglish (US)

Give your API token a descriptive name.

Edit zone DNS

Permissions

Select edit or read permissions to apply to your accounts or websites for this token.

ZoneCache PurgePurge

+ Add more

Zone Resources

Select zones to include or exclude.

IncludeSpecific zonegreencoin.cf

+ Add more

Client IP Address Filtering

Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.

OperatorValue

Select...e.g. 192.168.1.88

+ Add more

TTL

Define how long this token will stay active.

Dec 8, 2021 → Dec 16, 2021

Help

←→↻https://dash.cloudflare.com/profile/api-tokens

CLOUDFLARESelect AccountAdd siteSupportEnglish (US)

PreferencesAuthenticationAPI TokensSessions

API Tokens

[← Edit token](#)

Edit zone DNS API token summary

This API token will affect the below accounts and zones, along with their respective permissions

Blazeclan - Partner Demo Account

greencoin.cf - **Cache Purge:Purge**

TTL

Start Date - **December 8, 2021**

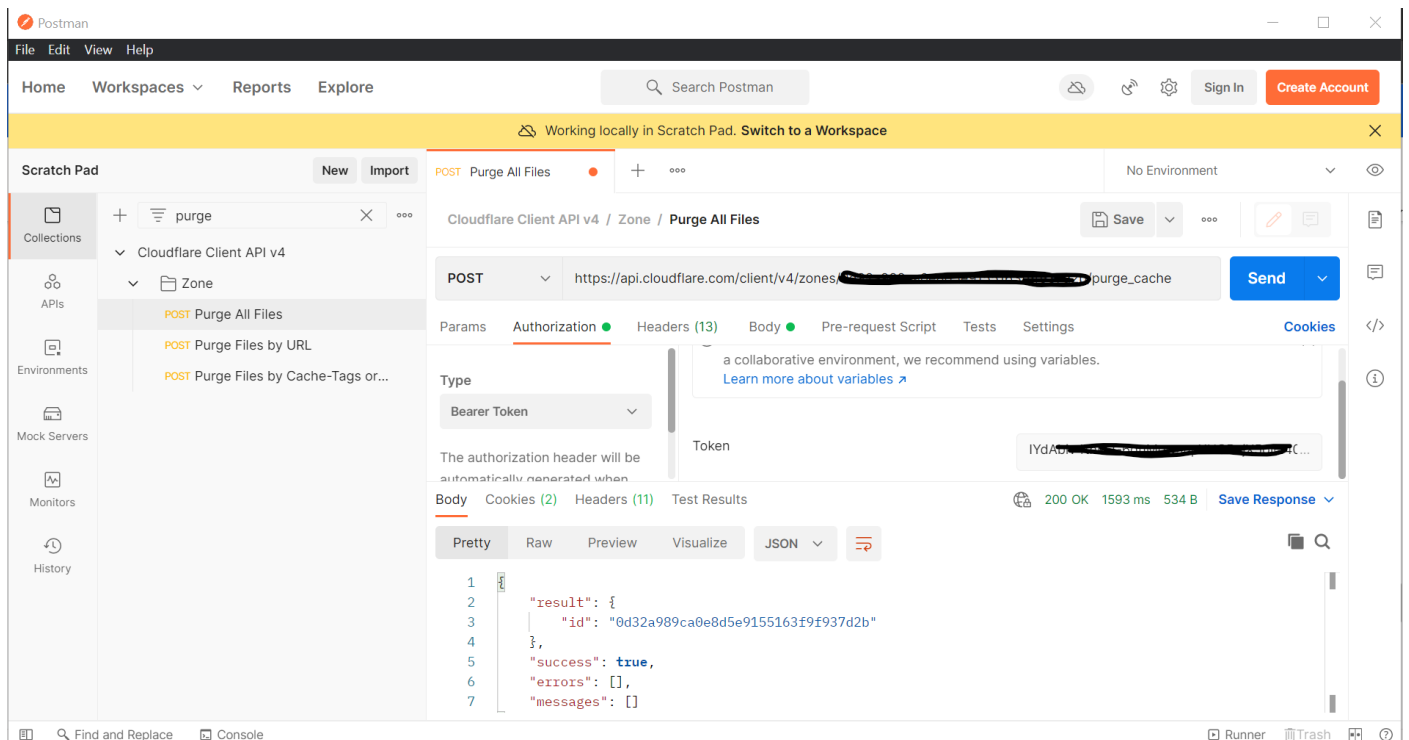
End Date - **December 16, 2021**

Cancel

Update token

Help

6. C. Run the API call to purge all the cache from Cloudflare edge using the above API token



Optional(s)

7. B. Turn on Tiered Caching and set it to Smart Tiered Caching Topology

