

REFCARDS (/resources/refcards/)

REPORTS (/reports/)

TRENDREPORTS (/trendreports/)

Search

Culture and Methodologies

Integrating PostgreSQL Databases With ANF: Join this workshop and learn how to create PostgreSQL server using stacustr's managed service

Reserve Your Spot

https://dzone.com/events/video-rary/Seamlessly-Integrating-ur-PostgreSQL-Database-th-ANF)

Data Engineering

Mobile Database Essentials: Assess data needs, storage requirements, and more when leveraging databases for cloud and edge applications.

Download the Refcard

(https://dzone-resources.dzone.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp:&qf=w_defa4255&ch=sitenote)

Software Design and Architecture (/software-design-and-architecture/)

Mobile Database Essentials: Assess data needs, storage requirements, and more when leveraging databases for cloud and edge applications.

Register Now

(https://dzone-resources.dzone.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp:&qf=w_defa5085&ch=sitenote)

Coding (/coding)

Monitoring and Observability for LLMs: Datadog and Google Cloud discuss how to achieve optimal AI model performance.

Download the Trend Report

(https://dzone-resources.dzone.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp:&qf=w_defa5076&ch=sitenote)

Testing, Deployment, and Maintenance (/testing-deployment-and-maintenance/)

Automated Testing: The latest on architecture, TDD, and the benefits of AI and low-code tools.

Download the Trend Report

(https://dzone-resources.dzone.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp:&qf=w_defa5076&ch=sitenote)

RELATED

- Penetration Testing: A Comprehensive Guide (/articles/penetration-testing-a-comprehensive-guide)
- Demystifying SPF Record Limitations (/articles/demystifying-spf-record-limitations-strategies-for)
- 5 DNS Troubleshooting Tips for Network Teams (/articles/5-dns-troubleshooting-tips-for-network-teams)
- Difference Between DNS Over TLS and DNS Over HTTPS (/articles/difference-between-dns-over-tls-amp-dns-over-https)

Partner Resources



REFCARDS (/REFC) REFERENCE REPORTS (/TRN) TRIP REPORTS (/TRP) TRIP REPORTS (/TRP)

REFCARDS (/REFCARDS) REPORTS (/reports) TRENDING (/trending)

TS/TRENDRE
(/users/login.html)

WEST(\$\$

~~REDST(\$search)~~

Data
Engineering
(/data-
engineering)

Coding
(/coding)

Testing, Deployment, and
Maintenance (/testing-
deployment-and-maintenance)



Protect Your Domain With DNSSEC on AWS Route53 and GoDaddy Registrar

In this article, learn more about how DNSSEC is an important tool for ensuring the security and reliability of the Internet's address book.



by **Rahul Nagpure** (/users/4861304/rahulnagpure.html) · Feb. 16, 23 · Tutorial

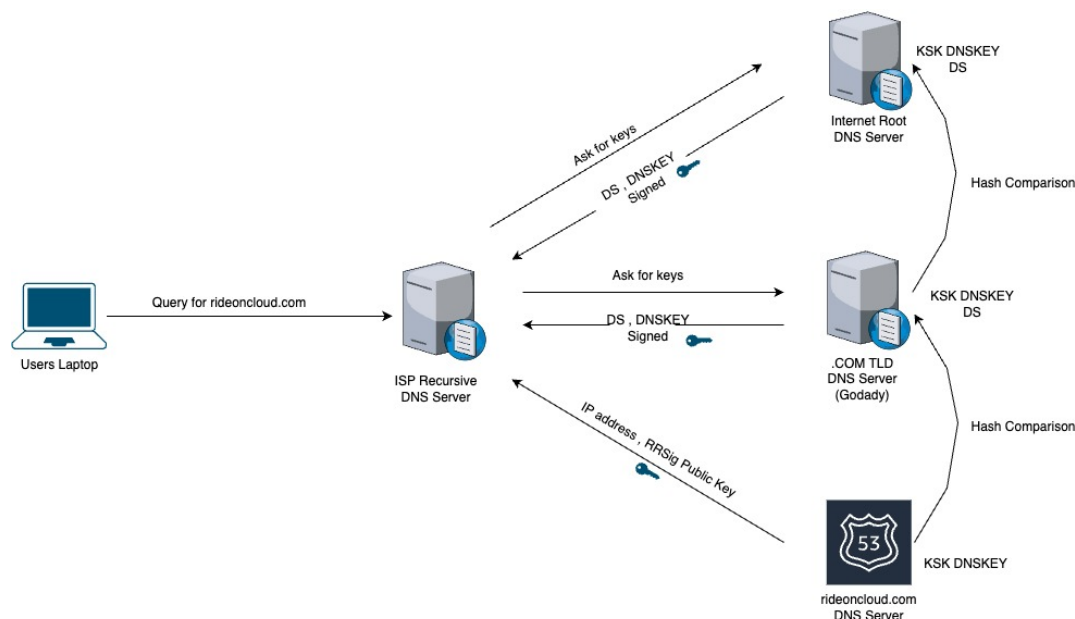
Like (1) Comment (0) Save Tweet Share 3.60K Views

DNSSEC, short for Domain Name System Security Extensions, is a set of protocols that aim to secure the domain name system (DNS) (https://dzone.com/refcardz/dns) against various security threats such as spoofing, cache poisoning, and eavesdropping. DNSSEC is designed to protect the authenticity and integrity of the information in the DNS, ensuring that users receive the correct information from authoritative sources.

How Does DNSSEC Work?

DNSSEC works by adding cryptographic signatures to DNS data. The signatures are created by a trusted third party, known as a key signing key (KSK), and are stored in the DNS record along with the original data. When a user sends a DNS query, the DNSSEC-enabled server will use the signatures to verify the authenticity of the data and ensure that it has not been altered in transit. If the data is not valid, the server will reject the request and the user will receive an error message.

Understanding DNSSEC can be a bit complicated and confusing, but I will try to explain it in a simple manner with a few steps with a dummy domain.



1. The user laptop asks the recursive DNS server for domain IPs. (It follows all DNS standard processes to get the IP from the authoritative DNS server. I will not go into how DNS works here. Instead, I will start when the recursive server gets the final IP from the DNS server.)
2. The recursive DNS server connects to the rideoncloud.com DNS server and gets the IP addresses, signed record (RRSig), and corresponding public key used to sign that information.
3. Various validations are performed. However, anyone can sign the DNS resource records data with public and private key (https://dzone.com/articles/public-key-cryptography-the-puzzle-of-the-private) pairs.
4. Therefore, there is an added step to validate this public key with a chain of trust that mimics the same domain tree used to resolve information.
5. The recursive DNS server asks the .com TLD: "I got the public key from the rideoncloud.com DNS server. Do you validate it?"



6. The .com TLD comes back and says, "Yes, my DS info indicates that the key has been provided to me by the rideoncloud.com provider, and here is the hash of that key. I am going to sign this information with my key."

7. This information is then used to query the root server in the same manner and ask for the .com information.

8. Root servers provide the DS record and signed that information also provides its public key.

9. The recursive server, being configured with the root public key as a trusted key, can now check that key against its configuration and passed information for secure resolution.

Note: The recursive server needs to be configured with the public key of the root, and there is a mechanism to automatically adapt changes made on the internet root server.

The Latest DZone Refcard

Threat Modeling

DOWNLOAD THE CHEAT SHEET

([https://dzone-](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421)

[resources.tradepub.com/c/pubRD.mpl?](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421)

[secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421))



([https://dzone-](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421)

[resources.tradepub.com/c/pubRD.mpl?](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421)

[secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421](https://dzone-resources.tradepub.com/c/pubRD.mpl?secure=1&sr=pp&_t=pp&qf=w_defa4696&ch=inarticlepubs3350421))

Why Is DNSSEC Important?

The DNS is the Internet's address book, mapping human-readable domain names to IP addresses. Without DNSSEC, attackers can easily redirect users to malicious websites, steal sensitive information, or spread malware (<https://dzone.com/articles/5-types-of-software-malware-and-how-to-recognize-t>). By implementing DNSSEC, domain owners and users can be confident that the information they receive from the DNS is accurate and has not been tampered with.

How To Implement DNSSEC

Implementing DNSSEC requires the coordination of several different entities, including domain owners, registrars, and DNS operators. The first step is to generate a key signing key (KSK) and a zone signing key (ZSK). The KSK is used to sign the ZSK, which is used to sign the DNS data. The keys must be securely stored and regularly updated to ensure the security of the DNSSEC implementation.

Once the keys are in place, the domain owner must publish the DNSSEC records in the DNS and configure their DNS servers to use DNSSEC. This process involves creating and publishing DNS Resource Records (RRs), such as the DNSKEY, RRSIG, and DS records, which contain the information necessary for the DNSSEC validation process.

I am using AWS Route53 as the DNS server for my domain, rideoncloud.com, and GoDaddy as the registrar.

1. I am assuming that you are already using AWS Route53 for your domain. My domain is rideonclouds.com here.
2. To enable DNSSEC on Route53, you will be asked to create a Key Signing Key (KSK) with a customer-managed customer master key (CMK).

Route 53 > Hosted zones > rideoncloud.com > Enable DNSSEC signing

Enable DNSSEC signing [Info](#)

Complete the DNSSEC signing steps in order [Info](#)

If you don't complete all of the steps, or you complete them out of order, your domain might become unavailable on the internet.

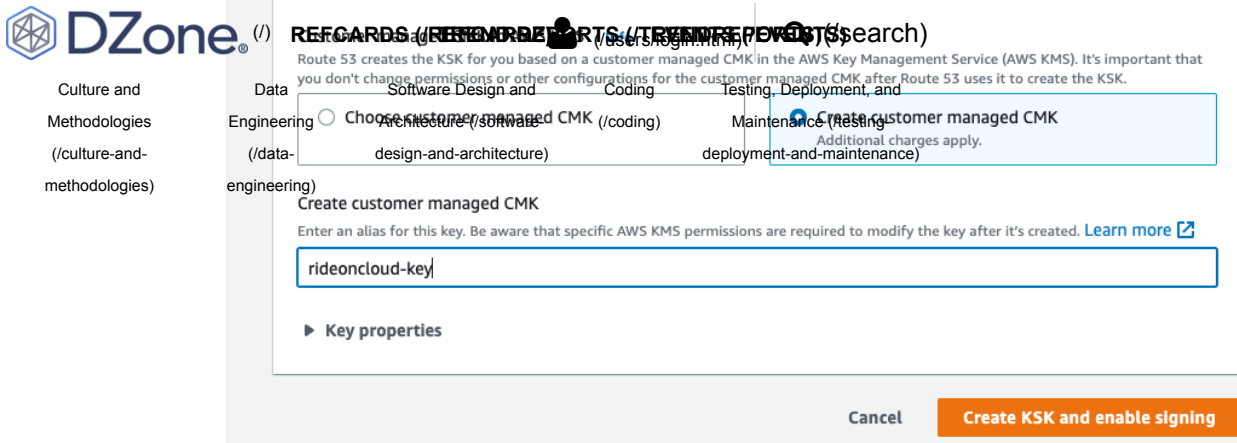
Key-signing key (KSK) creation

On this page, Route 53 will create the key-signing key (KSK) for your hosted zone, based on a customer managed customer master key (CMK) that you choose.

Provide KSK name [Info](#)

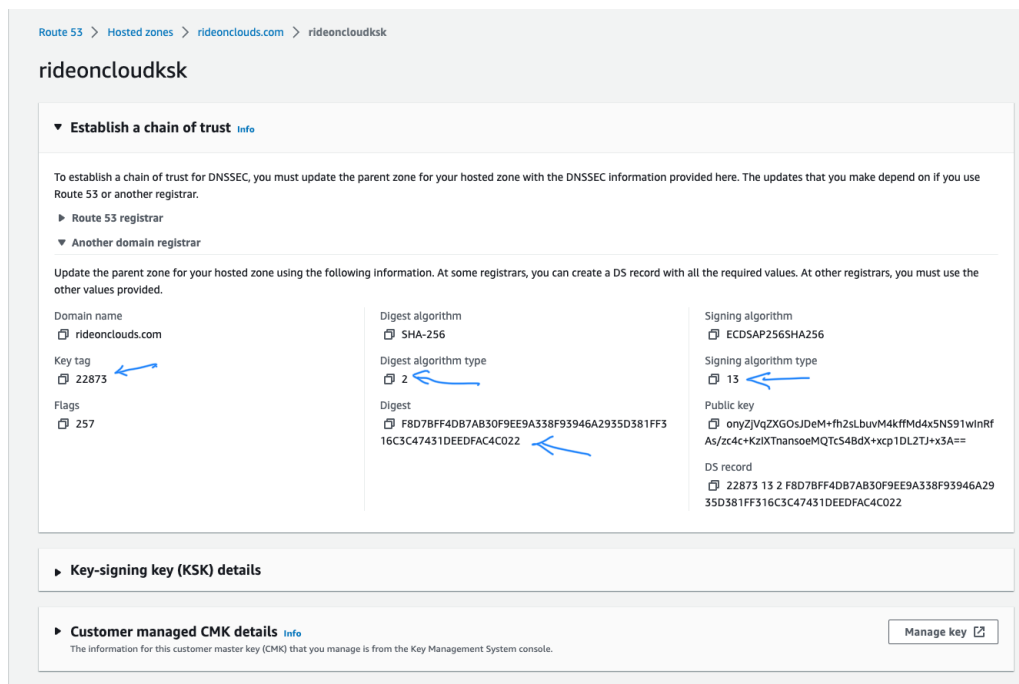
Provide a name for the KSK that Route 53 creates for you automatically.

The name must have 3 - 128 characters. Valid characters: A-Z, a-z, and 0-9.



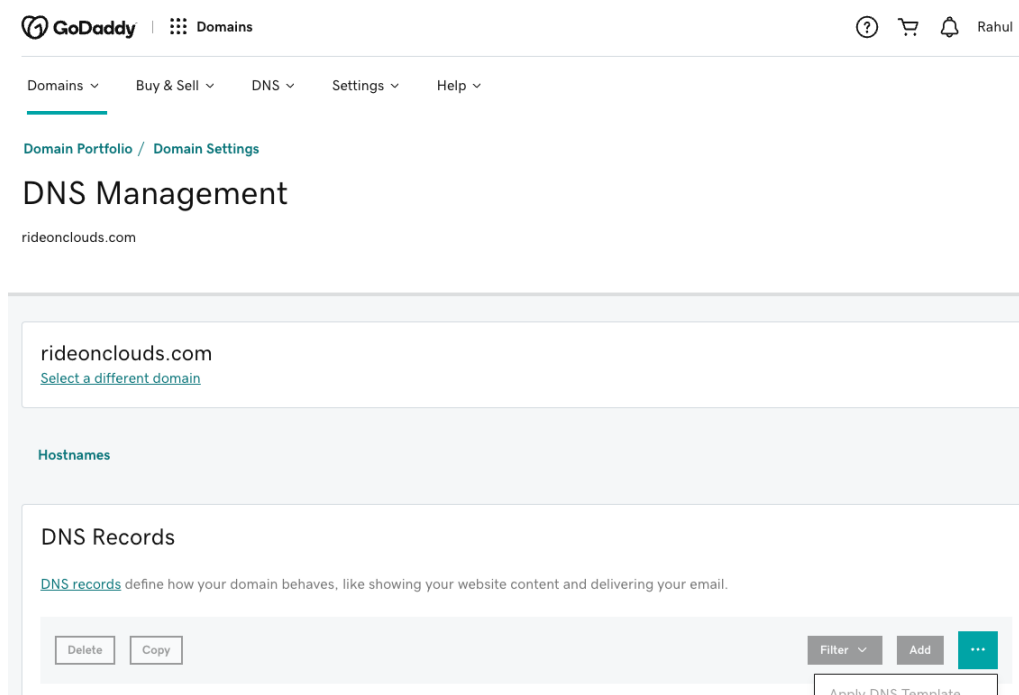
3. After enabling DNSSEC, click on **View Information to Create DS Record**.

4. You will have two options: Route53 registrar and another domain registrar. Since we are using GoDaddy, we will need to use the information provided under **Another Domain Registrar**. This information will need to be entered into GoDaddy in the next steps.



5. Log into your GoDaddy account. Please note that GoDaddy also provides DNSSEC services in their Premium DNS plan, but you do not need to purchase this plan since we are using DNSSEC on AWS Route53.

6. Go to **Domain Portfolio -> Domain Settings** for your domain and select **DNSSEC**.



7. Create a new DS record with the following information.

[ADD](#)

- **Key Tag:** Key Tag in AWS
- **Algorithm:** Signing Algorithm Type in AWS
- **Digest Type:** Digest Algorithm Type in AWS
- **Digest:** Digest in AWS

Test Your Domain

- Run the following command (replace your domain name) in the command line.

```
% dig rideonclouds.com dnskey +dnssec
```

You should get the following output answer section.

```
;; ANSWER SECTION:
rideonclouds.com. 3600 IN DNSKEY 256 3 13 3QJL2Rsu1pgscm0K3Cp13UgvK71VrWpPaP1S8fMI/sitybQ1YYOwS5eu I/Bc+QG5AnTDIQko/PJNLhARcoarGg==
rideonclouds.com. 3600 IN DNSKEY 257 3 13 onyZjVqZXG0sJDeM+fh2sLbuvM4kffMd4xSNS91wInRfAs/zc4c+KzIX TnansoeMQTcS4BdX+xcplDL2TJ+x3A==
rideonclouds.com. 3600 IN RRSIG DNSKEY 13 2 3600 20230205100000 20230204230000 22873 rideonclouds.com. 8pFqJb5d0NWQxDv9oH0zAkRaW+I
2JbhYHNTjfkpUBkd44n17w6FZGnhA E08N6Aq1a/69HueZD4s10M7VX4Qgkg==
```

You will receive two DNSKEYs (one for ZSK and another for KSK) and a signed resource record, confirming that your DNS servers are successfully using DNSSEC.

- Check the chain of trust with your TLD. First, get your TLD server name by using the following command.

```
% dig com NS +short
```

- Make sure that you get the DS record for your domain from TLD.

```
%dig rideonclouds.com DS @m.gtld-servers.net.
```

You should get the following output.

```
;; ANSWER SECTION:
rideonclouds.com. 86400 IN DS 22873 13 2 F8D7BFF4D87AB30F9EE9A338F93946A2935D381FF316C3C47431DEED FAC4C022
```

- The last step is to check your resource record sets with signatures. I have created a dummy A record for my domain. Here is the



REFCARDS (/REFCARDS) REPORTS (/REPORTS) TRENDS (/TRENDS)

Culture and Methodologies (/culture-and-methodologies)	www.rideoncloud.com + Data Engineering (/data-engineering)	Software Design and Architecture (/software-design-and-architecture)	Coding (/coding)	Testing, Deployment, and Maintenance (/testing-deployment-and-maintenance)
--	--	--	------------------	--

You should get the following output for your resource record.

```

[+] ANSWER SECTION:
www.rideonclouds.com. 0 IN A 10.10.10.10
www.rideonclouds.com. 0 IN RRSIG A 13 3 0 20230125032807 20230205012807 26638 rideonclouds.com. AHO/n6lWL2cVZ
7i6nWtTj4wRq0xbx6tA/XYcibQCd0KMc5wy4TXVM/is QdknSHzSJjepi9tTiBKqecKOC4dzXAM=

```

Alternatively, you can use online free tools to validate your DNSSEC.

Please note: DNS propagation can take anywhere from a few minutes to 24 hours, depending on various factors such as the geographical location of the user, the type of DNS record being updated, and the TTL (time to live) value set for the record. During this time, the updated DNS information may not be available to all users and systems immediately.

Conclusion

DNSSEC is an important tool for ensuring the security and reliability of the Internet's address book. By adding cryptographic signatures to DNS data, DNSSEC helps to protect against various security threats (<https://dzone.com/articles/top-five-network-security-risks>), such as spoofing, cache poisoning (<https://dzone.com/articles/what-is-a-host-header-attack>), and eavesdropping. By implementing DNSSEC, domain owners and users can be confident that the information they receive from the DNS is accurate and has not been tampered with.

Domain Name System Security

Opinions expressed by DZone contributors are their own.

RELATED

Penetration Testing: A Comprehensive Guide

Demystifying SPF Record Limitations

5 DNS Troubleshooting Tips for Network Teams

Difference Between DNS Over TLS and DNS Over HTTPS

ABOUT US

About DZone (/pages/about)

Send feedback (<mailto:support@dzzone.com>)

Careers (<https://careers.dzone.com/>)

Sitemap (/sitemap)

ADVERTISE

Advertise with DZone (<https://advertise.dzone.com>)

CONTRIBUTE ON DZONE

[Article Submission Guidelines \(/articles/dzones-article-submission-guidelines\)](#)

[Become a Contributor \(/pages/contribute\)](#)

Visit the Writers' Zone (/writers-zone)

LEGAL

Terms of Service (<https://technologyadvice.com/terms-conditions/>)

Privacy Policy (<https://technologyadvice.com/privacy-policy/>)

CONTACT US

3343 Perimeter Hill Drive


Suite 100

Nashville, TN 37211

support@dzzone.com (<mailto:support@dzzone.com>)

Let's be friends:

(/pages/16658111/https://www.dzintell.com/DZcoelpahy/dzone/)



REFCARDS (/refcards)

RECORDS (/records)

REPORTS (/reports)

TRICKS (/tricks)

POWERS (/powers)

SEARCH (/search)

Culture and Methodologies (/culture-and-methodologies)

Data Engineering (/data-engineering)

Software Design and Architecture (/software-design-and-architecture)

Coding (/coding)

Testing, Deployment, and Maintenance (/testing-deployment-and-maintenance)