# Oracle Linux

## Enabling Network-Bound Disk Encryption

F43691-07
June 2022

Oracle Linux Enabling Network-Bound Disk Encryption,

F43691-07

# Contents

# Preface

Oracle Linux: Enabling Network-Bound Disk Encryption provides information about the Tang server and Clevis framework, used to implement Network-Bound Disk Encryption (NBDE) on Oracle Linux systems. The instructions provided in this document are tested on Oracle Linux 8 and on Oracle LInux 9 but the tools and services are equally available for Oracle Linux 7 and work similarly. Commands to install software using `dnf` can be substituted with `yum` equivalents where required.

## Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

## Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

# Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

# About Network-Bound Disk Encryption

This chapter provides an overview of the Network-Bound Disk Encryption (NBDE) methodology and how the feature works with other Oracle Linux encryption features.

Network-Bound Disk Encryption (NBDE) is a methodology that is used to automatically encrypt and decrypt disks or volumes by using a network-based resource to obtain the information that is required to perform decryption. This facility extends Linux Unified Key Setup (LUKS), which is commonly used to encrypt disks and volumes on Oracle Linux to provide an additional mode of security, as well as facilitate automated decryption at boot.

While LUKS is useful for encrypting data and protecting it when it is not in use, for server systems, LUKS can pose a problem if the root partition is encrypted because it requires a passphrase to be entered at boot to decrypt the data. NBDE helps to solve this issue by using a network-based resource to obtain a key that LUKS uses to perform the decryption automatically at boot. In this security model, the data on the disk is protected as long as the system boots within a trusted network. If the disk is removed from the server and is not booted within the trusted network, the data remains encrypted, unless the usual LUKS passphrase is provided.

NBDE is achieved on Oracle Linux by configuring a Tang server on your trusted network and then installing the Clevis decryption software on the client host where the encryption is used. Tang runs a simple web-based service that uses HTTP to advertise a public signing key that is used by clients to generate key pairs which are used to encrypt data. The Clevis client generates a strong cryptographic key pair, using the signing key that is provided by the Tang server, to perform an encryption. Encryption is performed by using the generated private key, which is discarded after encryption is complete, thereby protecting the data until the private key is reconstituted.

The Clevis client uses an ephemeral key to obtain the information that is required from the Tang server to reconstitute the private key so that it can decrypt the data. This process is known as the McCallum-Relyea exchange and has the advantage of avoiding key escrow, which can result in management overhead and can also introduce security risks. In this key exchange process, the keys that are used to encrypt the data on the client side are never directly shared with the Tang server and never actually move across the network. All of the information that is exchanged is either public or encrypted by nature, which means that no TLS is required either.

Because LUKS can store multiple keys in different slots that are used to decrypt data, the primary passphrase that is used to lock a disk or a volume can be maintained alongside the key that is provided for NBDE. At boot, the usual passphrase prompt is displayed for LUKS decryption to allow passphrase entry, but if Clevis is able to contact the Tang server no user input is required and the passphrase prompt closes automatically after the key is decrypted and access is granted to the data that is stored on the disk or volume.

More information about the Tang server is available at https://github.com/latchset/tang.

More information about the Clevis framework is available at https://github.com/latchset/clevis.

General information about public key cryptography is available in Oracle Linux: Managing Certificates and Public Key Infrastructure.

Information about using LUKS for disk encryption is available in Oracle Linux 8: Managing Storage Devices and Oracle Linux 9: Managing Storage Devices

2

# Install and Configure a Tang Server

A Tang server is used to store and manage encryption keys that are accessed by a Clevis client to perform automatic encryption and decryption. The following instructions describe how to install and configure the Tang server and how to initialize it with a set of signing keys.

## Install the Tang Package and Enable the Tang Socket in Systemd

Install the Tang package and related dependencies.

```
sudo dnf install -y tang
```

Enable the Tang socket in Systemd.

```
sudo systemctl enable tangd.socket
```

## Optionally Configure the Tang Server to Run on a Specified Port

By default, Tang runs on TCP port 80. If you intend to override this setting to run your Tang server on an alternate port, you must configure SELinux to allow Tang to work with the desired TCP port.

For example, to configure Tang to listen on TCP port 7500, run:

```
sudo semanage port -a -t tangd_port_t -p tcp 7500
```

If you have chosen to run Tang on an alternate port, you must configure a Systemd override by configuring a Socket entry:

```
sudo mkdir -p /etc/systemd/system/tangd.socket.d/
sudo cat <<EOF > /etc/systemd/system/tangd.socket.d/port.conf
[Socket]
ListenStream=
ListenStream=7500
EOF
```

If you edit Systemd configuration you must reload Systemd daemon configuration for the changes to take effect:

```
sudo systemctl daemon-reload
```

## Update the Firewall Policy

Set firewall policy to allow traffic on the TCP port that you configure Tang to run on and make the rule permanent. In this example it is assumed that an alternate port is configured for the Tang server.

```
sudo firewall-cmd --add-port=7500/tcp
sudo firewall-cmd --runtime-to-permanent
```

# Start the Systemd Tang Socket

Start the Tang socket to allow incoming connections to access the Tang server:

```
sudo systemctl start tangd.socket
```

The Tang process runs when a connection is initiated on the configured socket.

# Initialize Tang Signing Keys

Initialize keys for Tang to use by running.

```
sudo /usr/libexec/tangd-keygen /var/db/tang
```

Check that one of the keys in `/var/db/tang` is advertised by the Tang server on the port for which you have configured it to listen, for example:

```
sudo tang-show-keys 7500
```

You can use the output from this command to validate the key hash that is used when you configure a client to use this Tang server.

# Rotate Tang Keys

Periodically you should rotate your Tang keys to improve security. Rotaion of keys is manual and is not a mandatory procedure.

To rotate Tang keys, simply rename old keys within the `/var/db/tang` directory to prefix them with a period (.) so that they are hidden and rerun the initialization command. For example:

```
cd /var/db/tang; for i in *; do mv $i .$i; done
sudo /usr/libexec/tangd-keygen /var/db/tang
```

When you are absolutely certain that no client systems are still dependent on any of the old keys you can remove them from the system. Removing the old keys while clients are still using them will result in a failed attempt to unlock a disk or volume and you must provide an existing LUKS passphrase manually at boot.

When you rotate keys on the Tang server, you must update clients to use the new keys. See Update Clevis for Tang Key Rotation for more information.

3

# Perform Automated Encryption and Decryption With Clevis

Clevis is client software that can perform automated decryption by using different plugin provider services. Clevis works well with the Tang server provider and can handle encryption and decryption operations securely while avoiding key escrow.

You can use Clevis with LUKS to automatically unlock encrypted storage. Tools are also provided to integrate with Dracut so that you can update your initrd boot image to enable Clevis to be used at boot to automatically decrypt a device, provided that the system has access to the Tang server.

## Install and Test Clevis

The following instructions describe how to install the Clevis client software on your Oracle Linux instance, how to test the Clevis software by performing a basic encryption task using keys provided by a Tang server, and how to update existing initrd boot images to integrate with the Clevis client for automatic decryption of LUKS encrypted partitions at boot time.

### Install the Clevis Packages

Install the `clevis` package and related dependencies.

```
sudo dnf install -y clevis clevis-luks clevis-udisks2 clevis-dracut
```

Each package has a different function:

- `clevis` provides the basic decryption client that is capable of communicating with a Tang server
- `clevis-luks` is required to integrate Clevis with LUKS to perform automatic disk or volume decryption
- `clevis-udisks2` is required to integrate Clevis with the udisks framework that is used for removable storage so the Clevis can trigger to perform LUKS decryption on removable disks
- `clevis-dracut` is required to integrate Clevis with Dracut so that the Clevis tools can be included in initrd images for early boot integration

### Test Clevis

To test that Clevis is able to encrypt data using the keys provided by the Tang server, follow these steps:

1. Create a plain text file with some content that you intend to encrypt:

   ```
   echo "this is my secret message" > unencrypted.txt
   ```

2. Encrypt the plain text file using the Tang server that you have set up and configured on your network and pipe the output into an a separate file.

Note that the command also prompts you to turst the signing key.

```
clevis encrypt tang '{"url":"http://tang-server.example.org:7500"}' <
unencrypted.txt > secret.jwe
...
The advertisement contains the following signing keys:

i9sPMu_sn6vMjzyJm8ZALj7opDE

Do you wish to trust these keys? [ynYN] Y
```

The Tang server responds to the request by providing a signing key that is used to restore the strong cryptographic key that is used to encrypt the data during the provisioning process.

3. You can inspect the encrypted content that is returned by the `clevis encrypt` command as follows:

```
cat secret.jwe
eyJhbGciOiJFQ0RILUVTIiwiY2xldmlzIjp7InBpbiI6InRhbmciLCJ0YW5n
Ijp7ImFkdiI6eyJrZXlzIjpbeyJhbGciOiJFQ01SIiwiY3J2IjoiUC01MjEi
LCJrZXlfb3BzIjpbImRlcml2ZUtleSJdLCJrdHkiOiJFQyIsIngiOiJBUVNs
...
bTJIWkpva19ETXZXTzVBejN0Zzg0dzBRd01xam9pczVnVFNzZlhTbERyNUVI
```

4. Decrypt the data in the encrypted file to ensure that decryption is possible:

```
cat secret.jwe |clevis decrypt
this is my secret message
```

The `clevis decrypt` command uses metadata that is stored during the encryption process to derive the key used to decrypt the data through information returned from a POST request to the Tang server.

## Update initrd Boot Images for Clevis Integration

The `clevis-dracut` package is installed so that Clevis operations can be introduced into the initrd boot image for early boot decryption operations. After you have installed this package, you can run the `dracut` command to rebuild your existing initrd boot image to integrate it with Clevis:

```
sudo dracut -f
```

This step makes it possible for Clevis to unlock a LUKS encrypted partition at boot time, as long as the Tang server is accessible. Note that you are still prompted for a LUKS passphrase at boot; but, if one is not provided and Clevis is able to contact the Tang server, LUKS is able to unlock the device and the passphrase prompt closes after a period of time.

# Use Clevis With LUKS

Clevis includes LUKS integration that allows you to bind Clevis to a LUKS slot for any volume or device that is LUKS encrypted. Once Clevis is bound to a LUKS slot, automatic network-bound decryption is triggered when a user would usually be prompted for a LUKS passphrase entry.

The following instructions explain how to bind and unbind Clevis against a LUKS slot, verify that Clevis is integrated with LUKS for a volume or device and update Clevis for a volume or device if the Tang keys are rotated.

## Bind Clevis to a LUKS Slot

To bind Clevis to a LUKS slot to unlock a LUKS encrypted device by using a Tang server, run the `clevis luks bind` command. Note that the command prompts you to trust the key that is being advertised by the Tang server. Likewise, the command prompts you for the LUKS password.

When typing the command, provide the path to the device that is LUKS encrypted. In the following example, the system uses LVM and the root volume is LUKS encrypted, so */dev/ol/root* is used as the device path. You could equally use a block device such as `/dev/sda1`. Also, you must provide the URL to the Tang server in a JSON string.

See the following example:

```
sudo clevis luks bind -d /dev/ol/root tang '{"url": "http://tang-
server.example.org:7500"}'
...
The advertisement is signed with the following keys:
        i9sPMu_sn6vMjzyJm8ZALj7opDE

Do you wish to trust the advertisement? [yN] y
Enter existing LUKS password:
```

This operation performs several steps:

- Clevis creates a new key with the same entropy as the primary LUKS key.
- The new key is encrypted by Clevis using the Tang key.
- Clevis stores the token and metadata to contact the Tang server in the LUKS header.
- The key is enabled for use with LUKS.

## Verify Clevis Integration with LUKS

You can check the LUKSMeta information for a device by using the `cryptsetup` command, for example:

```
sudo cryptsetup luksDump /dev/ol/root
```

You should notice that the Clevis key has been added to one of the slots and a `clevis` token is assigned for that slot.

You can also check which slot is used by Clevis and the Tang server information for the binding by running the `clevis luks list` command, for example:

```
sudo clevis luks list -d /dev/ol/root
```

If the device is required at boot and `clevis-dracut` is installed and configured, the system continues to prompt you for a LUKS passphrase at boot; however, Clevis attempts to decrypt its key by using the Tang server and unlocks the device automatically. The passphrase prompt closes after a period of time if Clevis is successful.

# Update Clevis for Tang Key Rotation

Periodically a Tang server administrator may rotate Tang keys on the server for additional security. When this happens, it is possible that Clevis is unable to decrypt the LUKS token correctly and this must be regenerated using the new Tang key. If Clevis fails to decrypt the LUKS token, you must authenticate to LUKS using passphrase entry at boot.

To check whether Tang keys have been rotated and to regenerate a newly encrypted token, perform the following steps:

1. Identify the LUKS slot that Clevis is bound to:

   ```
   sudo clevis luks list -d /dev/ol/root

   1: tang '{"url":"http://tang-server.example.org:7500"}'
   ```

2. Obtain a report for the LUKS slot to indicate whether the Tang key has been updated and to automatically regenerate the LUKS token:

   ```
   sudo clevis luks report -d /dev/ol/root -s 1

   ...
   Report detected that some keys were rotated.
   Do you want to regenerate luks metadata with
   "clevis luks regen -d /dev/ol/root -s 1"? [ynYN]
   ```

   Enter `y` to allow Clevis to automatically regenerate the LUKS token.

Note that you can optionally unbind Clevis from an existing LUKS slot and then bind it again if the instructions to regenerate a token do not work for you.

# Unbind Clevis from a LUKS Slot

You can unbind Clevis from a LUKS slot by using the `clevis luks unbind` command:

```
sudo clevis luks unbind -d /dev/ol/root -s 1
```

Note that you must specify the slot number that Clevis is currently bound to by specifying the `-s` option, followed by the slot number. Be aware that this operation is destructive and wipes the LUKSMeta data for the slot that is specified, so you are prompted to confirm the operation.