Rocky Enterprise Linux 9.2 Manual Pages on command 'clevis-encrypt-sss.1'

$ man clevis-encrypt-sss.1

CLEVIS-ENCRYPT-SSS(1) CLEVIS-ENCRYPT-SSS(1)

NAME

clevis-encrypt-sss - Encrypts using a Shamir's Secret Sharing policy

SYNOPSIS

clevis encrypt sss CONFIG [-y] < PT > JWE

OVERVIEW

The clevis encrypt sss command encrypts using a Shamir?s Secret Sharing policy. Its only argument is the JSON configuration object.

Shamir?s Secret Sharing (SSS) provides a way to mix pins together to create sophisticated unlocking and high availability policies. SSS is a thresholding scheme. It creates a key and divides it into a number of pieces. Each piece is encrypted using another pin (possibly even SSS recursively). Additionally, you define the threshold t. If at least t pieces can be decrypted, then the encryption key can be recovered and decryption can succeed.

For example, let?s create a high-availability setup using Tang:

$ cfg='{"t":1,"pins":{"tang":[{"url":...},{"url":...}]}}'

$ clevis encrypt sss "$cfg" < PT > JWE

In this policy, we are declaring that we have a threshold of 1, but that there are multiple key fragments encrypted using different Tang servers. Since our threshold is 1, so long as any of the Tang servers are available, decryption will succeed. As always, decryption is simply:

$ clevis decrypt < JWE > PT

CONFIG

This command uses the following configuration properties:

? t (integer) : Number of pins required for decryption (REQUIRED)

? pins (object) : Pins used for encrypting fragments (REQUIRED)

The format of the pins property is as follows:

{PIN:CFG,...} OR {PIN:[CFG,CFG,...],...}

When the list version of the format is used, multiple pins of that type will receive key fragments.

OPTIONS

? -y : Automatically answer yes for all questions. For the tang pin, it will skip the advertisement trust check, which can be useful in automated deployments:

$ cfg='{"t":1,"pins":{"tang":[{"url":...},{"url":...}]}}'

$ clevis encrypt sss "$cfg" -y < PT > JWE

SEE ALSO

clevis-encrypt-tang(1), clevis-decrypt(1)

01/25/2023 CLEVIS-ENCRYPT-SSS(1)