



## ***Rocky Enterprise Linux 9.2 Manual Pages on command 'clevis-encrypt-tang.1'***

**\$ man clevis-encrypt-tang.1**

CLEVIS-ENCRYPT-TAN(1)

CLEVIS-ENCRYPT-TAN(1)

### NAME

clevis-encrypt-tang - Encrypts using a Tang binding server policy

### SYNOPSIS

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

### OVERVIEW

The clevis encrypt tang command encrypts using a Tang binding server policy. Its only argument is the JSON configuration object.

Clevis provides support for the Tang network binding server. Tang provides a stateless, lightweight alternative to escrows. Encrypting data using the Tang pin works like this:

```
$ clevis encrypt tang '{"url":"http://tang.srv"}' < PT > JWE
```

The advertisement contains the following signing keys:

```
_OsIk0T-E2l6qjfdDiwVmidoZjA
```

Do you wish to trust these keys? [ynYN] y

To decrypt the data, just pass it to the clevis decrypt command:

```
$ clevis decrypt < JWE > PT
```

As you can see above, Tang utilizes a trust-on-first-use workflow. If

you already know the thumbprint of a trusted key, you can specify it in the configuration at encryption time:

```
$ cfg='{ "url": "http://tang.srv", "thp": "_Oslk0T-E2l6qjfdDiwVmid0ZjA" }'  
$ clevis encrypt tang "$cfg" < PT > JWE
```

Obtaining the thumbprint of a trusted signing key is easy. If you have access to the Tang server, simply execute:

```
$ tang-show-keys <PORT>
```

where <PORT> is the port that the Tang server is listening on.

If tang-show-keys is not available, but you have access to the Tang server's database directory, you can execute this instead:

```
$ jose jwk thp -i $DBDIR/$SIG.jwk
```

Tang can also perform entirely offline encryption if you pre-share the server advertisement. You can fetch the advertisement with a simple command (just be careful your network isn't compromised!):

```
$ curl -f $URL/adv > adv.jws
```

Once you have the advertisement file, just provide it:

```
$ clevis encrypt tang '{ "url": "...", "adv": "adv.jws" }' < PT > JWE
```

## CONFIG

This command uses the following configuration properties:

- ? url (string) : The base URL of the Tang server (REQUIRED)
- ? thp (string) : The thumbprint of a trusted signing key
- ? adv (string) : A filename containing a trusted advertisement
- ? adv (object) : A trusted advertisement (raw JSON)

## OPTIONS

- ? -y : Automatically answer yes for all questions. Use this option for skipping the advertisement trust check. This can be useful in automated deployments:

```
$ clevis encrypt tang '{ "url": "... }' -y < PT > JWE
```

## SEE ALSO

clevis-decrypt(1)

01/25/2023

CLEVIS-ENCRYPT-TAN(1)