dnssec-signzone

Outil de signature de zone DNSSEC

dnssec-signzone permet de signer une zone. Il génère des records NSEC et RRSIG et produit une version signée de la zone. Le status de sécurité de la zone signée (c'est à dire si les zones enfants sont sécurisées ou non) est déterminé par la présence ou l'absence d'un fichier keyset pour chaque zone enfant.

OPTIONS

-a Vérifie toutes les signatures générées

-c class Spécifie la classe de la zone

-C mode compatibilité : génère un fichier keyset-zonename en plus de dsset-zonename utilisé par d'anciennes versions de dnssec-signzone

-d directory Répertoire où trouver les fichier dsset- ou keyset-

-D Affiche seulement les type de record automatiquement gérés par dnssec-signzone, ex RRSIG, NSEC, NSEC3 et NSEC3PARAM.

engine Hardware cryptographique à utiliser.

-g Génère les records DS pour les zones enfant depuis le fichier dsset- ou keyset-. Les records DS existant seront supprimés.

-K directory Répertoire où trouver les clés

-k key Traite la clé spécifiée comme clé de signature de clé en ignorant les flags de clé. Peut être spécifié plusieurs fois.

-l domain Génère un set DLV en plus d'un set DS. Le domain spécifié est ajouté au nom des records.

-M maxttl Définis le TTL maximum pour la zone signée. Un TTL supérieur sera réduit à cette valeur dans la sortie.

-s start-time Spécifie la date et l'heure où les records RRSIG deviennent valides

end-time Spécifie la date et l'heure où les records RRSIG expirent.

-X extended end-time Spécifie la date à laquelle les records RRSIG pour le DNSKEY RRset expire. Utilisé dans les cas où les signature DNSKEY doivent persister plus longtemp que les signatures dans d'autres records.

-f output-file Le nom du fichier de sortie contenant la zone signée. par défaut, ajoute .signed au nom du fichier d'entrée.

-i interval Quand un zone précédemment signée est passée en entrée, les records peuvent être resignés. Spécifie le cycle d'interval relatif à l'heure courante (en secondes).

-I input-format Le format du fichier de zone en entrée. peut être text ou raw.

-j jitter En signant une zone avec une durée de vie de signature fixe, tous les records RRSIG émis à la date d'expiration de signature expire en même temps. Si la zone est signée incrémentalement, toutes les signatures expirées doivent être générées au même moment. Cette option spécifie une fenêtre qui est utilisée pour rendre la date d'expiration aléatoire.

-L serial En écrivant une zone signée au format raw ou map, définis la valeur source serial dans l'en-tête à la valeur spécifiée.

ncpus Spécifie le nombre de threads à utiliser. Défaut : 1 thread par CPU

-N soa-serial-format Format du sérial SOA. Peut être keep (ne modifie pas le sérial), increment (incrément le SOA en utilisant l'arithmétique rfc1982) et unixtime(définis le sérial au temps epoch)

-o origin La zone d'origine. Si non spécifié, le nom du fichier de zone est assumé.

-O output-format Le format du fichier de sortie contenant la zone signée. Peut être text (défaut), full (format text utilisable pour le traitement pas des scripts), map, raw, et raw=N où N spécifie la version du format. à 0, le fichier peut être lu pat toute version, à 1 le fichier ne peut être lu que pas la version 9.9.0 ou supérieur. Défaut : 1.

-p Utilise des données pseudo-aléatoire en signant la zone. C'est plus rapide mais moins sécurisé.

-P Désactive le teste de vérification de signature

-Q Supprime les signatures depuis les clés qui ne sont plus actives.

-R Supprime les signatures des clés qui ne sont plus publiées

-r randomdev Spécifie la source de random

-S Recherche dans le répertoire de clés, les clés correspondant à la zone à signer, et les inclus dans la zone si approprié.

-T ttl Spécifie le ttl à utiliser pour les nouveaux records DNSKEY importés dans la zone.

-t Affiche les statistiques une fois terminé

-u Met à jour la chaîne NSEC/NSEC3 en re-signant une zone précédemment signée. Avec cette option, une zone signée avec NSEC peut passer en NSEC3, ou une zone signée avec NSEC3 peut passer en NSEC ou en NSEC3 avec des paramètres différents.

-v level Définis le niveau de debug

-x Signe uniquement le DNSKEY RRset avec les clés key-signing, et omet les signatures des clés zone-signing

-z Ignore le flag KSK dans la clé en déterminant quoi signer. Celà force les clés avec le flag KSK de signer tous les records, pas seulement le DNSKEY RRset.

-3 salt Génère une chaîne NSEC3 avec le salt spécifié (en hexa). Un point peut être utilisé pour indiquer qu'aucun 'salt' n'est utilisé.

-H iterations En générant une chaîne NSEC3, utilise le nombre d'itérations spécifié, 10 par défaut.

-A En générant une chaîne NSEC3, met le flag OPTOUT dans tous les records NSEC3 et ne génère pas de records NSEC3 pour les délégations non sécurisées. -AA désactive le flag OPTOUT pour tous les records, utile avec l'option -u

zonefile Le fichier contenant la zone à signer key

Spécifie quelle clé doit être utilisée pour signer la zone. Sinon recherche les records DNSKEY de la zone.

Exemples

Signer la zone example.com avec la clé DSA générée par dnssec-keygen (Kexample.com.+003+17247).
dnssec-signzone -g -o example.com db.example.com Kexample.com.+003+17247
Re-signer une zone précédemment signée avec les paramètres par défaut. Assume que la clé privée est dans le répertoire courant
cp db.example.com.signed db.example.com
dnssec-signzone -o example.com db.example.com