Red Hat
Enterprise Linux

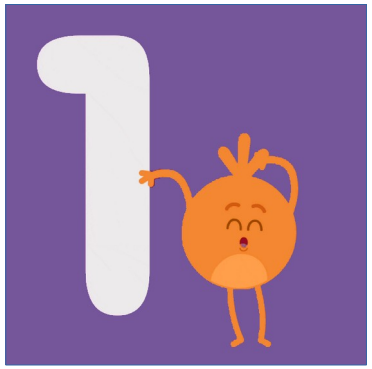
Red Hat RHEL9 Security Tip #1

Marc Skinner
Principal Soloutions Architect

Red Hat

TIP #1

Encryption at rest – encrypted file systems using LUKS



Red Hat

What is LUKS?

Linux **U**nified **K**ey **S**etup

Encrypt a block device, logical device or a partition

Requires a passphrase – stored in one KeySlot
Can store multiple passphrases

Ciphers
- Default = aes-xts-plain64
- AES
- Twofish
- Serpent

KeySize
- Default = 512 bits

cryptsetup benchmark

Red Hat

LUKS Setup – Passphrase Prompting

```
# cryptsetup luksFormat /dev/sdb
# cryptsetup luksDump /dev/sdb
# cryptsetup luksUUID /dev/sdb or # blkid /dev/sdb
# cryptsetup luksOpen /dev/sdb SECRET

### PROMPT FOR PASSPHRASE

# mkfs.xfs /dev/mapper/SECRET
# mount /dev/mapper/SECRET /mnt/SECRET
# blkid /dev/mapper/SECRET
```

Update files for mounting

/etc/crypttab

SECRET UUID=1e1f836b-fbcb-4907-949e-10a2661924b1 **none** luks,discard

/etc/fstab

UUID=831f480a-8b76-404b-b8bd-e0a41f69c1a6 /mnt/SECRET xfs defaults,discard 0 0

Red Hat

LUKS Setup – Passphrase in Keyfile

```
# cryptsetup luksFormat /dev/sdb
# cryptsetup luksDump /dev/sdb
# cryptsetup luksUUID /dev/sdb or # blkid /dev/sdb
# echo -n 'mysecretpassphrase' > /root/keyfile && history -c
# chmod 400 /root/keyfile
# cryptsetup luksOpen /dev/sdb SECRET --key-file /root/keyfile

# mkfs.xfs /dev/mapper/SECRET
# mount /dev/mapper/SECRET /mnt/SECRET
# blkid /dev/mapper/SECRET
```

Update files for mounting

/etc/crypttab

SECRET UUID=1e1f836b-fbcb-4907-949e-10a2661924b1 **/root/keyfile** luks,discard

/etc/fstab

UUID=831f480a-8b76-404b-b8bd-e0a41f69c1a6 /mnt/SECRET xfs defaults,discard 0 0

Red Hat

LUKS Upgrade/Conversion

LUKS2 was introduced in RHEL 7.6
LUKS2 supports 32 keys slots vs only 8 key slots in LUKS1
LUKS2 supports two JSON metadata headers
Can not upgrade LUKS1 to LUKS2 if
    Device is active
    CLEVIS is being used

```
# cypsetup luksHeaderBackup /dev/sdb --header-backup-file /root/luks-header-backup.bin
# cryptsetup convert --type luks2 /dev/sdb
```

LUKS Maintenance

LUKS2 supports online re-encryption

Change the encryption algorithm or key-size

MODES

Default = checksum (balance performance and protection)

journal (safest mode, requires two writes)

none (fastest mode)

cryptsetup reencrypt --resilience **MODE** --cipher twofish-xts-plain64 /dev/sdb
cryptsetup reencrypt --resilience **MODE** --key-size 256 /dev/sdb (*must be multiple of 8*)

LUKS2 re-encryption recovery will trigger automatically on next
“cryptsetup open” or “cryptsetup repair” command

LUKS1 does NOT support online re-encryption

Red Hat

LUKS Maintenance

LUKS2 supports passphrase additions, removals

View Keyslots
cryptsetup luksDump /dev/sdb

Change Passphrase
cryptsetup luksChangeKey /dev/sdb

Add Passphrase
cryptsetup luksAddKey /dev/sdb

Remove Passphrase
cryptsetup luksRemoveKey /dev/sdb

LUKS Encrypt existing File System?

Yes, it is possible

For XFS filesystem:
First need to unmount and extend existing file system by 32M for LUKS Header

```
# umount /mnt/DATA
# lvextend -L+32M /dev/mapper/NVME2048
```

Create LUKS volume with **reencrypt** option

```
# cryptsetup reencrypt --encrypt --reduce-device-size=32M /dev/mapper/NVME2048
# cryptsetup luksOpen /dev/mapper/NVME2048 SECRET
# mount /dev/mapper/SECRET /mnt/SECRET
```

For ext4, a filesystem you can also shrink by 32M vs extending if you want.
XFS can NOT shrink filesystems.

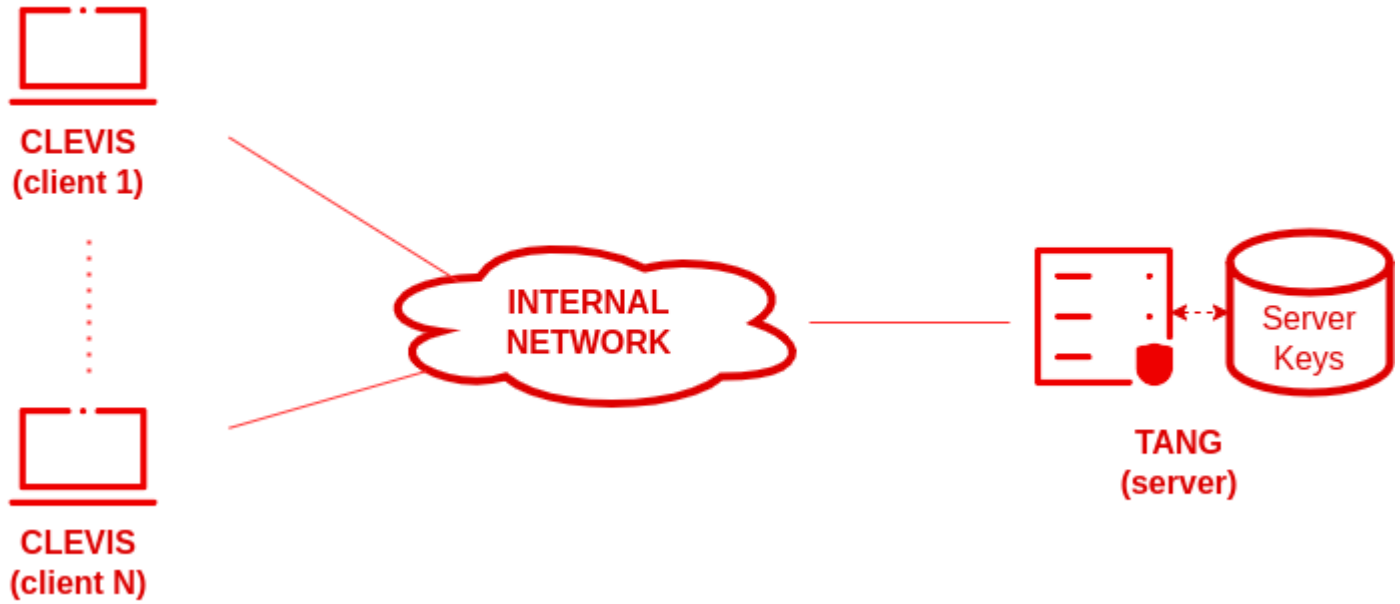
LUKS Removal

```
# cryptsetup status /dev/mapper/SECRET
# cryptsetup luksClose SECRET
# cryptsetup erase /dev/sdb

### PROMPT FOR PASSPHRASE
```

LUKS Network Bound Disk Encryption (NBDE)

Feature to unlock a LUKS volume via a network connection from a service
CLEVIS (client) → TANG (server/service)



Leverages the private/public key exchange algorithm: McCallum-Relyea

Red Hat

NBDE TANG Server Setup

```
# dnf -y install tang
# systemctl enable tangd.socket --now
```

Check for TANG service connectivity, is service publishing public keys?

```
# curl -f http://tang1.i.skinnerlabs.com/adv
# curl -f http://tang2.i.skinnerlabs.com/adv
```

NBDE CLEVIS Client

Supports three modes:

- tang (single remote key lookup)
- tpm2 (Trusted Platform Module 2.0)
- sss (multiple tang servers “Shamir’s Secret Sharing”)

LUKS NBDE CLEVIS Setup / Registration

dnf -y install clevis clevis-luks clevis-dracut

Bind TANG pin/token to an existing LUKS volume SECRET

clevis luks bind -d /dev/mapper/SECRET **tang** ‘{“url”: “http://tang1.i.skinnerlabs.com”}’

Or Bind to multiple pins/tokens to an existing LUKS volume SECRET

clevis luks bind -d /dev/mapper/SECRET **sss**
'{"t":1,"pins":{"tang":[{"url":"http://tang1.i.skinnerlabs.com"},{"url":"http://tang2.i.skinnerlabs.com"}]}}'

clevis luks list -d /dev/mapper/SECRET

/etc/crypttab
SECRET UUID=1e1f836b-fbcb-4907-949e-10a2661924b1 **none** luks,discard

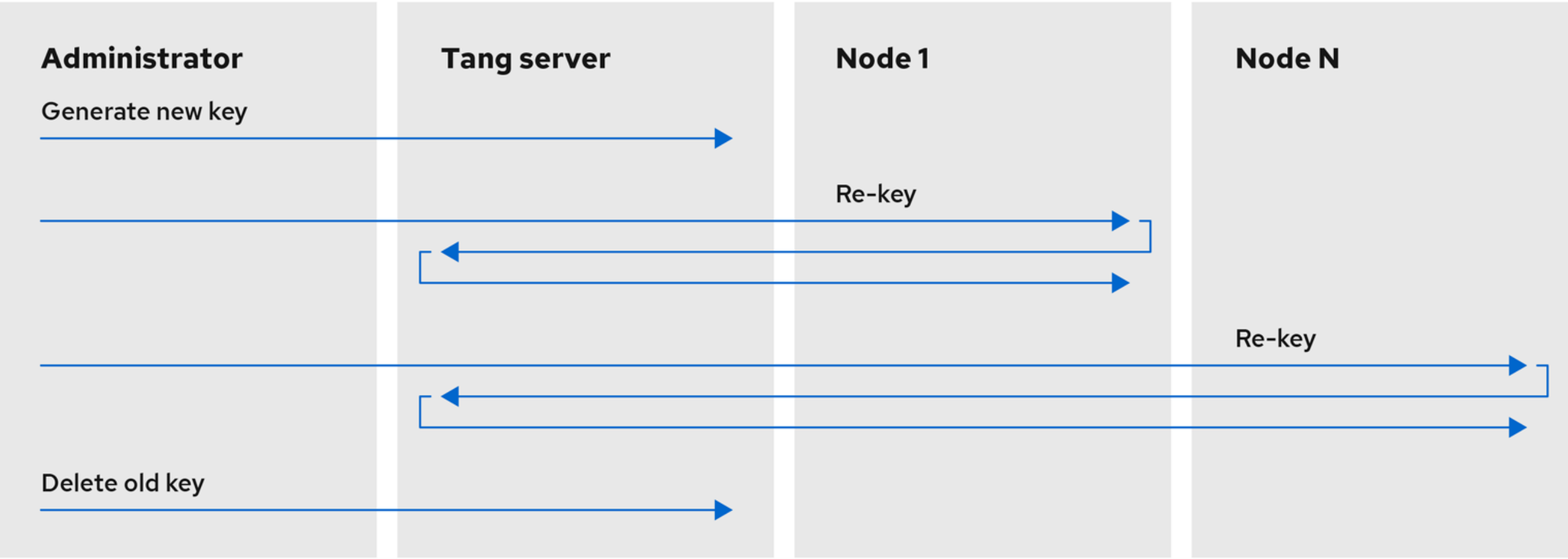
Red Hat

LUKS NBDE on root?

```
# grubby --update-kernel=ALL --args="rd.neednet=1"
# dracut -fv –-regenerate-all
```

Red Hat

LUKS NBDE TANG/CLEVIS Key Rotation



Red Hat

LUKS NBDE TANG/CLEVIS Key Rotation

On TANG Server:

Private keys are stored at: /var/db/tang

Rotate TANG keys:
tang-show-keys
tangd-keygen /var/db/tang

Delete old keys after ALL clients updated!

On CLEVIS Client:

clevis luks list -d /dev/mapper/SECRET -s 1
clevis luks regen -d /dev/mapper/SECRET -s 1
OR
clevis luks unbind -d /dev/mapper/SECRET -s 1
THEN REBIND

CLEVIS Trusted Platform Module (TPM2) Registration

Does your devices have TPM?

```
# ls /dev/tpm*
# cat /sys/class/tpm/tpm*/tpm_version_major
```

```
# clevis luks bind -d /dev/sdb tpm2 '{"hash":"sha256","key":"rsa","pcr_bank":"sha256","pcr_ids":"0,1"}'
# clevis luks list -d /dev/sdb
```

```
/etc/crypttab
SECRET UUID=831f480a-8b76-404b-b8bd-e0a41f69c1a6
```

OR

```
# systemd-cryptenroll --tpm2-device=auto --tpm2-pcrs=0,1 /dev/sdb
```

```
/etc/crypttab
SECRET UUID=1e1f836b-fbcb-4907-949e-10a2661924b1 - --tpm2-device=auto
```

Red Hat

LUKS NBDE RHEL System Roles (now over 30)

dnf -y install rhel-system-roles ansible-core

Configure CLEVIS clients (does not currently support CLEVIS TPM2)
nbde_client

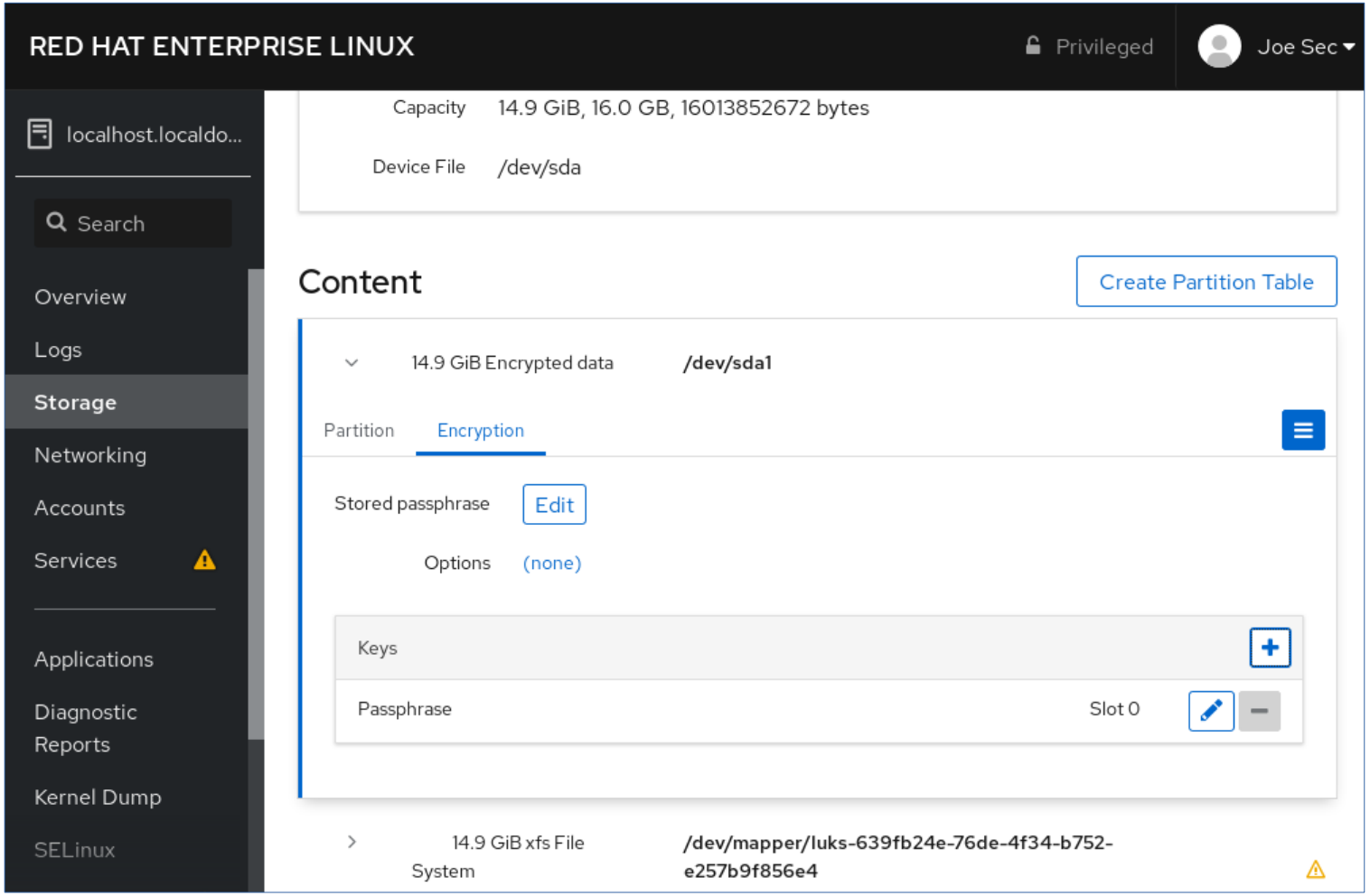
Configure TANG server
nbde_server

Documentation and examples:

/usr/share/doc/rhel-system-roles/nbde_client/
/usr/share/ansible/roles/rhel-system-roles.nbde_server/

LUKS NBDE CLEVIS with Cockpit

dnf -y install cockpit-storaged, cockpit



Red Hat

LUKS Kickstart Options

part pv.01 --size=10240 --grow **--encrypted** --passphrase=kickstart

--encrypted
--passphrase
--escrowcert
--backuppassphrase
--cipher
--luks-version

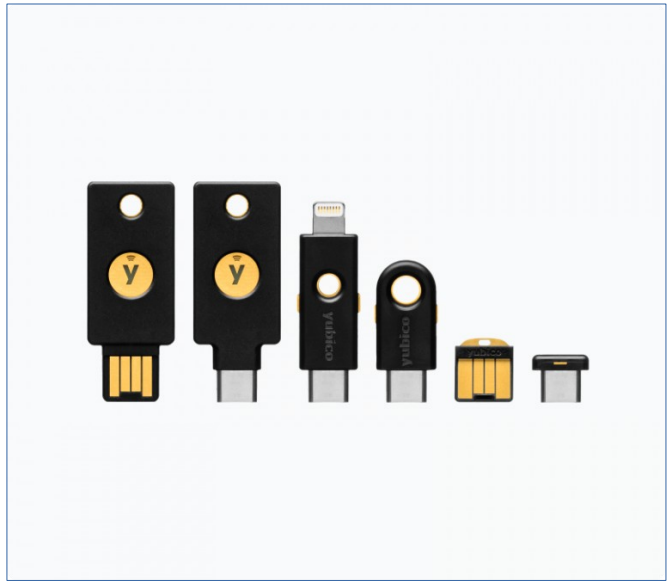
YubiKey Registration

What is a YubiKey?

Two-factor authentication device

dnf -y install ykpers yubikey-manager-qt

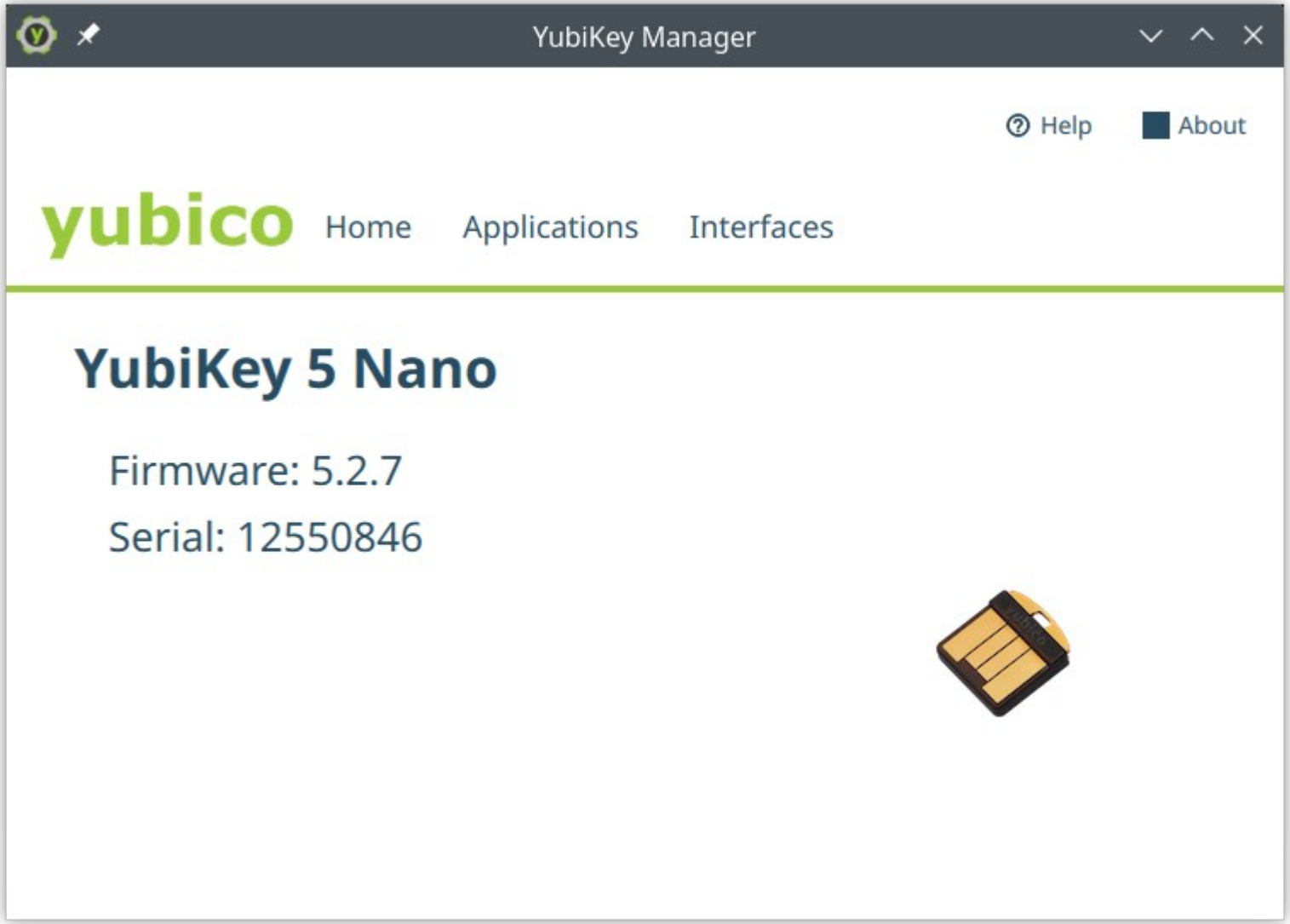
Launch YubiKey Manager GUI



Red Hat

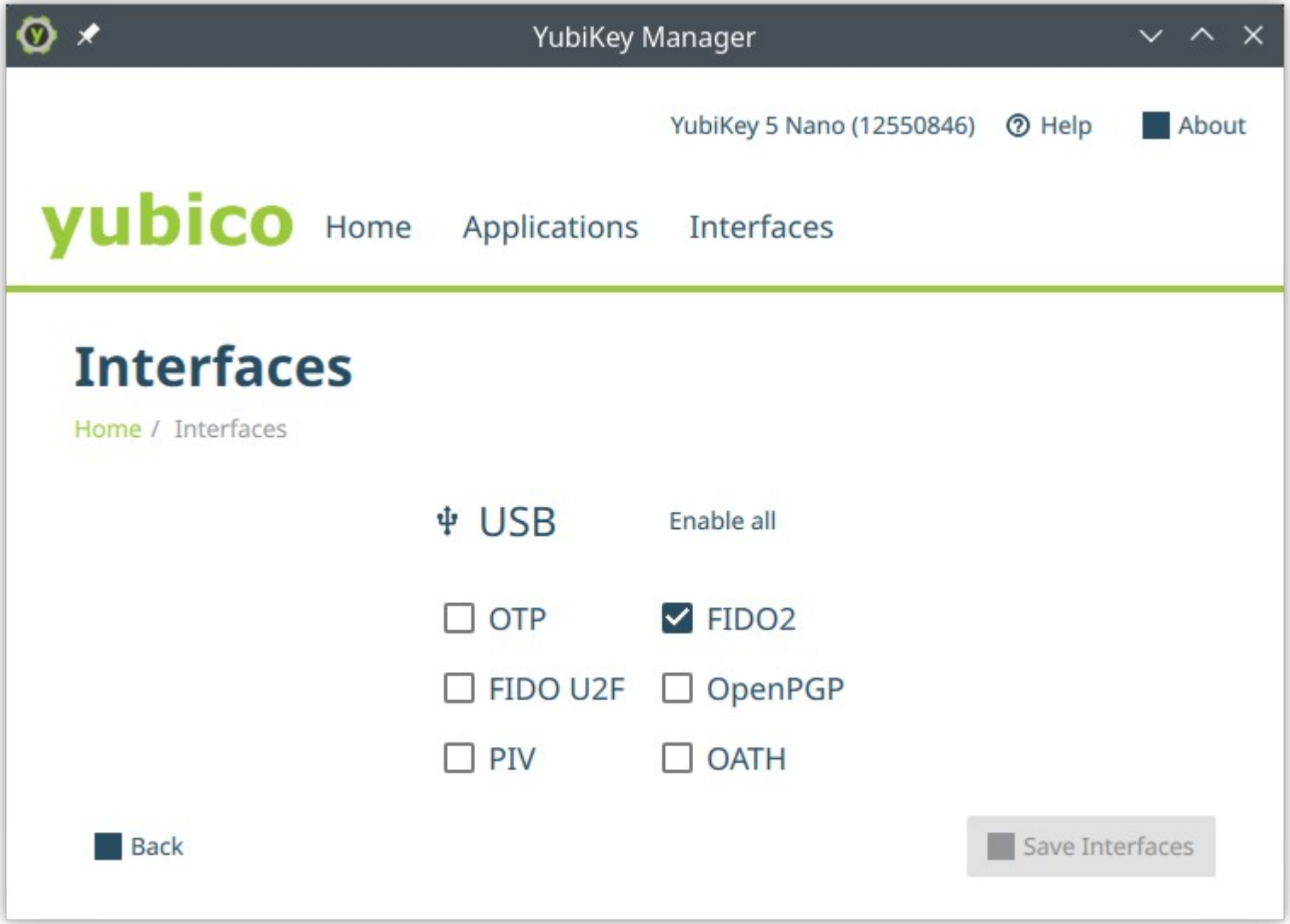
YubiKey Manager

Get details about your YubiKey
Is it detected?



YubiKey Manager

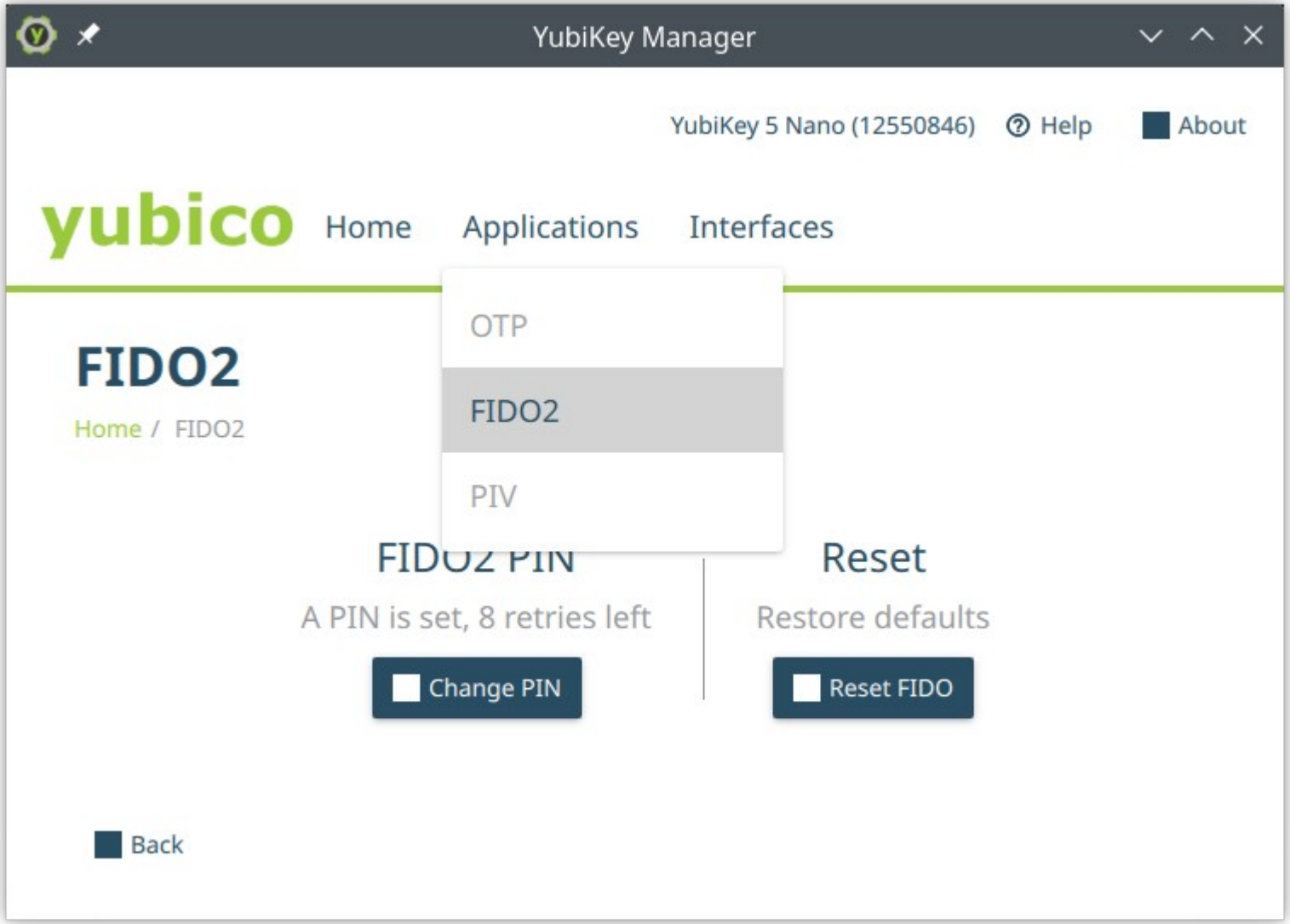
Enable only FIDO2 Interface



Red Hat

YubiKey Manager

Select FIDO2
Change PIN via GUI



Red Hat

YubiKey Binding

Updated pin via CLI
ykman fido access change-pin

Confirm YubiKey settings and detection
systemd-cryptenroll --fido2-device=list

Bind YubiKey to LUKS device
systemd-cryptenroll /dev/mapper/NVME2048 --fido2-device=auto –-fido2-with-client-pin=yes

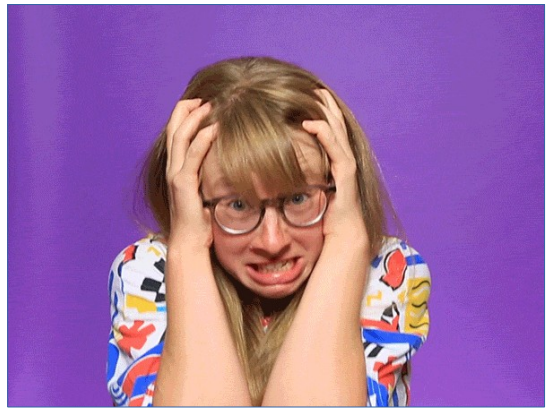
OR

systemd-cryptenroll /dev/mapper/NVME2048 --fido2-device=auto
--fido2-with-client-pin=yes -–wipe-slot=fido2

/etc/crypttab
SECRET UUID=1e1f836b-fbcb-4907-949e-10a2661924b1 none luks,discard,fido2-device=auto

Red Hat

YubiKey Gotcha



Which KeySlot was consumed by FIDO2?
cryptsetup luksDump /dev/mapper/NVME2048

If it is KeySlot 2, you will need to press your YubiKey twice
If it is KeySlot 3, you will need to press your YubiKey thrice
Etc …

I recommend making sure your FIDO2 KeySlot is assigned to slot 1, or this will drive you crazy!

Which Option is Best?

TYPE	INTERACTIVE	AUTOMATED	TIED TO SYSTEM	TIED TO NETWORK	MULTIFACTOR
Passphrase	X				
Keyfile		X	X/*	X/*	
NBDE CLEVIS		X		X	
CLEVIS TPM2		X	X		
TPM2		X	X		
YUBIKEY	X				X

* Depends on where Keyfile is stored: local disk or network disk

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat