Generative AI and DNS
Own the Narrative

Pallavi Aras-Mathai

Agenda

Generative AI and DNS

- Context setting
- Experiment using Gen AI tools

Own the Narrative

- Conclusion
- Proposed Solution

DNS protocol knowledge

- IETF RFC documents
- Blogs like Cloudflare
- Mailing lists
- DNS Subject Matter Experts (SME)

Use cases for non-SME using DNS

Service Owners add CNAME or TXT

Domain ownership proof

- Google Sites

Cert issuance

- Domain control validation (DVC)

Service Owners add MX records to setup emails

Where do non-SMEs find DNS information?

Where do non-SMEs find DNS information?

Generative (Gen) Artificial Intelligence (AI)

Generative AI is the kind of AI you can use to create new text, visual, and audio content.[1]

Do GEN AI tools answer correctly???

Generative AI research experiment

Ask Gen AI tool, DNS related questions of increasing difficulty.

Verify answers against real world

Gen AI tools used in the research

Chat GPT

Meta AI

Gen AI research experiment

Questions -

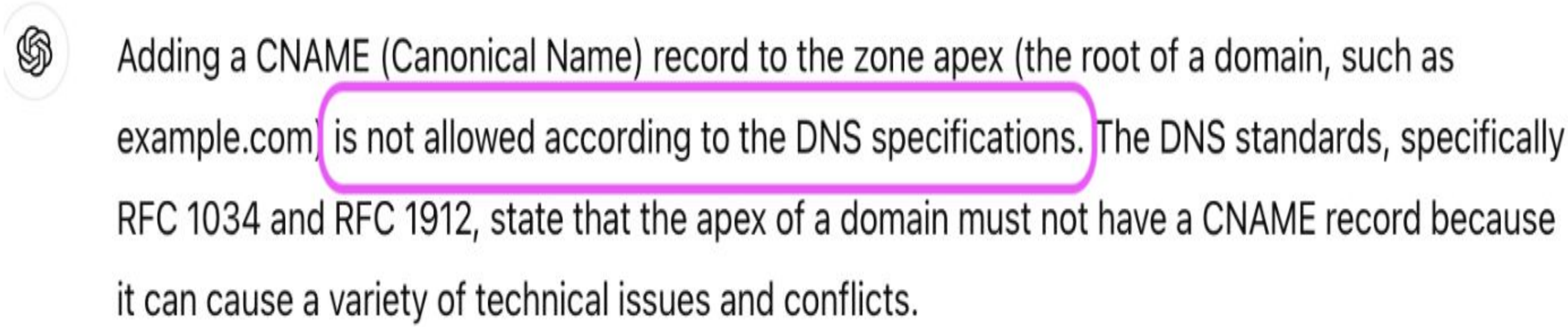
1. Can CNAME be added to zone apex?
2. How do wildcards resolve a DNS query?
3. How do you specify CAA for wildcard FQDN?

Question 1

Can CNAME be added to zone apex?

Can CNAME be added to zone apex?

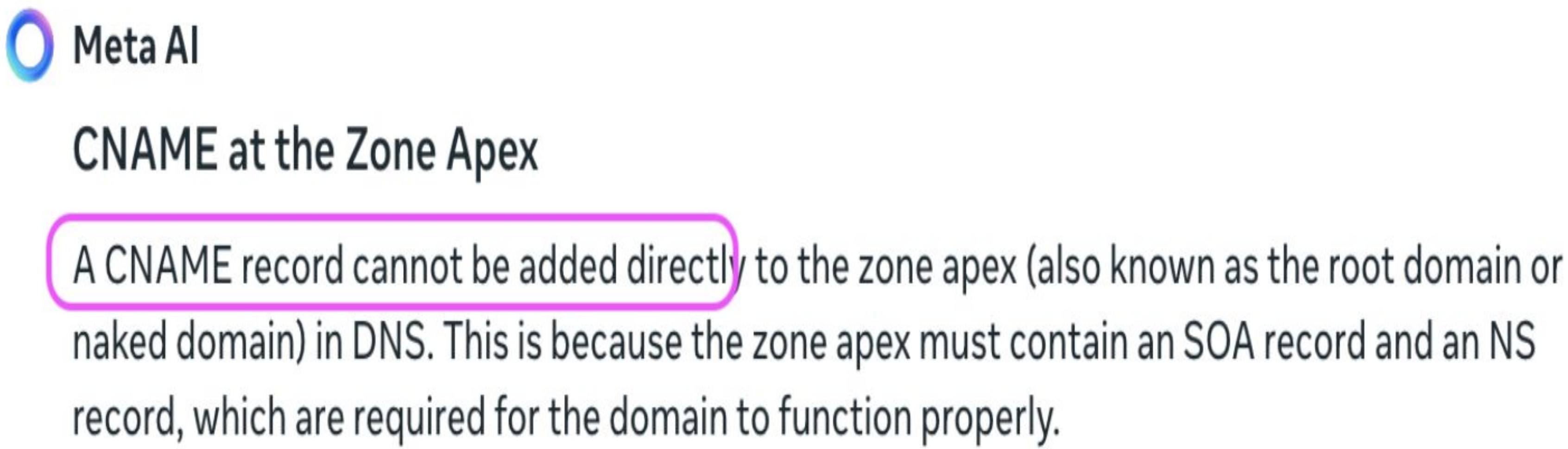
ChatGPT is Correct



Adding a CNAME (Canonical Name) record to the zone apex (the root of a domain, such as example.com) is not allowed according to the DNS specifications. The DNS standards, specifically RFC 1034 and RFC 1912, state that the apex of a domain must not have a CNAME record because it can cause a variety of technical issues and conflicts.

Can CNAME be added to zone apex?

Meta AI is Correct



Meta AI

CNAME at the Zone Apex

A CNAME record cannot be added directly to the zone apex (also known as the root domain or naked domain) in DNS. This is because the zone apex must contain an SOA record and an NS record, which are required for the domain to function properly.

Can CNAME be added to zone apex? - Reality

Correct answer

CNAME cannot be created at zone apex.

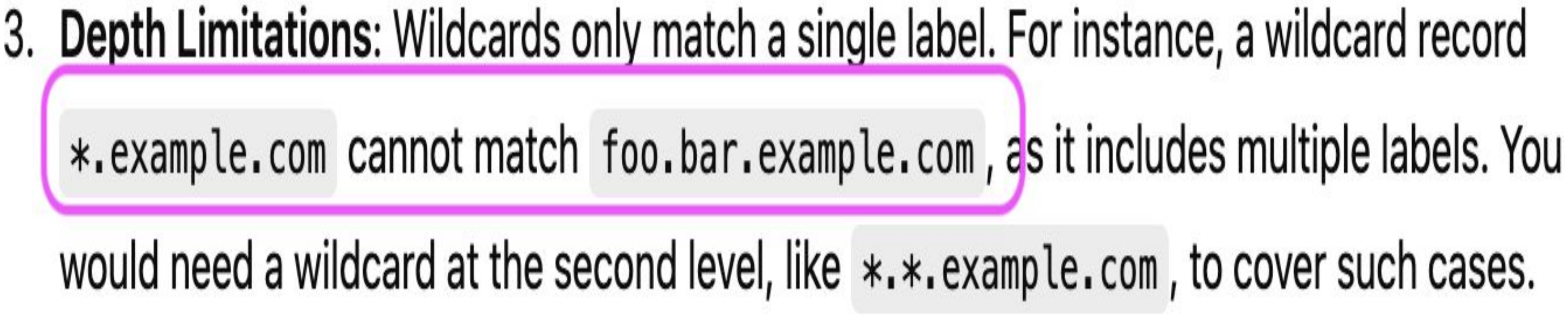
AI tools answered correctly

Question 2

How do wildcards resolve a DNS query?

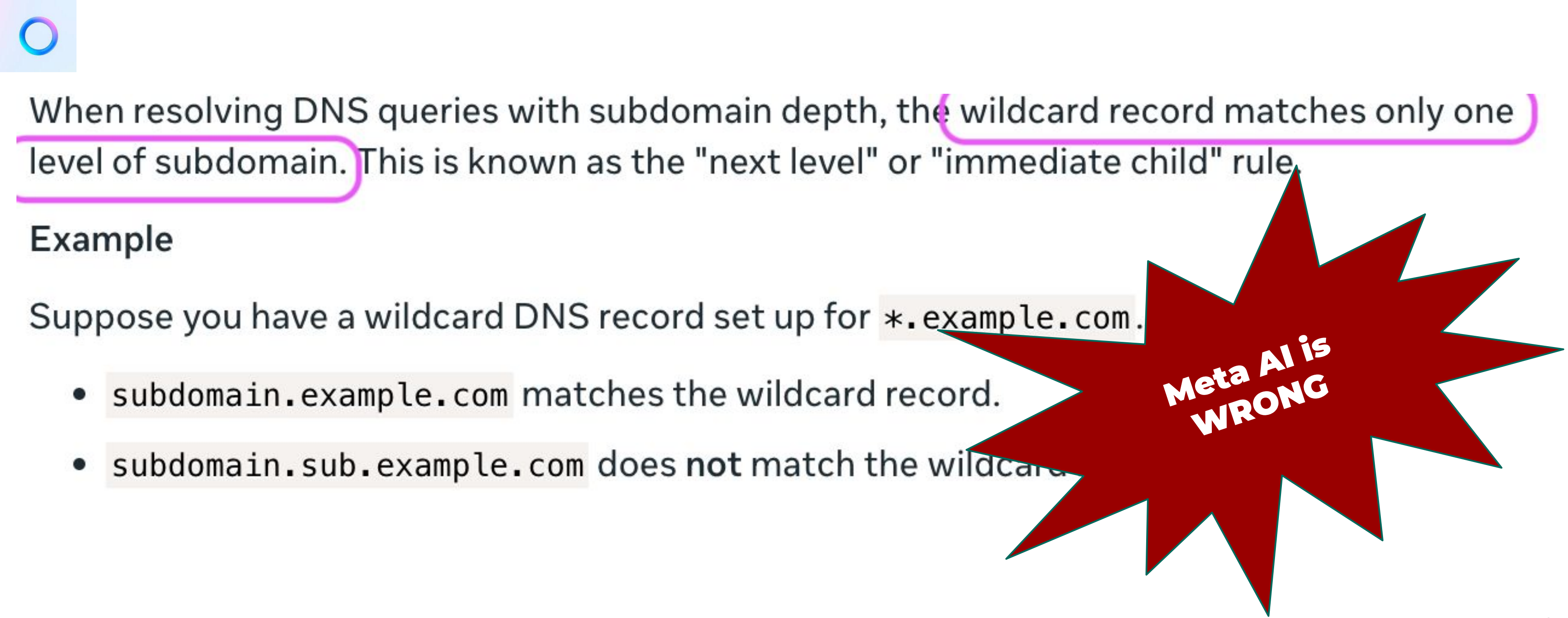
How do wildcards resolve a DNS query?

Chat GPT is WRONG



3. **Depth Limitations:** Wildcards only match a single label. For instance, a wildcard record `*.example.com` cannot match `foo.bar.example.com`, as it includes multiple labels. You would need a wildcard at the second level, like `*.*.example.com`, to cover such cases.

How do wildcards resolve a DNS query?



When resolving DNS queries with subdomain depth, the wildcard record matches only one level of subdomain. This is known as the "next level" or "immediate child" rule.

Example

Suppose you have a wildcard DNS record set up for `*.example.com`.

- `subdomain.example.com` matches the wildcard record.
- `subdomain.sub.example.com` does **not** match the wildca

How do wildcards resolve a DNS query? - Reality

```
% dig '*.pallavitest.com.' +short
testgoogle.pallavitest.com.
8.8.8.8
```

```
% dig 'label.pallavitest.com.' +short
testgoogle.pallavitest.com.
8.8.8.8
```

```
% dig 'label3.label2.label.pallavitest.com.' +short
testgoogle.pallavitest.com.
8.8.8.8
```

How do wildcards resolve a DNS query? - Reality

Correct answer:

Wildcard DNS record can resolve multi-label subdomains.

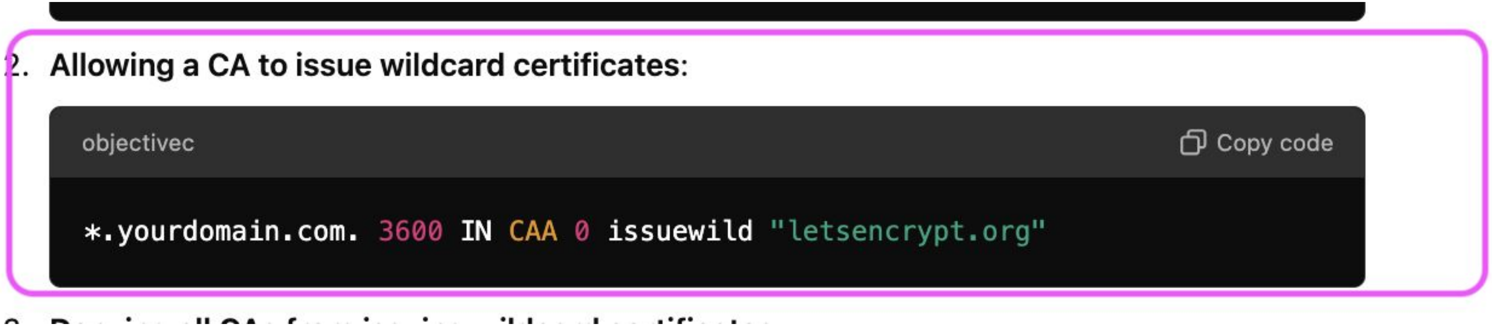
AI tools answers are WRONG

Question 3

How do you specify CAA for wildcard FQDN?

How do you specify CAA for wildcard FQDN?

Chat GPT is WRONG

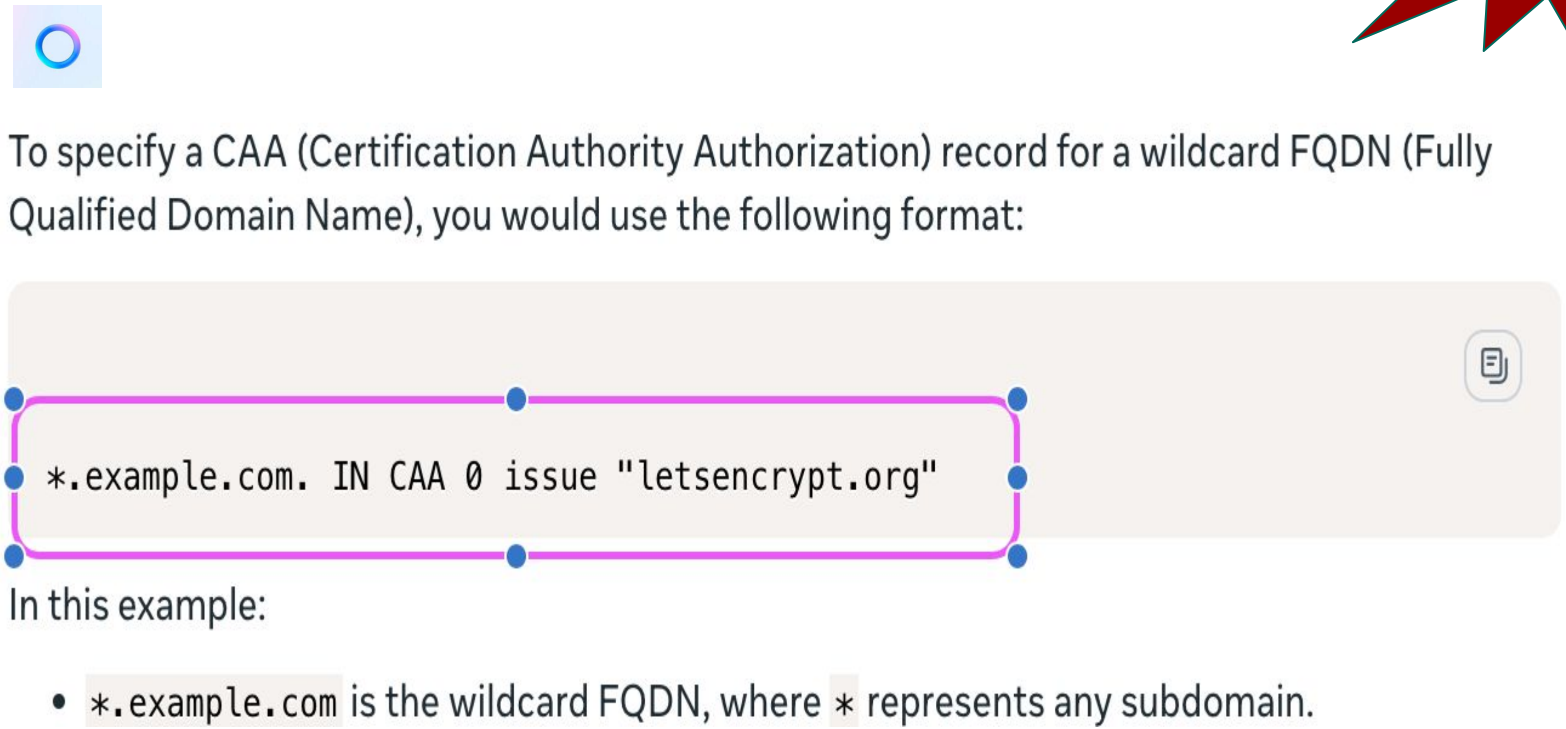


2. Allowing a CA to issue wildcard certificates:

```
*.yourdomain.com. 3600 IN CAA 0 issuewild "letsencrypt.org"
```

How do you specify CAA for wildcard FQDN?

Meta AI is WRONG



To specify a CAA (Certification Authority Authorization) record for a wildcard FQDN (Fully Qualified Domain Name), you would use the following format:

```
*.example.com. IN CAA 0 issue "letsencrypt.org"
```

In this example:

- `*.example.com` is the wildcard FQDN, where `*` represents any subdomain.

How do you specify CAA for wildcard FQDN? - Reality

RFC 8659 - DNS Certification Authority Authorization (CAA) Resource Record

Given a request for a specific FQDN X or a request for a Wildcard Domain Name *.X, the Relevant RRset RelevantCAASet(X)

AI tools answers are WRONG

Conclusion of the experiment

Responses of GenAI tools, cannot be trusted

Proposed Solution

DNSchat tool using **Retrieval Augmented Generation (RAG)**

Retrieval Augmented Generation (RAG)

Retrieval Augmented Generation (RAG) is an architecture that augments the capabilities of a Large Language Model (LLM) like ChatGPT by adding an information retrieval system that provides grounding data. [2]

DNSchat tool - Proof of Concept (PoC)

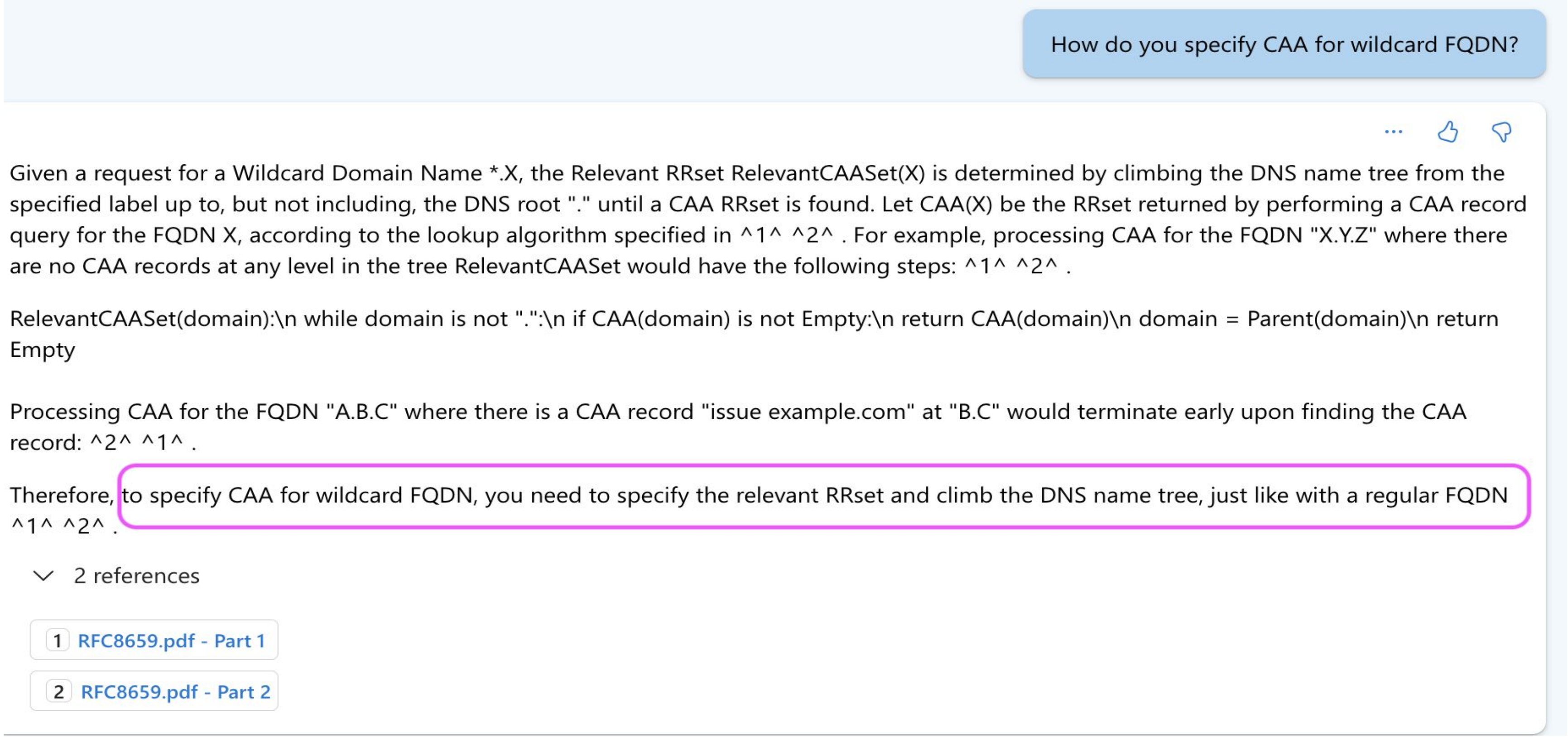
Used Azure Open AI for the POC

- Create Azure AI service
- Upload RFC 8659 to the AI service
- Create Open AI Chatbot linking to the AI service

Question 3

How do you specify CAA for wildcard FQDN?

DnsChat tool - POC



How do you specify CAA for wildcard FQDN?

Given a request for a Wildcard Domain Name *.X, the Relevant RRset RelevantCAASet(X) is determined by climbing the DNS name tree from the specified label up to, but not including, the DNS root "." until a CAA RRset is found. Let CAA(X) be the RRset returned by performing a CAA record query for the FQDN X, according to the lookup algorithm specified in ^1^ ^2^ . For example, processing CAA for the FQDN "X.Y.Z" where there are no CAA records at any level in the tree RelevantCAASet would have the following steps: ^1^ ^2^ .

RelevantCAASet(domain):\n while domain is not ".":\n if CAA(domain) is not Empty:\n return CAA(domain)\n domain = Parent(domain)\n return Empty

Processing CAA for the FQDN "A.B.C" where there is a CAA record "issue example.com" at "B.C" would terminate early upon finding the CAA record: ^2^ ^1^ .

Therefore, to specify CAA for wildcard FQDN, you need to specify the relevant RRset and climb the DNS name tree, just like with a regular FQDN ^1^ ^2^ .

2 references

1 RFC8659.pdf - Part 1

2 RFC8659.pdf - Part 2

Next Steps - Own the narrative

DNSchat tool ....

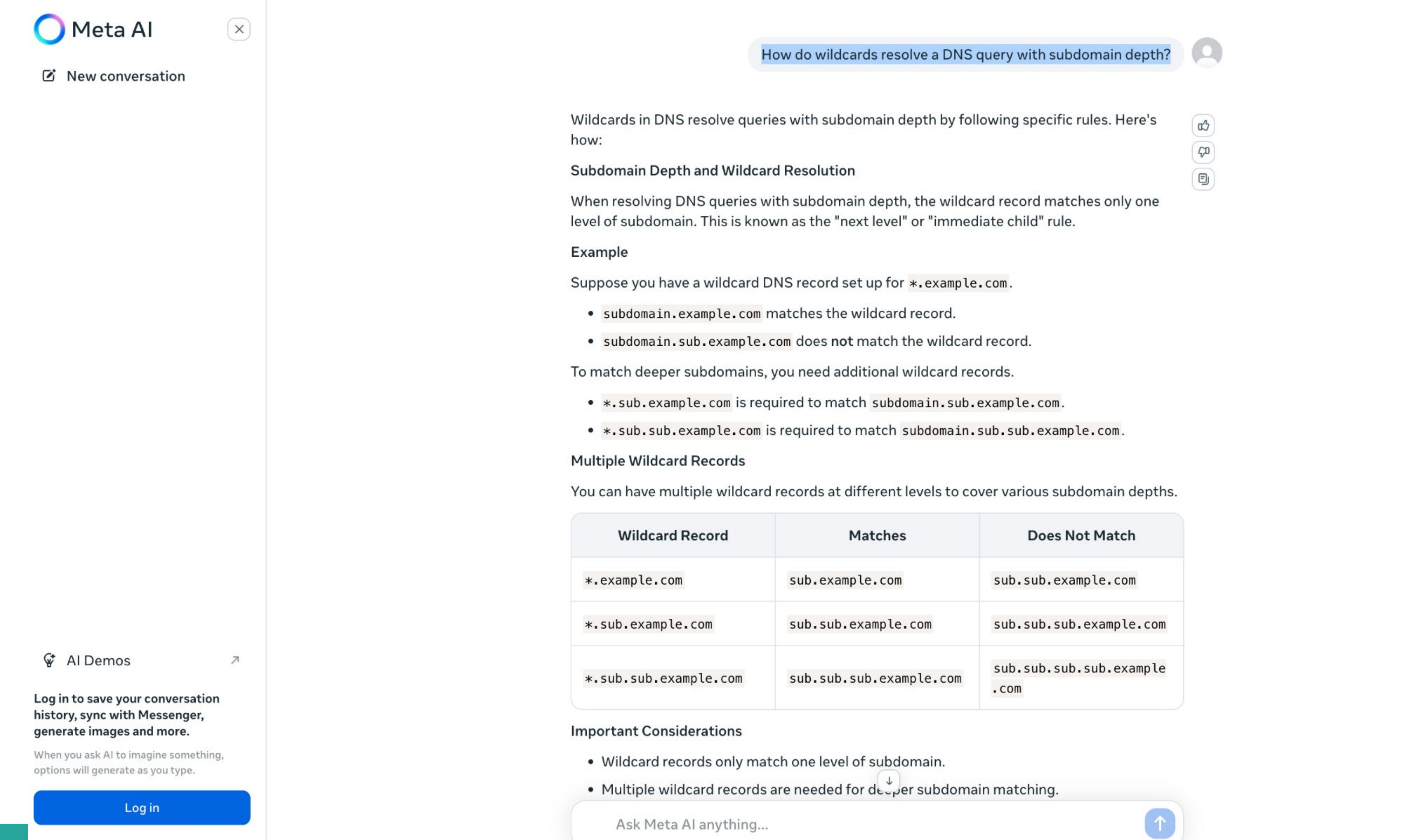
- Collaboration with DNS-OARC
- Managed and verified by DNS community
- Trustworthy to give correct information

Reference

[1]
https://appian.com/learn/topics/enterprise-ai/what-is-generative-ai#:~:text=Generative%20AI%20is%20the%20kind,speed%20up%20content%20creation%20tasks.

[2]

https://learn.microsoft.com/en-us/azure/search/retrieval-augmented-generation-overview



How do wildcards resolve a DNS query with subdomain depth?

Wildcards in DNS resolve queries with subdomain depth by following specific rules. Here's how:

Subdomain Depth and Wildcard Resolution

When resolving DNS queries with subdomain depth, the wildcard record matches only one level of subdomain. This is known as the "next level" or "immediate child" rule.

Example

Suppose you have a wildcard DNS record set up for `*.example.com`.

- `subdomain.example.com` matches the wildcard record.
- `subdomain.sub.example.com` does **not** match the wildcard record.

To match deeper subdomains, you need additional wildcard records.

- `*.sub.example.com` is required to match `subdomain.sub.example.com`.
- `*.sub.sub.example.com` is required to match `subdomain.sub.sub.example.com`.

Multiple Wildcard Records

You can have multiple wildcard records at different levels to cover various subdomain depths.

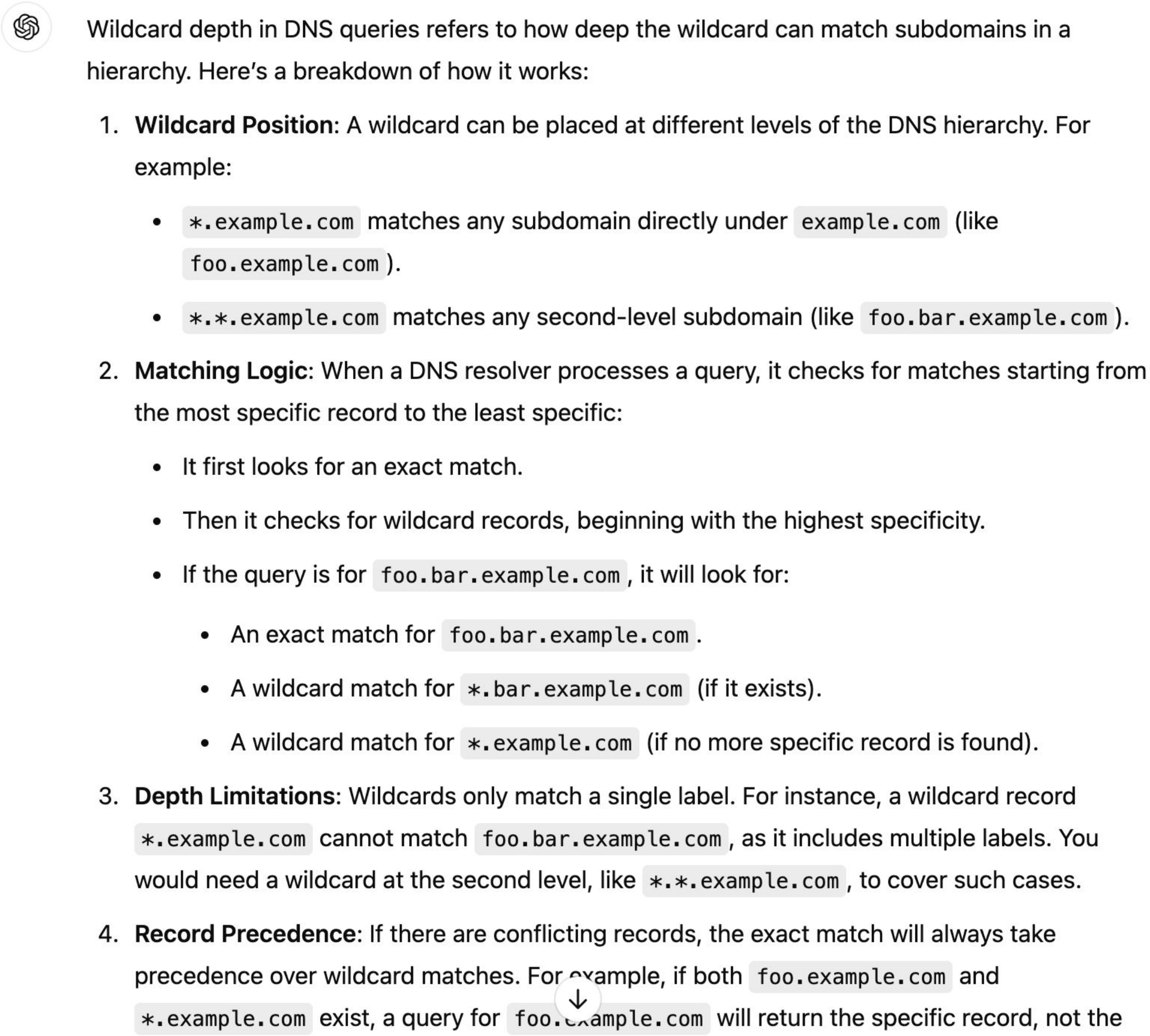
Wildcard Record	Matches	Does Not Match
`*.example.com`	`sub.example.com`	`sub.sub.example.com`
`*.sub.example.com`	`sub.sub.example.com`	`sub.sub.sub.example.com`
`*.sub.sub.example.com`	`sub.sub.sub.example.com`	`sub.sub.sub.sub.example.com`

Important Considerations

- Wildcard records only match one level of subdomain.
- Multiple wildcard records are needed for deeper subdomain matching.

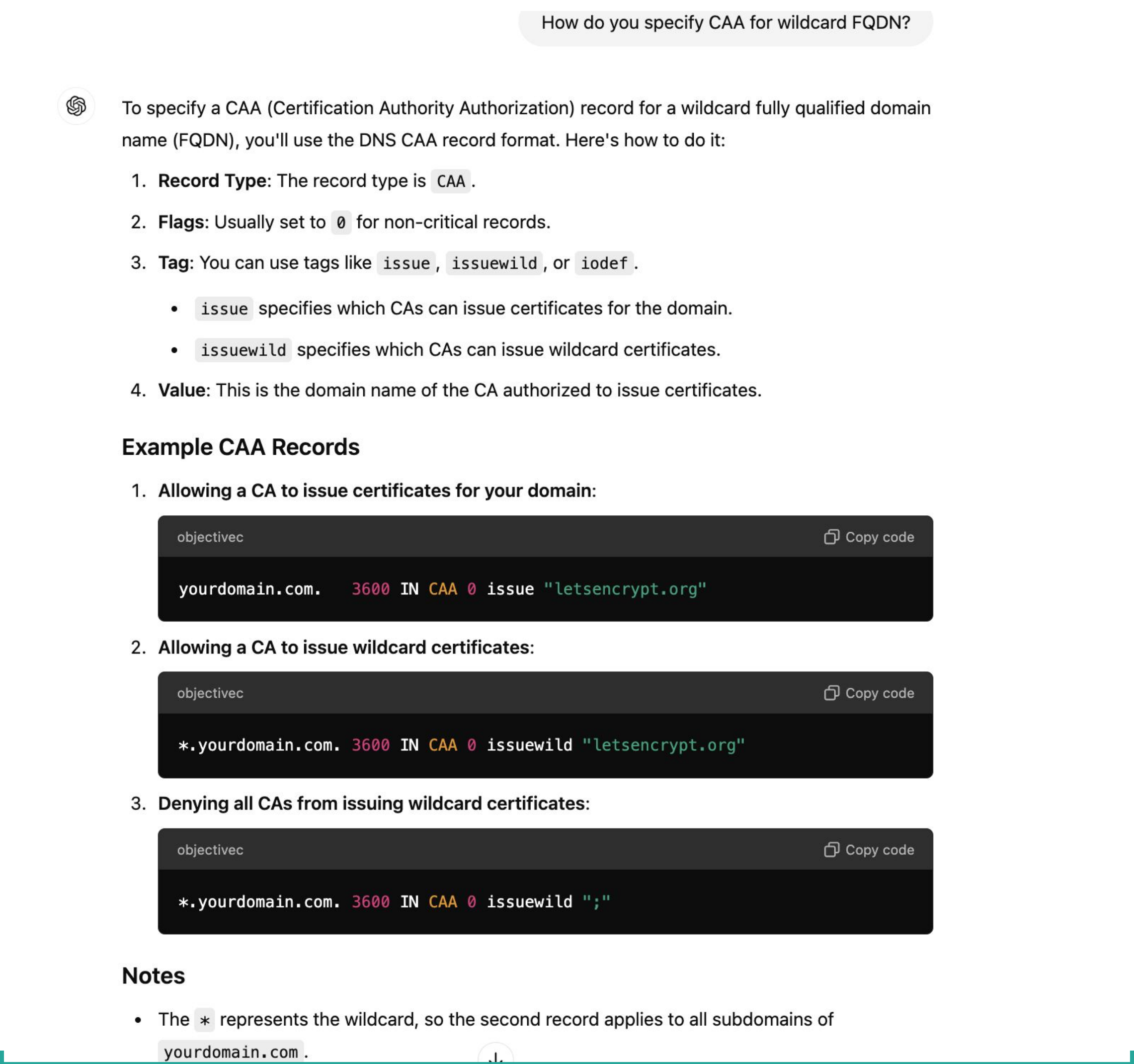
Log in to save your conversation history, sync with Messenger, generate images and more.

When you ask AI to imagine something, options will generate as you type.



Wildcard depth in DNS queries refers to how deep the wildcard can match subdomains in a hierarchy. Here's a breakdown of how it works:

1. **Wildcard Position**: A wildcard can be placed at different levels of the DNS hierarchy. For example:
    - `*.example.com` matches any subdomain directly under `example.com` (like `foo.example.com`).
    - `*.*.example.com` matches any second-level subdomain (like `foo.bar.example.com`).
2. **Matching Logic**: When a DNS resolver processes a query, it checks for matches starting from the most specific record to the least specific:
    - It first looks for an exact match.
    - Then it checks for wildcard records, beginning with the highest specificity.
    - If the query is for `foo.bar.example.com`, it will look for:
        - An exact match for `foo.bar.example.com`.
        - A wildcard match for `*.bar.example.com` (if it exists).
        - A wildcard match for `*.example.com` (if no more specific record is found).
3. **Depth Limitations**: Wildcards only match a single label. For instance, a wildcard record `*.example.com` cannot match `foo.bar.example.com`, as it includes multiple labels. You would need a wildcard at the second level, like `*.*.example.com`, to cover such cases.
4. **Record Precedence**: If there are conflicting records, the exact match will always take precedence over wildcard matches. For example, if both `foo.example.com` and `*.example.com` exist, a query for `foo.example.com` will return the specific record, not the



How do you specify CAA for wildcard FQDN?

To specify a CAA (Certification Authority Authorization) record for a wildcard fully qualified domain name (FQDN), you'll use the DNS CAA record format. Here's how to do it:

1. **Record Type**: The record type is `CAA`.
2. **Flags**: Usually set to `0` for non-critical records.
3. **Tag**: You can use tags like `issue`, `issuewild`, or `iodef`.
    - `issue` specifies which CAs can issue certificates for the domain.
    - `issuewild` specifies which CAs can issue wildcard certificates.
4. **Value**: This is the domain name of the CA authorized to issue certificates.

Example CAA Records

1. **Allowing a CA to issue certificates for your domain**:

```objectivec
yourdomain.com.   3600 IN CAA 0 issue "letsencrypt.org"
```

2. **Allowing a CA to issue wildcard certificates**:

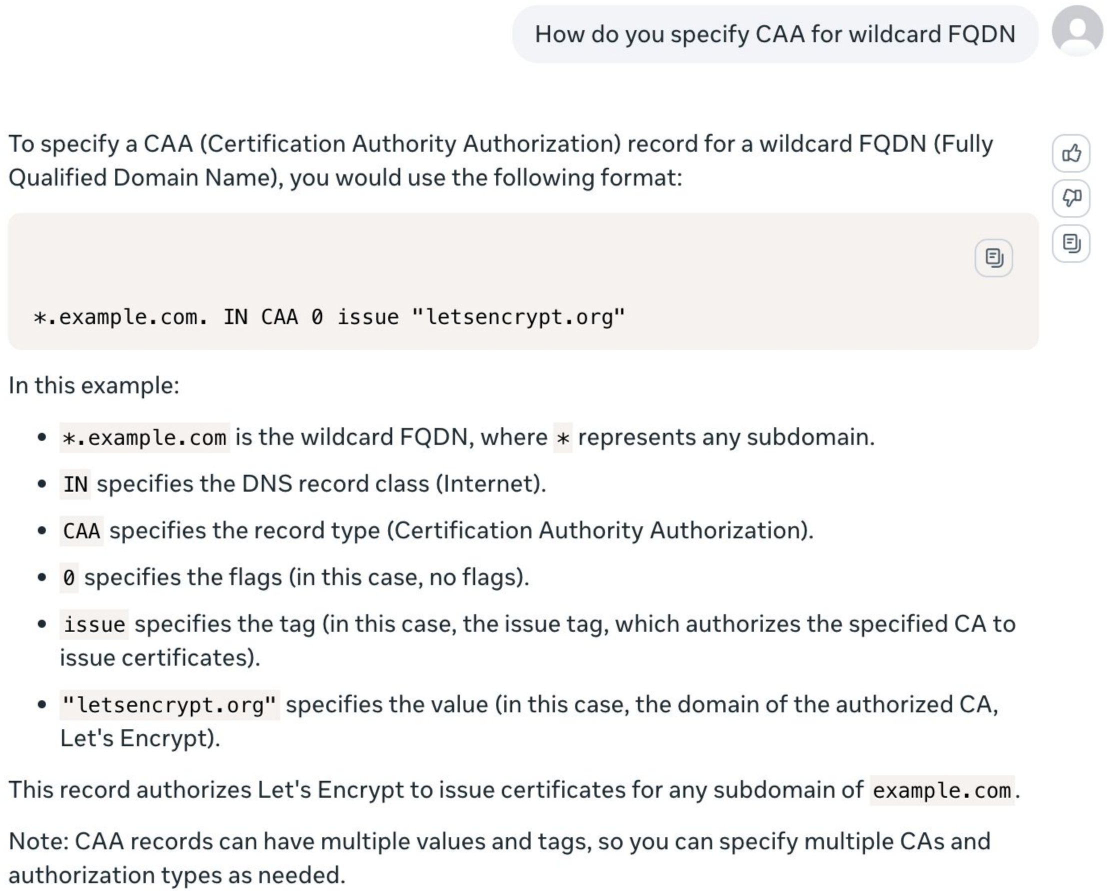
```objectivec
*.yourdomain.com. 3600 IN CAA 0 issuewild "letsencrypt.org"
```

3. **Denying all CAs from issuing wildcard certificates**:

```objectivec
*.yourdomain.com. 3600 IN CAA 0 issuewild ";"
```

Notes

- The `*` represents the wildcard, so the second record applies to all subdomains of `yourdomain.com`.



How do you specify CAA for wildcard FQDN

To specify a CAA (Certification Authority Authorization) record for a wildcard FQDN (Fully Qualified Domain Name), you would use the following format:

```
*.example.com. IN CAA 0 issue "letsencrypt.org"
```

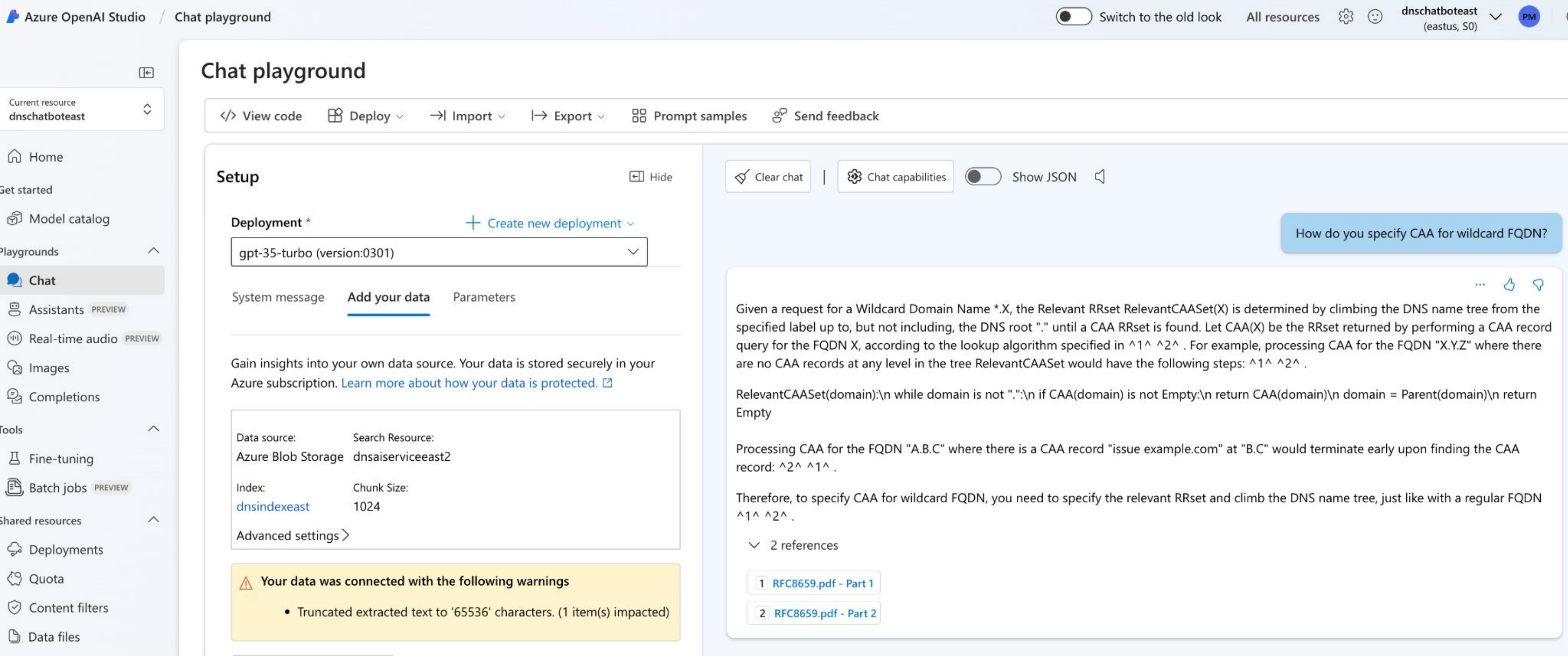
In this example:

- `*.example.com` is the wildcard FQDN, where `*` represents any subdomain.
- `IN` specifies the DNS record class (Internet).
- `CAA` specifies the record type (Certification Authority Authorization).
- `0` specifies the flags (in this case, no flags).
- `issue` specifies the tag (in this case, the issue tag, which authorizes the specified CA to issue certificates).
- `"letsencrypt.org"` specifies the value (in this case, the domain of the authorized CA, Let's Encrypt).

This record authorizes Let's Encrypt to issue certificates for any subdomain of `example.com`.

Note: CAA records can have multiple values and tags, so you can specify multiple CAs and authorization types as needed.

Azure Open AI



Chat playground

Setup

Deployment *

gpt-35-turbo (version:0301)

Gain insights into your own data source. Your data is stored securely in your Azure subscription. Learn more about how your data is protected.

Data source:	Search Resource:
Azure Blob Storage	dnsaiserviceeast2
Index:	Chunk Size:
dnsindexeast	1024

Your data was connected with the following warnings

- Truncated extracted text to '65536' characters. (1 item(s) impacted)

How do you specify CAA for wildcard FQDN?

Given a request for a Wildcard Domain Name *.X, the Relevant RRset RelevantCAASet(X) is determined by climbing the DNS name tree from the specified label up to, but not including, the DNS root "." until a CAA RRset is found. Let CAA(X) be the RRset returned by performing a CAA record query for the FQDN X, according to the lookup algorithm specified in ^1^ ^2^ . For example, processing CAA for the FQDN "X.Y.Z" where there are no CAA records at any level in the tree RelevantCAASet would have the following steps: ^1^ ^2^ .

RelevantCAASet(domain):\n while domain is not ".":\n if CAA(domain) is not Empty:\n return CAA(domain)\n domain = Parent(domain)\n return Empty

Processing CAA for the FQDN "A.B.C" where there is a CAA record "issue example.com" at "B.C" would terminate early upon finding the CAA record: ^2^ ^1^ .

Therefore, to specify CAA for wildcard FQDN, you need to specify the relevant RRset and climb the DNS name tree, just like with a regular FQDN ^1^ ^2^ .

1 RFC8659.pdf - Part 1

2 RFC8659.pdf - Part 2