How to Rotate a DNSSEC Key

Overview
Rotate the key
Rotate the key
Additional documentation

Overview

This document describes how to rotate a domain's DNS Security Extensions (DNSSEC) keys on a server. You can rotate your domains' DNSSEC keys regularly to increase your DNS record's security.

Important:

- We recommend that you rotate your domain's DNSSEC keys yearly.
- If you transfer the account to another server, you **must** create new DNSSEC keys for the account and update the registrar with the new keys. The system does not include DNSSEC keys in an account's backup file.
- DNSSEC keys remain on a server after you terminate an account. If you restore an account on the same server from which you deleted it, the account's DNSSEC keys remain valid.
- For more information about DNSSEC key rotation, we **strongly** suggest that you read the RFC 6781 documentation.

cPanel & WHM version 76 and later (PowerDNS 4.1) cPanel & WHM version 60 through 74 (PowerDNS 3.0 to 4.0)

Rotate the key

To rotate the DNSSEC key, perform the following steps:

1. Add a new Key Sign Key (KSK) to the domain's DNS zone. To do this, run the following command:

```
pdnsutil add-zone-key example.com ksk active 2048 rsasha512
```

   The output will resemble the following example:

```
Jun 29 15:22:35 [bindbackend] Done parsing domains, 3 rejected, 8 new,
0 removed
Added a KSK with algorithm = 10, active=1
Requested specific key size of 2048 bits
```

   Note:
   `example.com` represents your domain.

2. Increase the DNS zone's Start of Authority (SOA) serial number. To do this, run the following command:

```
grep "Serial Number" /var/named/example.com.db| sed -e 's/^\s*//' -e
'/^$/d' | cut -d';' -f1
## The system will output the serial number. The serial number is
1234567890 in this example.
## Then, increment the serial number by one.
whmapi1 editzonerecord domain=example.com type=SOA serial=1234567890x
line=5
```

   For more information on SOA records, read the Edit DNS Zone documentation.

3. Review the updated zone's DNSSEC details for the Domain Server (DS) records that correspond to the new key. To do this, run the following command:

```
pdnsutil show-zone example.com
```

Thie output resembles the following example:

Click to view...

```
Added a KSK with algorithm = 8, active=1
Requested specific key size of 2048 bits
Zone has NARROW hashed NSEC3 semantics, configuration: 1 0 7
9827d1a1a467a387
keys:
ID = 1 (KSK), tag = 41686, algo = 8, bits = 2048 Active: 1 (
RSASHA256 )
KSK DNSKEY = example.com IN DNSKEY 257 3 8
AwEAAa2vycAp3tqgqxXP8Q7TYlWGgUzLMPG/e/zzH3feFA1y1JbXKo0tlM/D6HG+aKr
EBottuVIzmtIQcCBhxbDo69MrZ+OsUb1Elbf3ryEKrECRZegG1hjVfR82DDVJFoNYKZ
PsPSlmLOdbCze+2/liv954U7UayN0Bt1TiYtX9mXJEltkVODaxm4xnr+T49aKN3cC2h
tZ2Kv+wsmEEgfF403uGx08yvBYaEFj4Um7+Ll1JE/I8R2piwzCxBWkZv1ioDNxKxvS9
0A5E/GDDRc/91VJeQDKSj412dA/810W6bEhAfXf5EzJT/Usdo+Xo93sf+pM1muFb85h
a4VvRFXVJ7nc= ; ( RSASHA256 )
DS = example.com IN DS 41686 8 1
cc2bbc84733abfea5c1c06e42536e56f947eec6f ; ( SHA1 digest )
DS = example.com IN DS 41686 8 2
09ffb322a1697230a8a7b86301f8a80540ed1c78210778fe863f25c08cdfc6c6 ;
( SHA256 digest )
DS = example.com IN DS 41686 8 4
c179cd343402e979cd48638c91d011b0cf5866e8e63d76a15da22597a59f650d369
17de1dec35c5a269dd6e7a632cc99 ; ( SHA-384 digest )

ID = 3 (KSK), tag = 31361, algo = 8, bits = 2048 Active: 1 (
RSASHA256 )
KSK DNSKEY = example.com IN DNSKEY 257 3 8
AwEAAdNQ2mk+pMUeDi/vXwEHrptEQHe4wbkEg7xB/V20sFunPX+gcaW5HiFnrcr/5/S
AyqlFaQI17u9Revy0pVToSnNPCr3uNA2kt0F/9KqOC5kX8trMKKZlCAf4tbiLoecNpq
pPWcCU6/ttGBCaatmor0lTrPD4DElh0/0sb2/2gIdRz1nw/07jTerLGrj6y/1gb7m14
0K8fZbFQ7HKIUqlzrWqKQVzCQz5oW0dHiok7yK1Z8mj5Mci4Gwl9flsbtjaos0NWKh+
N8S2bTfALRT8ucQiZYzYdlRB8UCeXoavYU75kShbNesNBBkmo7hc3R1CdP7TMjDE8f7
f30ky8pKvYn0= ; ( RSASHA256 )
DS = example.com IN DS 31361 8 1
0741f7349684a39004e2b0b431a04b4e44f5dc69 ; ( SHA1 digest )
DS = example.com IN DS 31361 8 2
b0cfc8e92dfe77686542032051a1150173075d485fa77656309baefdcbe807b1 ;
( SHA256 digest )
DS = example.com IN DS 31361 8 4
7fdae2e7fb53b4444dde36854cb91a5f03607b30f716e9c28ffb7fc25ee92e7b872
cbf697a936a08a637ccb73951a1a9 ; ( SHA-384 digest )

ID = 2 (ZSK), tag = 39844, algo = 8, bits = 1024 Active: 1 (
RSASHA256 )
```

4. Add a new DS record for the domain through your nameserver registrar. To do this, follow the directions in our How to Set Up Nameservers in a cPanel Environment documentation.
5. Wait 24 to 48 hours for the DS record to propagate.

> **Warning:**
> If you do **not** wait for the DS record to propagate, your domain may experience DNS resolution issues.

6. Remove the domain's **old** KSK. To do this, run the following command:

```
pdnsutil remove-zone-key example.com key-id
```

> **Note:**
> `keyid` represents the old KSK's key ID. The `pdnssec show-zone` command's output contains the key's ID.

Rotate the key

To rotate the DNSSEC key, perform the following steps:

1. Add a new Key Sign Key (KSK) to the domain's DNS zone. To do this, run the following command:

```
pdnssec add-zone-key example.com ksk 2048 active
```

The output will resemble the following example:

```
Added a KSK with algorithm = 8, active=1
Requested specific key size of 2048 bits
```

> **Note:**
> `example.com` represents your domain.

2. Increase the DNS zone's Start of Authority (SOA) serial number. To do this, run the following command:

```
grep "Serial Number" /var/named/example.com.db| sed -e 's/^\s*//' -e
'/^$/d' | cut -d';' -f1
## The system will output the serial number. The serial number is
1234567890 in this example.
## Then, increment the serial number by one.
whmapi1 editzonerecord domain=example.com type=SOA serial=1234567890x
line=5
```

For more information on SOA records, read the Edit DNS Zone documentation.

3. Review the updated zone's DNSSEC details for the Domain Server (DS) records that correspond to the new key. To do this, run the following command:

```
pdnssec show-zone example.com
```

Thie output resembles the following example:

Click to view...

```
Jun 29 15:32:56 [bindbackend] Done parsing domains, 0 rejected, 8
new, 0 removed
Zone is not presigned
Zone has NSEC semantics
keys:
ID = 2 (KSK), tag = 65017, algo = 8, bits = 2048 Active: 1 (
RSASHA256 )
KSK DNSKEY = example.com IN DNSKEY 257 3 8
AwEAAcvy22Lte30KEn2ZJ/+TIdvmIKM8m2TzIlKlV3zB8OGi8UEixkowAwvefbRaxlM
mbqmUJE2Gn6rjNPoJBANjAaf8DkchdDIfyyfVJKKjuqAb5hr8hW4BcapZquiRmpXinV
HLmQmAxt1rGAo5zdIwpntk3fjsPnEC/dGCJeWzVrUTkX9ucYJRG+4yE9xEzMyx89Vnw
n+UWBdoQejtthm6IqNC5ilPQDrfTi/cj//5LTXUNGxs8329qgGtQP9uUf0SOaf3PUIW
ux2n7b1IRKqZ7cN9EAQCU0ye2D38xqpegsM726lzK//QOuj66I9p+c6l5owKzTMPWsb
VKqmx5SEJAYc= ; ( RSASHA256 )
DS = example.com IN DS 65017 8 1
4b3114ef11b7c329703b986bf0a1eae971f37257 ; ( SHA1 digest )
DS = example.com IN DS 65017 8 2
d6b31f08f67486dbf7dafac825f180f3907b1b9bf55481b028c2a67ea3a2e38c ;
( SHA256 digest )
DS = example.com IN DS 65017 8 4
97bf836b64506d7dc9cea16ae8ac512c76eecf35f2260c5296d816ca45927a5b69b
eb66c2e98007e48fc957a85f29684 ; ( SHA-384 digest )

ID = 3 (KSK), tag = 33926, algo = 8, bits = 2048 Active: 1 (
RSASHA256 )
KSK DNSKEY = example.com IN DNSKEY 257 3 8
AwEAAYV+hR7YDw6hfEPh1DHKmycHmQKB4P0JuIVd/eNAu2Q40jbPkxsBUYUcviZDdGc
IYgO7Giu7lGePytebMDBAk9y46saAaTh4RK8cu4sN2sefx+rBj3CZB9lVU5KmePQHYD
VlompP/Gh+pmCcBGKhzMwwK9QXz+FG4Yn3AJSQfzsEUKxRhoTIhxFmbraG4Zuf6iBj1
D7VPFJBJc6TsfJZvC1nMaN2MQSphwrOdIVVCBJYUNy8VzbflAv/ItpTBBH0BXhyNcAD
EIFwp0R53v4KxWb483Hb5SOaLjdUFQ4RBQ21Lly1MKVuq3xH1dXdqT1N6IIBKlZpMgj
aNfDLw4d36K0= ; ( RSASHA256 )
DS = example.com IN DS 33926 8 1
1687f21b62f9ea9a140048060b4f469ded1e5276 ; ( SHA1 digest )
DS = example.com IN DS 33926 8 2
260765a78971aea6ca50504403efcb45a1dcad45d00ceba07bef3ed1ca954592 ;
( SHA256 digest )
DS = example.com IN DS 33926 8 4
72939651d3df84b85861213fe2c26293b081a518cf6431ddc0e21a9e30fc6831663
05697e6fe8fc7427db0eb5f4057bf ; ( SHA-384 digest )
```

4. Add a new DS record for the domain through your nameserver registrar. To do this, follow the directions in our How to Set Up Nameservers in a cPanel Environment documentation.
5. Wait 24 to 48 hours for the DS record to propagate.

Warning:
If you do **not** wait for the DS record to propagate, your domain may experience DNS resolution issues.

6. Remove the domain's **old** KSK. To do this, run the following command:

```
pdnssec remove-zone-key example.com key-id
```

Note:
`keyid` represents the old KSK's key ID. The `pdnssec show-zone` command's output contains the key's ID.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- How to Rotate a DNSSEC Key
- How to List Domains with DNSSEC
- Server Profiles Roadmap
- How to Use MyDNS-NG
- How to Set Up Nameservers in a cPanel Environment

- How To Clear Your DNS Cache

- How to Rotate a DNSSEC Key
- How to List Domains with DNSSEC
- Server Profiles Roadmap
- How to Use MyDNS-NG
- How to Set Up Nameservers in a cPanel Environment

- UAPI Functions - DNSSEC::enable_dnssec
- UAPI Functions - DNSSEC::unset_nsec3
- UAPI Functions - DNSSEC::disable_dnssec
- UAPI Functions - DNSSEC::fetch_ds_records
- UAPI Modules - DNSSEC