SSL-TLS: the SSL/TLS protocol is designed to securely negotiate encryption keys without ever transmitting private keys over the network

- Public key (public lock) → for encryption
- Private key → for decryption

How use SSL for our web server:

① this server send CSR to any CA

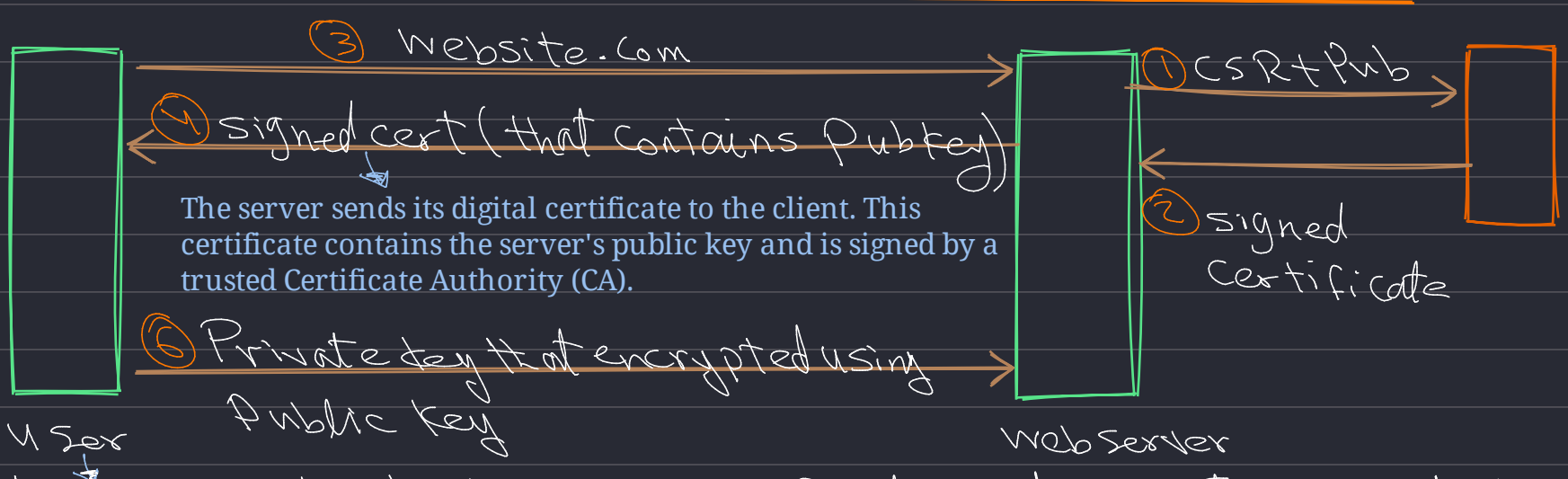
Certificate Signing Request (CSR) :

A Certificate Signing Request (CSR) is a message sent from an applicant to a Certificate Authority (CA) to apply for a digital certificate. The CSR contains information that will be included in the certificate, such as the organization name, domain name, and public key.

Certificate Authority (CA) :

A Certificate Authority (CA) is an entity that issues digital certificates. The CA verifies the information provided in the CSR and, if the information is deemed valid, issues a certificate that binds the public key to the identified entity

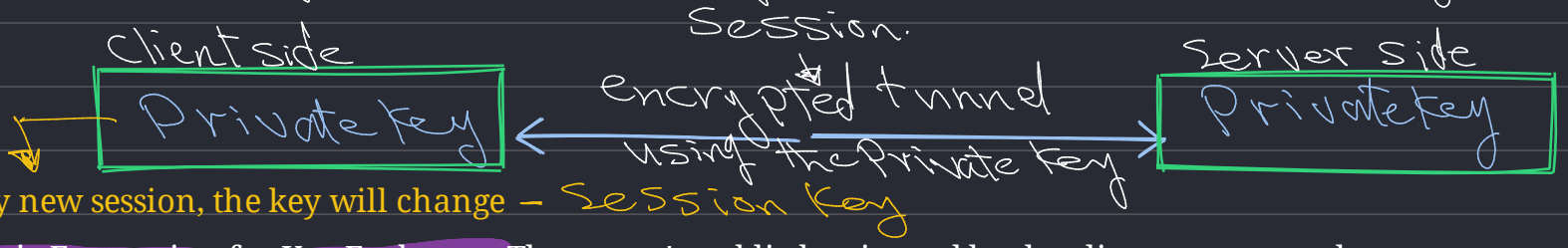
② CA generates a certificate and Sends a certificate to the server



⑤ client browser will check this certificate, and generate a private key then encrypt it using the public key

⑦ web server will decrypt the message in order to get the private key.

⑧ User send the username and password encrypted and the server can decrypt it using the private key then the two sides are ready to start secure session.



With every new session, the key will change – Session key

- Asymmetric Encryption for Key Exchange: The server's public key is used by the client to encrypt the pre-master secret. Only the server can decrypt this with its private key.
- Symmetric Encryption for Data Transmission: Once the session keys are established, symmetric encryption is used for the actual data transmission, providing both security and efficiency.

- How to create Self-signed certificate: Priv key >> CA cert >> CSR >> Cert

① Generate Private key:

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# openssl genrsa -des3 -out myCA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.............................+++++
e is 65537 (0x010001)
Enter pass phrase for myCA.key:
Verifying - Enter pass phrase for myCA.key:
root@ubuntu-vm-01:/home/ubuntu/ssl-dir#
```

encrypt this key using des3 algorithm

decrypt this key using this password

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# ls
myCA.key
root@ubuntu-vm-01:/home/ubuntu/ssl-dir#
```

② Generate a certificate (self signed certificate) using this Private key:

→ Private key

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# openssl req -x509 -new -nodes -key myCA.key -sha256 -days 3650 -out myCA.pem
Enter pass phrase for myCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

→ need to decrypt the Private key so it ask me about the password

→ CA cert

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# ls
myCA.key  myCA.pem
```

→ CA Certificate

③ Generate another Private key and generate CSR for the website:

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# openssl genrsa -out tls.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.................+++++
.........+++++
e is 65537 (0x010001)
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# ls
myCA.key  myCA.pem  tls.key
```

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# openssl req -new -key tls.key -out tls.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:mytest.website
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# ls
myCA.key  myCA.pem  tls.csr  tls.key
root@ubuntu-vm-01:/home/ubuntu/ssl-dir#
```

The public key is embedded within the CSR

④ issued this certificate using CA:

```
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# openssl x509 -req -in tls.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out tls.crt -days 365 -sha256
Signature ok
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = mytest.website
Getting CA Private Key
Enter pass phrase for myCA.key:
root@ubuntu-vm-01:/home/ubuntu/ssl-dir# ls
myCA.key  myCA.pem  myCA.srl  tls.crt  tls.csr  tls.key
root@ubuntu-vm-01:/home/ubuntu/ssl-dir#
```

→ website certificate

to read the CSR contents:

```
# openssl x509 -text -in tls.crt | less
```

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            33:23:40:5a:78:5d:39:dc:59:54:17:23:1f:b4:a6:28:c5:d5:53:ef
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = EG, ST = Some-State, O = Internet Widgits Pty Ltd, CN = myprivate.ca
        Validity
            Not Before: May  8 07:21:23 2022 GMT
            Not After : May  8 07:21:23 2023 GMT
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = mytest.website
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c2:eb:15:28:ed:92:c6:9b:81:f3:f7:91:d0:d9:
                    42:68:e9:87:7b:68:34:77:fc:ea:63:8f:7d:df:be:
                    54:d0:ed:e0:a3:0b:bf:54:89:93:da:64:5b:ab:13:
                    40:21:c1:b5:af:b4:34:9e:ef:13:da:9f:3d:b3:8b:
                    fa:84:a5:df:e5:90:8c:06:9b:08:0b:cb:61:75:8f:
                    20:68:0a:08:64:68:ad:ba:a9:19:76:48:9a:4e:11:
                    6c:c6:f9:a6:40:f9:2b:93:d1:03:77:0a:d2:23:34:
                    2c:fa:b8:8a:62:1d:2e:0b:8b:93:e9:c6:60:a7:b3:
                    84:d7:bd:55:25:c8:a6:e4:7f:9d:68:03:48:b9:0d:
                    54:f7:9b:46:bb:a0:91:b5:f4:07:18:2a:9c:66:84:
                    f2:4d:ef:e3:3e:03:0e:2c:b6:08:ba:f8:5c:09:a6:
```

⑤ import this certificate from any browser and open: https: <link>

LVM:
stands for Logical Volume Manager. It's a tool that provides a more flexible and powerful way to manage storage space compared to traditional partitioning.

```
[aaron@LFCS-CentOS ~]$ sudo lvmdiskscan
[sudo] password for aaron:
  /dev/sda1 [       1.00 GiB]
  /dev/sda2 [     <19.00 GiB] LVM physical volume
  /dev/sdb1 [       4.00 GiB]
  /dev/sdb2 [       4.00 GiB]
  /dev/sdb3 [      <2.00 GiB]
  /dev/sdc  [       5.00 GiB]
  /dev/sdd  [       5.00 GiB]
  /dev/sde  [       5.00 GiB]
  3 disks
  4 partitions
  0 LVM physical volume whole disks
  1 LVM physical volume
[aaron@LFCS-CentOS ~]$
```

① Convert From Physical disk to Physical Volume:

```
[aaron@LFCS-CentOS ~]$ sudo pvcreate /dev/sdc /dev/sdd
  Physical volume "/dev/sdc" successfully created.
  Physical volume "/dev/sdd" successfully created.
[aaron@LFCS-CentOS ~]$
```

- display information about physical volumes:

```
[aaron@LFCS-CentOS ~]$ sudo pvs
  PV         VG Fmt  Attr PSize   PFree
  /dev/sda2  cs lvm2 a--  <19.00g    0
  /dev/sdc      lvm2 ---    5.00g 5.00g
  /dev/sdd      lvm2 ---    5.00g 5.00g
[aaron@LFCS-CentOS ~]$
```

sh Copy code

```
$ sudo pvs
  PV         VG     Fmt  Attr PSize   PFree
  /dev/sda1  my_vg  lvm2 a--  100.00g  50.00g
  /dev/sdb1  my_vg  lvm2 a--  200.00g 150.00g
```

In this example:

- `/dev/sda1` and `/dev/sdb1` are physical volumes.
- Both physical volumes are part of the volume group `my_vg`.
- The format is `lvm2`.
- The attributes are `a--` which indicates the physical volume is active.
- `/dev/sda1` has a size of `100.00g` with `50.00g` free.
- `/dev/sdb1` has a size of `200.00g` with `150.00g` free.

2- to add the PVS to a VG or a volume group :

Volume group name

```
[aaron@LFCS-CentOS ~]$ sudo vgcreate my_volume /dev/sdc /dev/sdd
  Volume group "my_volume" successfully created
[aaron@LFCS-CentOS ~]$
```

VolumeSize(my_volume) = Size(/dev/sdc + /dev/sdd)

5G 5G

- to expand our volume group :

```
[aaron@LFCS-CentOS ~]$ sudo pvcreate /dev/sde
  Physical volume "/dev/sde" successfully created.
[aaron@LFCS-CentOS ~]$ sudo vgextend my_volume /dev/sde
  Volume group "my_volume" successfully extended
[aaron@LFCS-CentOS ~]$
```

- to display volume group:

```
[aaron@LFCS-CentOS ~]$ sudo vgs
  VG        #PV #LV #SN Attr   VSize   VFree
  cs          1   2   0 wz--n- <19.00g      0
  my_volume   3   0   0 wz--n- <14.99g <14.99g
[aaron@LFCS-CentOS ~]$
```

15G

- to remove PV from vg:

```
[aaron@LFCS-CentOS ~]$ sudo vgreduce my_volume /dev/sde
  Removed "/dev/sde" from volume group "my_volume"
[aaron@LFCS-CentOS ~]$ sudo pvremove /dev/sde
  Labels on physical volume "/dev/sde" successfully wiped.
[aaron@LFCS-CentOS ~]$
```

Convert it to Physical disk

---

③ Create logical volume: Create Partition

```
[aaron@LFCS-CentOS ~]$ sudo lvcreate --size 2G --name partition1 my_volume
  Logical volume "partition1" created.
[aaron@LFCS-CentOS ~]$
```

vg

```
[aaron@LFCS-CentOS ~]$ sudo vgs
  VG         #PV #LV #SN Attr   VSize   VFree
  cs           1   2   0 wz--n- <19.00g    0
  my_volume    2   1   0 wz--n-   9.99g 7.99g
[aaron@LFCS-CentOS ~]$
```

```
[aaron@LFCS-CentOS ~]$ sudo lvcreate --size 6G --name partition2 my_volume
  Logical volume "partition2" created.
[aaron@LFCS-CentOS ~]$
```

```
[aaron@LFCS-CentOS ~]$ sudo lvs
  LV         VG        Attr       LSize   Pool Origin Data%  Meta%  Move Log Cpy
%Sync Convert
  root       cs        -wi-ao---- <17.00g

  swap       cs        -wi-ao----   2.00g

  partition1 my_volume -wi-a-----   2.00g

  partition2 my_volume -wi-a-----   6.00g

[aaron@LFCS-CentOS ~]$ sudo vgs
  VG         #PV #LV #SN Attr   VSize   VFree
  cs           1   2   0 wz--n- <19.00g    0
  my_volume    2   2   0 wz--n-   9.99g 1.99g
[aaron@LFCS-CentOS ~]$
```

- to expand the first logical volume to all the extents that it has available :

```
[aaron@LFCS-CentOS ~]$ sudo lvresize --extents 100%VG my_volume/partition1
  Reducing 100%VG to remaining free space 3.99 GiB in VG.
  Size of logical volume my_volume/partition1 changed from 2.00 GiB (512 extents
) to 3.99 GiB (1022 extents).
  Logical volume my_volume/partition1 successfully resized.
[aaron@LFCS-CentOS ~]$
```

- to shrink it again:

```
[aaron@LFCS-CentOS ~]$ sudo lvresize --size 2G my_volume/partition1
  WARNING: Reducing active logical volume to 2.00 GiB.
  THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce my_volume/partition1? [y/n]: y
  Size of logical volume my_volume/partition1 changed from 3.99 GiB (1022 extent
s) to 2.00 GiB (512 extents).
  Logical volume my_volume/partition1 successfully resized.
[aaron@LFCS-CentOS ~]$
```

- to create file system:

```
[aaron@LFCS-CentOS ~]$ sudo lvdisplay
  --- Logical volume ---
  LV Path                /dev/my_volume/partition1
  LV Name                partition1
  VG Name                my_volume
  LV UUID                EI1nFA-hqqM-F9Sp-3F7m-oPte-hElc-jRx4vN
  LV Write Access        read/write
  LV Creation host, time LFCS-CentOS, 2022-03-24 17:37:40 -0500
  LV Status              available
  # open                 0
  LV Size                2.00 GiB
  Current LE             512
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     8192
  Block device           253:2

  --- Logical volume ---
  LV Path                /dev/my_volume/partition2
  LV Name                partition2
```

```
[aaron@LFCS-CentOS ~]$ sudo mkfs.xfs /dev/my_volume/partition1
meta-data=/dev/my_volume/partition1 isize=512    agcount=4, agsize=131072 blks
         =                          sectsz=512   attr=2, projid32bit=1
         =                          crc=1        finobt=1, sparse=1, rmapbt=0
         =                          reflink=1    bigtime=0 inobtcount=0
data     =                          bsize=4096   blocks=524288, imaxpct=25
         =                          sunit=0      swidth=0 blks
naming   =version 2                 bsize=4096   ascii-ci=0, ftype=1
log      =internal log              bsize=4096   blocks=2560, version=2
         =                          sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                      extsz=4096   blocks=0, rtextents=0
[aaron@LFCS-CentOS ~]$
```

- to resize both the logical volume and the file system on it by passing another parameter :

```
[aaron@LFCS-CentOS ~]$ sudo lvresize --resizefs --size 3G my_volume/partition1
Phase 1 - find and verify superblock...
```

Without resize Parameter :

- That would only resize the logical volume from two gigabytes to three gigabytes. But that XFS file system still only use two gigabytes.

```
[aaron@LFCS-CentOS ~]$ sudo lvresize --size 3G myvolume/partition1
```

- keep in mind when you're doing this is that some file systems can be enlarged, they can be grown in size, but they can't shrink. So be aware of the limitations of the file system that you're using.

- Add these four disks as PVs (Physical Volumes) to LVM: /dev/vdb, /dev/vdc, /dev/vdd and /dev/vde :

```
[root@centos-host ~]# lvmdiskscan
  /dev/vda1 [      <10.00 GiB]
  /dev/vdb  [        1.00 GiB]
  /dev/vdc  [        1.00 GiB]
  /dev/vdd  [        1.00 GiB]
  /dev/vde  [        1.00 GiB]
  /dev/vdf  [        1.00 GiB]
  5 disks
  1 partition
  0 LVM physical volume whole disks
  0 LVM physical volumes
[root@centos-host ~]#
[root@centos-host ~]# pvcreate /dev/vdb /dev/vdc /dev/vdd /dev/vde
  Physical volume "/dev/vdb" successfully created.
  Physical volume "/dev/vdc" successfully created.
  Physical volume "/dev/vdd" successfully created.
  Physical volume "/dev/vde" successfully created.
  Creating devices file /etc/lvm/devices/system.devices
[root@centos-host ~]# lvmdiskscan
  /dev/vdb [        1.00 GiB] LVM physical volume
  /dev/vdc [        1.00 GiB] LVM physical volume
  /dev/vdd [        1.00 GiB] LVM physical volume
  /dev/vde [        1.00 GiB] LVM physical volume
  0 disks
  0 partitions
  4 LVM physical volume whole disks
  0 LVM physical volumes
[root@centos-host ~]# pvs
  PV         VG Fmt  Attr PSize PFree
  /dev/vdb      lvm2 ---  1.00g 1.00g
  /dev/vdc      lvm2 ---  1.00g 1.00g
  /dev/vdd      lvm2 ---  1.00g 1.00g
  /dev/vde      lvm2 ---  1.00g 1.00g
[root@centos-host ~]#
```

- Remove the /dev/vde physical volume from LVM :

```
[root@centos-host ~]# pvremove /dev/vde
  Labels on physical volume "/dev/vde" successfully wiped.
[root@centos-host ~]# pvs
  PV         VG Fmt  Attr PSize PFree
  /dev/vdb      lvm2 ---  1.00g 1.00g
  /dev/vdc      lvm2 ---  1.00g 1.00g
  /dev/vdd      lvm2 ---  1.00g 1.00g
[root@centos-host ~]#
```

- Add /dev/vdd to this volume group so that we gain more usable storage space:

```
[root@centos-host ~]# vgs
  VG      #PV #LV #SN Attr   VSize VFree
  volume1   2   0   0 wz--n- 1.99g 1.99g
[root@centos-host ~]# pvs
  PV         VG      Fmt  Attr PSize    PFree
  /dev/vdb   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdc   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdd           lvm2 ---     1.00g    1.00g
[root@centos-host ~]# vgextend volume1 /dev/vdd
  Volume group "volume1" successfully extended
[root@centos-host ~]# pvs
  PV         VG      Fmt  Attr PSize    PFree
  /dev/vdb   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdc   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdd   volume1 lvm2 a--  1020.00m 1020.00m
[root@centos-host ~]#
```

- Remove /dev/vdd from the volume group volume1 :

```
[root@centos-host ~]# vg
vgcfgbackup      vgconvert       vgextend        vgmerge         vgrename
vgcfgrestore     vgcreate        vgimport        vgmknodes       vgs
vgchange         vgdisplay       vgimportclone   vgreduce        vgscan
vgck             vgexport        vgimportdevices vgremove        vgsplit
[root@centos-host ~]# vgreduce volume1 /dev/vdd
  Removed "/dev/vdd" from volume group "volume1"
[root@centos-host ~]# pvs
  PV         VG      Fmt  Attr PSize    PFree
  /dev/vdb   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdc   volume1 lvm2 a--  1020.00m 1020.00m
  /dev/vdd           lvm2 ---     1.00g    1.00g
[root@centos-host ~]#
```

- Storage Monitoring :

```
$ sudo apt install sysstat
```

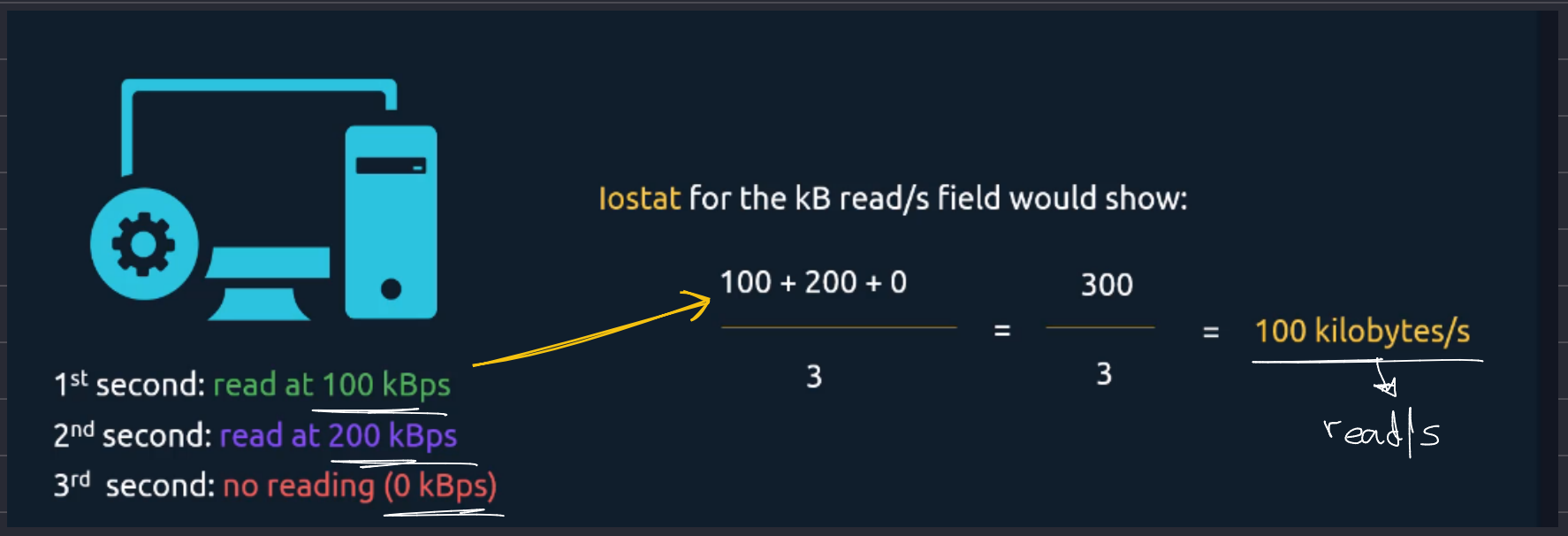
```
$ iostat
Linux 5.19.0-41-generic (user1)  07/18/2023          _x86_64_   (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          19.45   13.74    8.49    1.82    0.00   56.50

Device            tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
loop0            0.16         3.06         0.00         0.00       1126          0          0
loop1            0.13         0.98         0.00         0.00        362          0          0
loop2            0.15         2.92         0.00         0.00       1073          0          0
sda             99.48      4839.84      3120.54         0.00    1779997    1147673          0
sr0              0.12         0.40         0.00         0.00        148          0          0
```

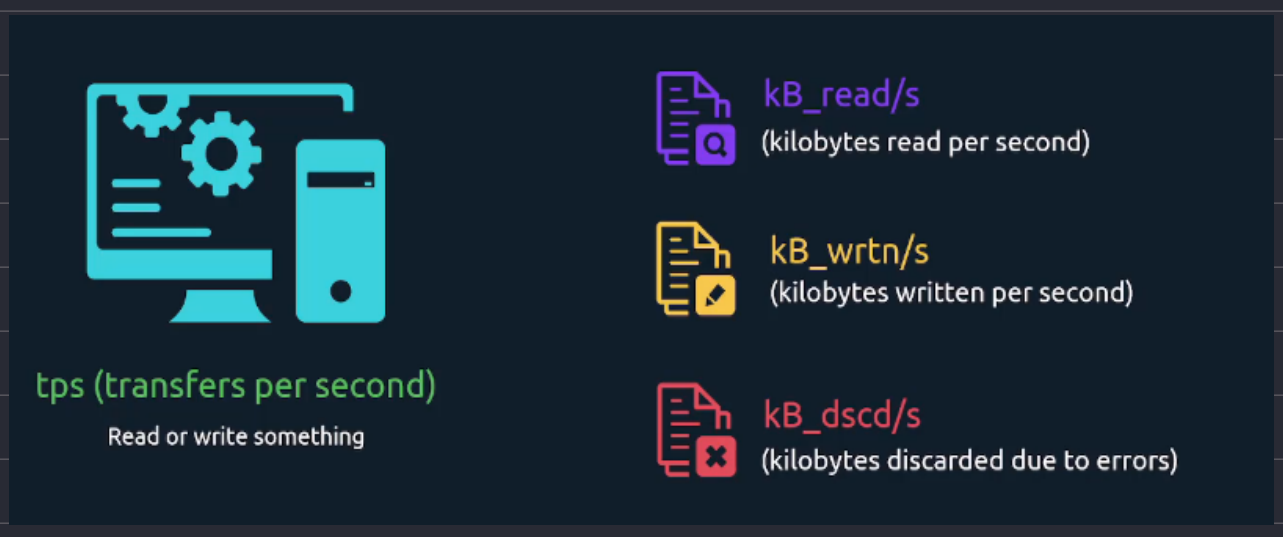
Historical data since bootup

the total values, So that's kilobytes read since the uptime

all of these numbers include data from the start of your server. so it takes the average usage. → read | s

- we have a server that's been up for three seconds :





- tps : the number of I/O operations (both read and write) per second that were issued to the device

- dscd: kilobytes of discarded due to errors per second.

- continuously show us every second:

```
❯ iostat 1
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          14.05    0.04    6.52    0.18    0.00   79.21

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda               4.55        44.29       159.79         0.00   15775933   56920479          0


avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           7.77    0.00    5.22    0.00    0.00   87.01

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda               0.00         0.00         0.00         0.00          0          0          0


avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           9.10    0.00    3.41    0.13    0.00   87.36

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda               2.00         0.00         8.00         0.00          0          8          0
```

```
user1@kodekloud:~$ pidstat
Linux 5.15.0-67-generic (kodekloud)     07/20/23        _x86_64_        (1 CPU)

23:24:24      UID       PID    %usr %system  %guest   %wait    %CPU   CPU  Command
23:24:24        0         1    0.01    0.02    0.00    0.01    0.03     0  systemd
23:24:24        0        13    0.00    0.00    0.00    0.01    0.00     0  ksoftirqd/0
23:24:24        0        14    0.00    0.00    0.00    0.01    0.00     0  rcu_sched
23:24:24        0        15    0.00    0.00    0.00    0.00    0.00     0  migration/0
23:24:24        0        25    0.00    0.00    0.00    0.00    0.00     0  kcompactd0
23:24:24        0        83    0.00    0.03    0.00    0.00    0.03     0  kworker/0:1H-kblockd
23:24:24        0       258    0.00    0.04    0.00    0.01    0.04     0  jbd2/vda1-8
23:24:24        0       331    0.00    0.00    0.00    0.01    0.01     0  systemd-journal
23:24:24        0       372    0.00    0.00    0.00    0.00    0.01     0  multipathd
23:24:24      103       453    0.00    0.00    0.00    0.00    0.00     0  systemd-timesyn
23:24:24      100       529    0.00    0.00    0.00    0.00    0.00     0  systemd-network
23:24:24      101       549    0.00    0.00    0.00    0.00    0.00     0  systemd-resolve
23:24:24        0       573    0.00    0.00    0.00    0.00    0.00     0  systemd-udevd
23:24:24        0       631    0.00    0.00    0.00    0.00    0.00     0  cron
23:24:24      102       633    0.00    0.00    0.00    0.00    0.00     0  dbus-daemon
23:24:24        0       635    0.00    0.00    0.00    0.00    0.00     0  droplet-agent
23:24:24        0       640    0.00    0.00    0.00    0.00    0.00     0  networkd-dispat
23:24:24      104       641    0.00    0.00    0.00    0.00    0.00     0  rsyslogd
23:24:24        0       643    0.00    0.03    0.00    0.03    0.03     0  snapd
23:24:24        0       646    0.00    0.00    0.00    0.00    0.00     0  systemd-logind
```

-d parameter : Display I/O statistics : detailed information on the amount of data being read and written by each process :

```
❮ pidstat -d
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

12:48:23 AM   UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:48:23 AM  1000      1267      0.14      0.00      0.00       0  i3
12:48:23 AM  1000      1276      0.00      0.00      0.00       0  dbus-broker
12:48:23 AM  1000      1281      0.01      0.00      0.00       0  kitty
12:48:23 AM  1000      1282      0.00      0.00      0.00       0  kitty
12:48:23 AM  1000      1283      0.00      0.00      0.00       0  kitty
12:48:23 AM  1000      1284      0.01      0.00      0.00       0  kitty
12:48:23 AM  1000      1285      0.01      0.00      0.00       0  kitty
12:48:23 AM  1000      1288      0.02      0.00      0.00       0  nm-applet
12:48:23 AM  1000      1291      0.00      0.00      0.00       0  bash
12:48:23 AM  1000      1292      0.01      0.00      0.00       0  polkit-gnome-au
12:48:23 AM  1000      1297      0.01      0.00      0.00       0  dunst
12:48:23 AM  1000      1300      0.00      0.00      0.00       0  xfce4-power-man
12:48:23 AM  1000      1301      0.05      0.00      0.00       0  flameshot
12:48:23 AM  1000      1302      0.04      0.21      0.09       0  xfce4-clipman
12:48:23 AM  1000      1303      0.00      0.00      0.00       0  python3
12:48:23 AM  1000      1308      0.02      0.00      0.00       0  c
12:48:23 AM  1000      1309      0.00      0.00      0.00       0  python3
12:48:23 AM  1000      1310      0.00      0.00      0.00       0  autotiling
12:48:23 AM  1000      1312      0.00      0.00      0.00       0  sxhkd
12:48:23 AM  1000      1315      0.00      0.00      0.00       0  picom
12:48:23 AM  1000      1318      0.02      0.00      0.00       0  i3bar
12:48:23 AM  1000      1338      0.02      0.00      0.00       0  python3
12:48:23 AM  1000      1346      0.04      0.00      0.00       0  gvfsd
12:48:23 AM  1000      1370      0.00      0.00      0.00       0  gvfsd-fuse
12:48:23 AM  1000      1373      0.06      1.14      0.00       0  i3blocks
12:48:23 AM  1000      1384      0.00      0.00      0.00       0  python3
12:48:23 AM  1000      1512      0.03      0.00      0.00       0  mpd
12:48:23 AM  1000      1514      0.00      0.00      0.00       0  at-spi-bus-laun
12:48:23 AM  1000      1532      0.00      0.00      0.00       0  dbus-broker-lau
:
```

- To display I/O statistics for processes every 2 seconds :

```
❯ pidstat -d 2

Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

12:51:51 AM   UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:51:53 AM  1000      1373      0.00      3.94      0.00       0  i3blocks

12:51:53 AM   UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:51:55 AM  1000      1373      0.00      4.00      0.00       0  i3blocks
12:51:55 AM  1000   1413654      0.00     12.00      0.00       0  chromium
12:51:55 AM  1000   1413692      0.00      6.00      0.00       0  chromium

12:51:55 AM   UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:51:57 AM  1000      1373      0.00      4.00      0.00       0  i3blocks
12:51:57 AM  1000      1976      0.00    114.00      0.00       0  firefox
12:51:57 AM  1000   1413654      0.00      2.00      0.00       0  chromium

12:51:57 AM   UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:51:59 AM  1000      1373      0.00      4.00      0.00       0  i3blocks
12:51:59 AM  1000   1413654      0.00     26.00      0.00       0  chromium
^C

Average:      UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
Average:     1000      1373      0.00      3.99      0.00       0  i3blocks
Average:     1000      1976      0.00     28.39      0.00       0  firefox
Average:     1000   1413654      0.00      9.96      0.00       0  chromium
Average:     1000   1413692      0.00      1.49      0.00       0  chromium

~ 8s
❯
```

-h: human readable -d: display statistics every 1 sec

```
~
❯ pidstat -h -d 1
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

# Time        UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:54:34 AM  1000      1373      0.00      7.77      0.00       0  i3blocks
12:54:34 AM  1000   1413654      0.00     19.42      0.00       0  chromium

# Time        UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:54:35 AM  1000   1413654      0.00      8.00      0.00       0  chromium

# Time        UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:54:36 AM  1000      1373      0.00      8.00      0.00       0  i3blocks
12:54:36 AM  1000    278415     16.00      0.00      0.00       0  kitty

# Time        UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command

# Time        UID       PID   kB_rd/s   kB_wr/s kB_ccwr/s iodelay  Command
12:54:38 AM  1000      1373      0.00      8.00      0.00       0  i3blocks
12:54:38 AM  1000    278415     32.00      0.00      0.00       0  kitty
12:54:38 AM  1000   1413654      0.00     20.00      0.00       0  chromium
12:54:38 AM  1000   1413692      0.00     76.00      0.00       0  chromium
^C

~
❯ iostat -h -d 1 → every 1 sec   -d: remove CPU report
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

      tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd Device
     4.56        44.2k       160.1k         0.0k      15.1G      54.5G         0.0k sda

      tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd Device
    12.00         0.0k       140.0k         0.0k       0.0k     140.0k         0.0k sda

      tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd Device
     1.00        32.0k         0.0k         0.0k      32.0k       0.0k         0.0k sda
```

```
❯ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 931.5G  0 disk
├─sda1   8:1    0   700M  0 part /boot
├─sda2   8:2    0   100G  0 part /
├─sda3   8:3    0     8G  0 part [SWAP]
└─sda4   8:4    0 822.8G  0 part /home
sr0     11:0    1  1024M  0 rom

~
❯ iostat -p sda
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          14.07    0.04    6.52    0.19    0.00   79.19

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda               4.56        44.18       160.22         0.00   15785745   57245031          0
sda1              0.00         0.02         0.00         0.00       7443          5          0
sda2              0.47        12.48         1.55         0.00    4458653     552444          0
sda3              0.31         1.67         8.73         0.00     596424    3117504          0
sda4              3.78        29.99       149.95         0.00   10716597   53575078          0


~
❯ iostat sda1
Linux 6.9.3-arch1-1 (hera-81bf)         06/24/2024      _x86_64_        (8 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          14.07    0.04    6.52    0.19    0.00   79.19

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
sda1              0.00         0.02         0.00         0.00       7443          5          0
```

SELinux :

```
$ ls -l
-rw-rw-r--. 1 aaron aaron 160 Dec  1 18:19 archive.tar.gz
```

shows us what permissions are enabled or disabled for a file or directory.

```
$ ls -Z
unconfined_u:object_r:user_home_t:s0 archive.tar.gz
```

to see SELinux file and directory labels

SE linux labels = Context

```
unconfined_u:object_r:user_home_t:s0
user          role          type          level
```

- user : this is not the same as the username you log in with. It's an SELinux user. Every Linux user who logs in to a system is mapped to a Linux user as part of the Linux policy configuration.
- role : And after the user is identified, a decision is made to see if it can assume the role. Each user can only assume a predefined set of roles.

SELinux User	Roles
developer_u	developer_r, docker_r
guest_u	guest_r
root	staff_r, sysadm_r, system_r, unconfined_r

For example, developer_u should only be able to enter roles like developer_r or Docker_r that allow them to read and write application code, launch, docker containers and so on. But they should not be able to enter roles like sysadmins_r that let them change system settings.

- type uses to control access between subjects (users, processes, services) and objects (files, directories, network port).

going through this three step path (user then role then type) , the security module achieves three important things:

1. Only certain users can enter certain roles and certain types.
2. It lets authorized users and processes do their job, by granting the permissions they need.
3. Authorized users and processes are allowed to take only a limited set of actions.

4. Everything else is denied.

```
$ ps axZ
system_u:system_r:accountsd_t:s0    995 ?        Ssl    0:00 /usr/libexec/accoun
system_u:system_r:NetworkManager_t:s0 1024 ?     Ssl    0:00 /usr/sbin/NetworkMa
system_u:system_r:sshd_t:s0-s0:c0.c1023 1030 ?   Ss     0:00 /usr/sbin/sshd -D -
system_u:system_r:tuned_t:s0       1032 ?        Ssl    0:00 /usr/libexec/platfo
system_u:system_r:cupsd_t:s0-s0:c0.c1023 1033 ?  Ss     0:00 /usr/sbin/cupsd -l
```

- SSH daemon running here and that it's restricted to the sshd_t domain. this domain contains a strict set of policies that define what this process is allowed to do.

- Also important to note, not anything can enter the sshd_t domain. only files that have the sshd_exec_t SELinux type in their label can enter this domain.

```
$ ls -Z /usr/sbin/sshd
system_u:object_r:sshd_exec_t:s0 /usr/sbin/sshd
```

- Domains: A domain in SELinux typically refers to a security context for a running process. For example, sshd_t is a domain associated with the SSH daemon (sshd).

subject

- Types: A type in SELinux typically refers to the security context for files, directories, and other objects. For example, sshd_exec_t is a type associated with the SSH daemon executable files.

A process can only transition into the sshd_t domain if it executes a file that has the sshd_exec_t type.

only a file marked with a certain type (sshd_exec_t) can start a process that can shift into a certain domain (sshd_t) . ==> transition from the initial context (init_t or systemd_t) to the sshd_t domain

```
$ ps axZ
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1875 ? Ss   0:00 /usr/lib/
system_u:system_r:init_t:s0                            1881 ? S    0:00 (sd-pam)
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1891 ? Ssl  0:00 /usr/bin
```

Anything labeled with unconfined_t is running unrestricted. SELinux lets those processes do almost anything they want.

```
$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

this user is mapped to unconfined_u user

```
$ sudo semanage login -l
Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
```

if root logs in mapped to the linux user unconfined_u.
if any other user (_default_) logs in, they'll be mapped to unconfined_u.

```
$ sudo semanage user -l
SELinux User    Prefix     MCS Level  MCS Range                      SELinux Roles

guest_u         user       s0         s0                             guest_r
root            user       s0         s0-s0:c0.c1023                 staff_r sysadm_r system_r unconfined_r
staff_u         user       s0         s0-s0:c0.c1023                 staff_r sysadm_r unconfined_r
sysadm_u        user       s0         s0-s0:c0.c1023
```

to see the roles that each user can have on this system,

to see if SELinux is enabled and actively restricting actions :

```
$ getenforce
Enforcing
```

1- Enforcing : it's doing its job and denying unauthorized actions.

2- Permissive means it's allowing everything and just locking actions that should have been restricted

3- Disable : it's not doing anything. It isn't enforcing security and it isn't even logging.

Create and enforce MAC using SELinux :

Red Hat and CentOS operating systems have SELinux enabled by default, but Ubuntu has a different security module called apparmor, which is used by default.

```
user1@kodekloud:~$ sudo systemctl stop apparmor.service
[sudo] password for user1:
user1@kodekloud:~$ sudo systemctl disable apparmor.service
Synchronizing state of apparmor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable apparmor
Removed /etc/systemd/system/sysinit.target.wants/apparmor.service.
user1@kodekloud:~$ sudo apt install selinux-basics auditd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  checkpolicy libauparse0 libblas3 libgfortran5 liblapack3 libquadmath0 m4 make policycoreutils policycoreutil
  policycoreutils-python-utils python3-audit python3-decorator python3-networkx python3-numpy python3-selinux
  python3-sepolgen python3-sepolicy python3-setools selinux-policy-default selinux-policy-dev selinux-utils se
Suggested packages:
  audispd-plugins m4-doc make-doc python-networkx-doc python3-gdal python3-matplotlib python3-pydot python3-py
  python3-scipy gcc gfortran python-numpy-doc python3-dev python3-pytest logcheck syslog-summary setools-gui
```

```
user1@kodekloud:~$ sestatus
SELinux status:                 disabled
user1@kodekloud:~$ ls -Z /
? bin   ? dev  ? home  ? lib32  ? libx32      ? media  ? opt   ? root  ? sbin  ? srv  ? tmp  ? var
? boot  ? etc  ? lib   ? lib64  ? lost+found  ? mnt    ? proc  ? run   ? snap  ? sys  ? usr
user1@kodekloud:~$ sudo selinux-activate
Activating SE Linux
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.15.0-83-generic
Found initrd image: /boot/initrd.img-5.15.0-83-generic
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
SE Linux is activated.  You may need to reboot now.
user1@kodekloud:~$
```

it modified the grub bootloader to instruct the Linux kernel to load the Linux module at boot time.

$ Cat /etc/default/grub

```
GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT=""
GRUB_CMDLINE_LINUX=" security=selinux"
```

```
user1@kodekloud:~$ ls -a /
.   .autorelabel  boot  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
..  bin           dev   home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
user1@kodekloud:~$
```

This instructs the Linux to relabel every file with the proper security labels when we reboot.

$ systemctl reboot

```
         Starting LVM event activation on device 8:3...
[  OK  ] Found device VBOX_HARDDISK 2.
         Starting File System Check on /dev/d…/375db648-a50a-46d2-80e6-84a0938dcc32...
[  OK  ] Started File System Check Daemon to report status.
[  OK  ] Finished File System Check on /dev/d…id/375db648-a50a-46d2-80e6-84a0938dcc32.
         Mounting /boot...
[  OK  ] Mounted /boot.
[  OK  ] Reached target Local File Systems.
         Starting Create final runtime dir for shutdown pivot root...
         Starting Tell Plymouth To Write Out Runtime Data...
         Starting Set Up Additional Binary Formats...
         Starting Create Volatile Files and Directories...
[  OK  ] Finished LVM event activation on device 8:3.
[  OK  ] Finished Create final runtime dir for shutdown pivot root.
[  OK  ] Finished Tell Plymouth To Write Out Runtime Data.
         Mounting Arbitrary Executable File Formats File System...
[  OK  ] Mounted Arbitrary Executable File Formats File System.
[  OK  ] Finished Set Up Additional Binary Formats.
[  OK  ] Finished Create Volatile Files and Directories.
         Starting Network Time Synchronization...
         Starting Record System Boot/Shutdown in UTMP...
[  OK  ] Finished Record System Boot/Shutdown in UTMP.
[  OK  ] Started Network Time Synchronization.
[  OK  ] Reached target System Initialization.
[  OK  ] Reached target System Time Set.
         Starting Relabel all filesystems...

*** Warning -- SELinux default policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
[  OK  ] Finished Wait for Network to be Configured.
[  OK  ] Reached target Network is Online.
[  OK  ] Reached target Preparation for Remote File Systems.
[  OK  ] Finished Availability of block devices.
libsemanage.add_user: user sddm not in password file
Relabeling / /boot
 3.1%
```

to relabel everything

```
user1@kodekloud:~$ ls -Z /
          system_u:object_r:bin_t:s0 bin                  system_u:object_r:usr_t:s0 opt
         system_u:object_r:boot_t:s0 boot                 system_u:object_r:proc_t:s0 proc
       system_u:object_r:device_t:s0 dev          system_u:object_r:user_home_dir_t:s0 root
          system_u:object_r:etc_t:s0 etc                system_u:object_r:var_run_t:s0 run
    system_u:object_r:home_root_t:s0 home                   system_u:object_r:bin_t:s0 sbin
          system_u:object_r:lib_t:s0 lib                system_u:object_r:default_t:s0 snap
          system_u:object_r:lib_t:s0 lib32                  system_u:object_r:var_t:s0 srv
          system_u:object_r:lib_t:s0 lib64                system_u:object_r:sysfs_t:s0 sys
          system_u:object_r:lib_t:s0 libx32                 system_u:object_r:tmp_t:s0 tmp
   system_u:object_r:lost_found_t:s0 lost+found                 system_u:object_r:usr_t:s0 usr
          system_u:object_r:mnt_t:s0 media                  system_u:object_r:var_t:s0 var
          system_u:object_r:mnt_t:s0 mnt
user1@kodekloud:~$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested (insecure)
Max kernel policy version:      33
user1@kodekloud:~$ getenforce
Permissive
user1@kodekloud:~$
```

```
user1@kodekloud:~$ ps -eZ | grep sshd_t
system_u:system_r:sshd_t:s0-s0:c0.c1023 679 ?    00:00:00 sshd
system_u:system_r:sshd_t:s0-s0:c0.c1023 1095 ?   00:00:00 sshd
system_u:system_r:sshd_t:s0-s0:c0.c1023 1149 ?   00:00:00 sshd
user1@kodekloud:~$ ls -Z /usr/sbin/sshd
system_u:object_r:sshd_exec_t:s0 /usr/sbin/sshd
user1@kodekloud:~$
main  ⊗ 0 ⚠ 0  Connect
```

The file is labeled with the sshd_exec_t type and when Linux runs something labeled with a sshd_exec_t, the process will be transitioned into a domain labeled sshd_t

A domain is sort of a security bubble that contains this process and allows it to do only what is defined under the sshd_t type enforcement rules.

can take a look at what Linux recorded in the audit log by running :

```
user1@kodekloud:~$ sudo audit2why --all | less
```

→ then search ssh

is used to help diagnose and understand why SELinux is denying certain actions.

```
TERMINAL  PROBLEMS  OUTPUT  DEBUG CONSOLE  SQL CONSOLE                                   ssh

type=AVC msg=audit(1695221295.619:257): avc:  denied  { execute } for  pid=988 comm="run-parts" name="landscape-sysinfo.wrapper" dev
"dm-0" ino=154165 scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023 tcontext=system_u:object_r:usr_t:s0 tclass=file permissive=1
        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1695221295.619:258): avc:  denied  { execute_no_trans } for  pid=994 comm="run-parts" path="/usr/share/landscape/
andscape-sysinfo.wrapper" dev="dm-0" ino=154165 scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023 tcontext=system_u:object_r:usr_t:s0
tclass=file permissive=1
        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1695221295.623:259): avc:  denied  { getattr } for  pid=995 comm="find" path="/var/lib/landscape/landscape-sysinf
.cache" dev="dm-0" ino=266390 scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023 tcontext=system_u:object_r:var_lib_t:s0 tclass=file p
rmissive=1
        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1695221296.047:260): avc:  denied  { open } for  pid=1002 comm="landscape-sysin" path="/var/log/landscape/sysinfo
log" dev="dm-0" ino=266384 scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023 tcontext=system_u:object_r:var_log_t:s0 tclass=file perm
ssive=1
        Was caused by:
                Missing type enforcement (TE) allow rule.
:
```

access Vector cache.

This is simply shows that the action that the Linux would be denied by the current security policy. a process with this label (sshd_t) tried something that it's not permitted to do.

#another ex:

type=AVC msg=audit(1623333424.181:337): avc: denied { read } for pid=1234 comm="httpd" name="index.html" dev="sda1" ino=654321 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:httpd_sys_content_t:s0 tclass=file

Was caused by:
Missing type enforcement (TE) allow rule.

You can use audit2allow to generate a loadable module to allow this access.

- Explanation: It indicates that an HTTP server process (httpd) was denied read access to index.html because there is no SELinux policy allowing this action.

- Suggestion: It suggests using audit2allow to create a policy module that would permit this action if it's deemed appropriate and necessary.

type=AVC msg=audit(1623345678.123:456): avc: denied { write } for pid=2345 comm="httpd" name="access.log" dev="sda1" ino=789012 scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:object_r:var_log_t:s0 tclass=file

Was caused by:
Missing type enforcement (TE) allow rule.

You can use audit2allow to generate a loadable module to allow this access.

- **AVC (Access Vector Cache) Denial**:
  - `type=AVC`: Indicates an AVC denial message.
  - `msg=audit(1623345678.123:456)`: Provides a timestamp and unique identifier for the audit message.
  - `avc: denied { write }`: Specifies that a write operation was denied.
  - `pid=2345`: The process ID of the process that was denied access.
  - `comm="httpd"`: The command name or executable of the process (in this case, the Apache HTTP server).
  - `name="access.log"`: The name of the file the process attempted to write to.
  - `dev="sda1" ino=789012`: Device and inode numbers for the file.
  - `scontext=system_u:system_r:httpd_t:s0`: The SELinux context of the process trying to perform the operation.
  - `tcontext=system_u:object_r:var_log_t:s0`: The SELinux context of the target file.
  - `tclass=file`: The class of the object (file).
- **Cause**:
  - The denial was caused by a missing type enforcement (TE) allow rule. Specifically, the `httpd_t` domain (associated with the Apache HTTP server) is not allowed to write to files labeled with the `var_log_t` type (typically used for log files in `/var/log`).
- **Suggestion**:
  - The output suggests using `audit2allow` to create a policy module that would permit this access if it is deemed appropriate. This would involve generating a custom SELinux policy module to allow the `httpd_t` domain to write to `var_log_t` type files.

---

to generate selinux policy actions based on audit log messages : --all flag : tells a tool to inspect all logged events and -M : tells it to generate a module or policy package. This is simply a file that we can load into Linux to create a security policy that would allow all of those previously logged actions :

```
user1@kodekloud:~$ sudo audit2allow --all -M mymodule
****************** IMPORTANT ***********************
To make this policy package active, execute:

semodule -i mymodule.pp

user1@kodekloud:~$ semodule -i mymodule.pp
libsemanage.semanage_create_store: Could not read from module store, active subdirectory at /var/lib/selinux/default/active. (Permis
ion denied).
libsemanage.semanage_direct_connect: could not establish direct connection (Permission denied).
semodule:  Could not connect to policy handler
user1@kodekloud:~$ sudo semodule -i mymodule.pp
libsemanage.add_user: user sddm not in password file
user1@kodekloud:~$ sudo setenforce 1
user1@kodekloud:~$ getenforce
Enforcing
user1@kodekloud:~$ sudo vi /etc/selinux/config
```

→ ignore this message as it's a bug.

1 → puts Linux into enforcing mode only temporarily. Once we reboot, it will go back into permissive mode

→ we can permanently put Linux into enforcing mode.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
# default - equivalent to the old strict and targeted policies
# mls     - Multi-Level Security (for military and educational use)
# src     - Custom policy built from source
SELINUXTYPE=default

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
~
~
~
```

```
user1@kodekloud:~$ ls -lart
total 56
-rw-r--r--. 1 user1 user1  807 Jan  6  2022 .profile
-rw-r--r--. 1 user1 user1 3771 Jan  6  2022 .bashrc
-rw-r--r--. 1 user1 user1  220 Jan  6  2022 .bash_logout
drwxr-xr-x. 3 root  root  4096 Sep 12 01:11 ..
drwx------. 2 user1 user1 4096 Sep 12 01:11 .ssh
drwx------. 2 user1 user1 4096 Sep 12 01:13 .cache
-rw-r--r--. 1 user1 user1    0 Sep 12 01:14 .sudo_as_admin_successful
-rw-------. 1 user1 user1  331 Sep 20 14:48 .bash_history
-rw-------. 1 user1 user1   33 Sep 20 14:56 .lesshst
-rw-r--r--. 1 root  root  4772 Sep 20 14:59 mymodule.te
-rw-r--r--. 1 root  root  9772 Sep 20 14:59 mymodule.pp
drwxr-x---. 4 user1 user1 4096 Sep 20 14:59 .
user1@kodekloud:~$ less mymodule.te
```

→ then search ssh

```
#!!!! This avc can be allowed using the boolean 'ssh_sysadm_login'
allow sshd_t unconfined_t:process transition;
allow sshd_t usr_t:file { execute execute_no_trans };
allow sshd_t var_lib_t:file { getattr open read write };
allow sshd_t var_log_t:dir { add_name write };
allow sshd_t var_log_t:file { append create getattr ioctl open };
allow sshd_t var_t:file { getattr open read };

#!!!! This avc can be allowed using the boolean 'allow_polyinstantiation'
allow sshd_t xdg_cache_t:dir search;
allow sshd_t xdg_cache_t:file getattr;
```

the processes under this domain (sshd_t) should be able to do certain actions on files labeled var_log_t type.

```
user1@kodekloud:~$ ls -Z /var/log/auth.log
system_u:object_r:var_log_t:s0 /var/log/auth.log
user1@kodekloud:~$ ls -Z /var/log/auth.log grep var_log_t:file mymodule.te
ls: cannot access 'grep': No such file or directory
ls: cannot access 'var_log_t:file': No such file or directory
unconfined_u:object_r:user_home_t:s0 mymodule.te        system_u:object_r:var_log_t:s0 /var/log/auth.log
user1@kodekloud:~$ grep var_log_t:file mymodule.te
allow sshd_t var_log_t:file { append create getattr ioctl open };
user1@kodekloud:~$
```

to change user role and type :

```
user1@kodekloud:~$ ls -Z /var/log/auth.log
system_u:object_r:var_log_t:s0 /var/log/auth.log
user1@kodekloud:~$ sudo chcon -u unconfined_u /var/log/auth.log
user1@kodekloud:~$ ls -Z /var/log/auth.log
unconfined_u:object_r:var_log_t:s0 /var/log/auth.log
user1@kodekloud:~$ sudo chcon -r object_r /var/log/auth.log
user1@kodekloud:~$ sudo chcon -t user_home_t /var/log/auth.log
user1@kodekloud:~$ ls -Z /var/log/auth.log
unconfined_u:object_r:user_home_t:s0 /var/log/auth.log
user1@kodekloud:~$
```

what is a valid label for each part :

```
user1@kodekloud:~$ seinfo -u

Users: 7
   root
   staff_u
   sysadm_u
   system_u
   unconfined_u
   user_u
   xdm
user1@kodekloud:~$ seinfo -r

Roles: 15
   auditadm_r
   dbadm_r
   guest_r
   logadm_r
   nx_server_r
   object_r
   secadm_r
   staff_r
   sysadm_r
   system_r
   unconfined_r
   user_r
   webadm_r
   xdm_r
   xguest_r
user1@kodekloud:~$ seinfo -t
```

→ type

change the SELinux context of a file to match the context of a reference file :

```
user1@kodekloud:~$ ls -Z /var/log
        system_u:object_r:var_log_t:s0 alternatives.log          system_u:object_r:faillog_t:s0 faillog
    system_u:object_r:apt_var_log_t:s0 apt                       system_u:object_r:var_log_t:s0 installer
     system_u:object_r:auditd_log_t:s0 audit                 system_u:object_r:systemd_journal_t:s0 journal
  unconfined_u:object_r:user_home_t:s0 auth.log                  system_u:object_r:var_log_t:s0 kern.log
        system_u:object_r:var_log_t:s0 bootstrap.log             system_u:object_r:var_log_t:s0 landscape
        system_u:object_r:faillog_t:s0 btmp                      system_u:object_r:lastlog_t:s0 lastlog
        system_u:object_r:var_log_t:s0 cloud-init.log            system_u:object_r:var_log_t:s0 private
        system_u:object_r:var_log_t:s0 cloud-init-output.log     system_u:object_r:var_log_t:s0 syslog
        system_u:object_r:var_log_t:s0 dist-upgrade              system_u:object_r:var_log_t:s0 ubuntu-advantage.log
        system_u:object_r:var_log_t:s0 dmesg                     system_u:object_r:var_log_t:s0 unattended-upgrades
        system_u:object_r:var_log_t:s0 dmesg.0                      system_u:object_r:wtmp_t:s0 wtmp
        system_u:object_r:var_log_t:s0 dpkg.log
user1@kodekloud:~$ sudo chcon --reference=/var/log/syslog /var/log/auth.log
user1@kodekloud:~$ ls -Z /var/log
        system_u:object_r:var_log_t:s0 alternatives.log          system_u:object_r:faillog_t:s0 faillog
    system_u:object_r:apt_var_log_t:s0 apt                       system_u:object_r:var_log_t:s0 installer
     system_u:object_r:auditd_log_t:s0 audit                 system_u:object_r:systemd_journal_t:s0 journal
        system_u:object_r:var_log_t:s0 auth.log                  system_u:object_r:var_log_t:s0 kern.log
        system_u:object_r:var_log_t:s0 bootstrap.log             system_u:object_r:var_log_t:s0 landscape
        system_u:object_r:faillog_t:s0 btmp                      system_u:object_r:lastlog_t:s0 lastlog
        system_u:object_r:var_log_t:s0 cloud-init.log            system_u:object_r:var_log_t:s0 private
        system_u:object_r:var_log_t:s0 cloud-init-output.log     system_u:object_r:var_log_t:s0 syslog
        system_u:object_r:var_log_t:s0 dist-upgrade              system_u:object_r:var_log_t:s0 ubuntu-advantage.log
        system_u:object_r:var_log_t:s0 dmesg                     system_u:object_r:var_log_t:s0 unattended-upgrades
        system_u:object_r:var_log_t:s0 dmesg.0                      system_u:object_r:wtmp_t:s0 wtmp
        system_u:object_r:var_log_t:s0 dpkg.log
user1@kodekloud:~$
```

```
user1@kodekloud:~$ sudo touch /var/www/{1..10}
user1@kodekloud:~$ ls -Z /var/www
unconfined_u:object_r:var_t:s0 1   unconfined_u:object_r:var_t:s0 4  unconfined_u:object_r:var_t:s0 8
unconfined_u:object_r:var_t:s0 10  unconfined_u:object_r:var_t:s0 5  unconfined_u:object_r:var_t:s0 9
unconfined_u:object_r:var_t:s0 2   unconfined_u:object_r:var_t:s0 6
unconfined_u:object_r:var_t:s0 3   unconfined_u:object_r:var_t:s0 7
user1@kodekloud:~$ sudo restorecon -R /var/www/
user1@kodekloud:~$ ls -Z /var/www
unconfined_u:object_r:httpd_sys_content_t:s0 1   unconfined_u:object_r:httpd_sys_content_t:s0 5
unconfined_u:object_r:httpd_sys_content_t:s0 10  unconfined_u:object_r:httpd_sys_content_t:s0 6
unconfined_u:object_r:httpd_sys_content_t:s0 2   unconfined_u:object_r:httpd_sys_content_t:s0 7
unconfined_u:object_r:httpd_sys_content_t:s0 3   unconfined_u:object_r:httpd_sys_content_t:s0 8
unconfined_u:object_r:httpd_sys_content_t:s0 4   unconfined_u:object_r:httpd_sys_content_t:s0 9
user1@kodekloud:~$ sudo chcon -u staff_u /var/www/1
user1@kodekloud:~$ sudo restorecon -R /var/www/
user1@kodekloud:~$ ls -Z /var/www
     staff_u:object_r:httpd_sys_content_t:s0 1   unconfined_u:object_r:httpd_sys_content_t:s0 5
unconfined_u:object_r:httpd_sys_content_t:s0 10  unconfined_u:object_r:httpd_sys_content_t:s0 6
unconfined_u:object_r:httpd_sys_content_t:s0 2   unconfined_u:object_r:httpd_sys_content_t:s0 7
unconfined_u:object_r:httpd_sys_content_t:s0 3   unconfined_u:object_r:httpd_sys_content_t:s0 8
unconfined_u:object_r:httpd_sys_content_t:s0 4   unconfined_u:object_r:httpd_sys_content_t:s0 9
user1@kodekloud:~$ sudo restorecon -F -R /var/www/
user1@kodekloud:~$ ls -Z /var/www
system_u:object_r:httpd_sys_content_t:s0 1   system_u:object_r:httpd_sys_content_t:s0 4  system_u:object_r:httpd_sys_content_t:s0 8
system_u:object_r:httpd_sys_content_t:s0 10  system_u:object_r:httpd_sys_content_t:s0 5  system_u:object_r:httpd_sys_content_t:s0 9
system_u:object_r:httpd_sys_content_t:s0 2   system_u:object_r:httpd_sys_content_t:s0 6
system_u:object_r:httpd_sys_content_t:s0 3   system_u:object_r:httpd_sys_content_t:s0 7
user1@kodekloud:~$
```

is used to recursively restore the default SELinux security context for all files and directories within /var/www/ according to the SELinux policy

by default only restores the correct label for the type. => change the type label only . not user or role labels

force: to restore the correct label for u, r, t

- If the file system is relabeled again, the custom label we set on a file can be lost:

```
user1@kodekloud:~$ sudo semanage fcontext --add --type var_log_t /var/www/10
libsemanage.add_user: user sddm not in password file
user1@kodekloud:~$ sudo restorecon /var/www/10
user1@kodekloud:~$ ls -Z /var/www
system_u:object_r:httpd_sys_content_t:s0 1   system_u:object_r:httpd_sys_content_t:s0 4  system_u:object_r:httpd_sys_content_t:s0 8
        system_u:object_r:var_log_t:s0 10    system_u:object_r:httpd_sys_content_t:s0 5  system_u:object_r:httpd_sys_content_t:s0 9
system_u:object_r:httpd_sys_content_t:s0 2   system_u:object_r:httpd_sys_content_t:s0 6
system_u:object_r:httpd_sys_content_t:s0 3   system_u:object_r:httpd_sys_content_t:s0 7
user1@kodekloud:~$ sudo semanage fcontext --list
```

set default file context (--add) add this entry for the DB.

listing entire database

```
user1@kodekloud:~$ sudo semanage fcontext --list | grep "/var/www/uploads"
/var/www/uploads(/.*)?                             all files          system_u:object_r:httpd_cache_t:s0
user1@kodekloud:~$ sudo semanage fcontext --add --type nfs_t "/nfs/shares(/.*)?"
libsemanage.add_user: user sddm not in password file
user1@kodekloud:~$ sudo mkdir -p /nfs/shares
user1@kodekloud:~$ sudo restorecon -R /nfs/
user1@kodekloud:~$ ls -Z /nfs/
unconfined_u:object_r:nfs_t:s0 shares
user1@kodekloud:~$
```

set default context for all files under this path

- to display a list of SELinux booleans and their current values :

```
$ sudo semanage boolean --list

SELinux boolean                 State  Default Description
allow_console_login             off    off     Allow login from the console
httpd_enable_cgi                on     on      Allow httpd cgi support
httpd_enable_homedirs           off    off     Allow httpd to read home directories
httpd_execmem                   off    off     Allow httpd to execute memory
...
```

```
varnishd_connect_any          (off  ,  off)  Determine whether varnishd can use the full TCP network.
vbetool_mmap_zero_ignore      (off  ,  off)  Determine whether attempts by vbetool to mmap low regions should be silently blocked.
virt_use_comm                 (off  ,  off)  Determine whether confined virtual guests can use serial/parallel communication ports.
virt_use_evdev                (off  ,  off)  Determine whether confined virtual guests can use input devices via evdev pass through
virt_use_execmem              (off  ,  off)  Determine whether confined virtual guests can use executable memory and can make their
stack executable.
virt_use_fusefs               (off  ,  off)  Determine whether confined virtual guests can use fuse file systems.
virt_use_nfs                  (off  ,  off)  Determine whether confined virtual guests can use nfs file systems.
virt_use_samba                (off  ,  off)  Determine whether confined virtual guests can use cifs file systems.
virt_use_sysfs                (off  ,  off)  Determine whether confined virtual guests can manage device configuration.
virt_use_usb                  (off  ,  off)  Determine whether confined virtual guests can use usb devices.
virt_use_vfio                 (off  ,  off)  Determine whether confined virtual guests can use vfio for pci device pass through (vt
d).
virt_use_xserver              (off  ,  off)  Determine whether confined virtual guests can interact with xserver.
webadm_manage_user_files      (off  ,  off)  Determine whether webadm can manage generic user files.
webadm_read_user_files        (off  ,  off)  Determine whether webadm can read generic user files.
```

The `virt_use_nfs` SELinux boolean controls whether confined virtual guests can use NFS (Network File System) file systems.

Understanding `virt_use_nfs`

- **Boolean Name**: `virt_use_nfs`
- **Current State**: off (in your example)
- **Default State**: off (in your example)
- **Description**: This boolean determines whether virtual machines running under SELinux confinement (such as those managed by KVM, QEMU, or libvirt) are allowed to access NFS-mounted file systems.

Implications of the `virt_use_nfs` Boolean

- **When `off`**:
  - Confined virtual guests cannot access NFS file systems. This is the default setting, enhancing security by preventing virtual machines from potentially accessing sensitive data over NFS.
- **When `on`**:
  - Confined virtual guests are allowed to access NFS file systems. This might be necessary if your virtual machines need to access shared storage provided over NFS.

```
user1@kodekloud:~$
user1@kodekloud:~$ sudo setsebool virt_use_nfs 1
user1@kodekloud:~$ getsebool virt_use_nfs
virt_use_nfs --> on
user1@kodekloud:~$
```

- SELinux enforces rules about which ports specific daemons can bind to for listening to incoming connections. This enhances security by ensuring that only authorized daemons can use specified network ports.

```
user1@kodekloud:~$ sudo semanage port --list | grep ssh
ssh_port_t                     tcp      22
user1@kodekloud:~$ sudo semanage port --add --type ssh_port_t --proto tcp 2222
libsemanage.add_user: user sddm not in password file
user1@kodekloud:~$ sudo semanage port --list | grep ssh
ssh_port_t                     tcp      2222, 22
user1@kodekloud:~$ sudo semanage port --delete --type ssh_port_t --proto tcp 2222
libsemanage.add_user: user sddm not in password file
user1@kodekloud:~$ sudo semanage port --list | grep ssh
ssh_port_t                     tcp      22
user1@kodekloud:~$
```

Security Enhanced Linux (SELinux) provides an additional layer of system security. SELinux fundamentally answers the question: May <subject> do <action> to <object>?, for example: May a web server access files in users' home directories?

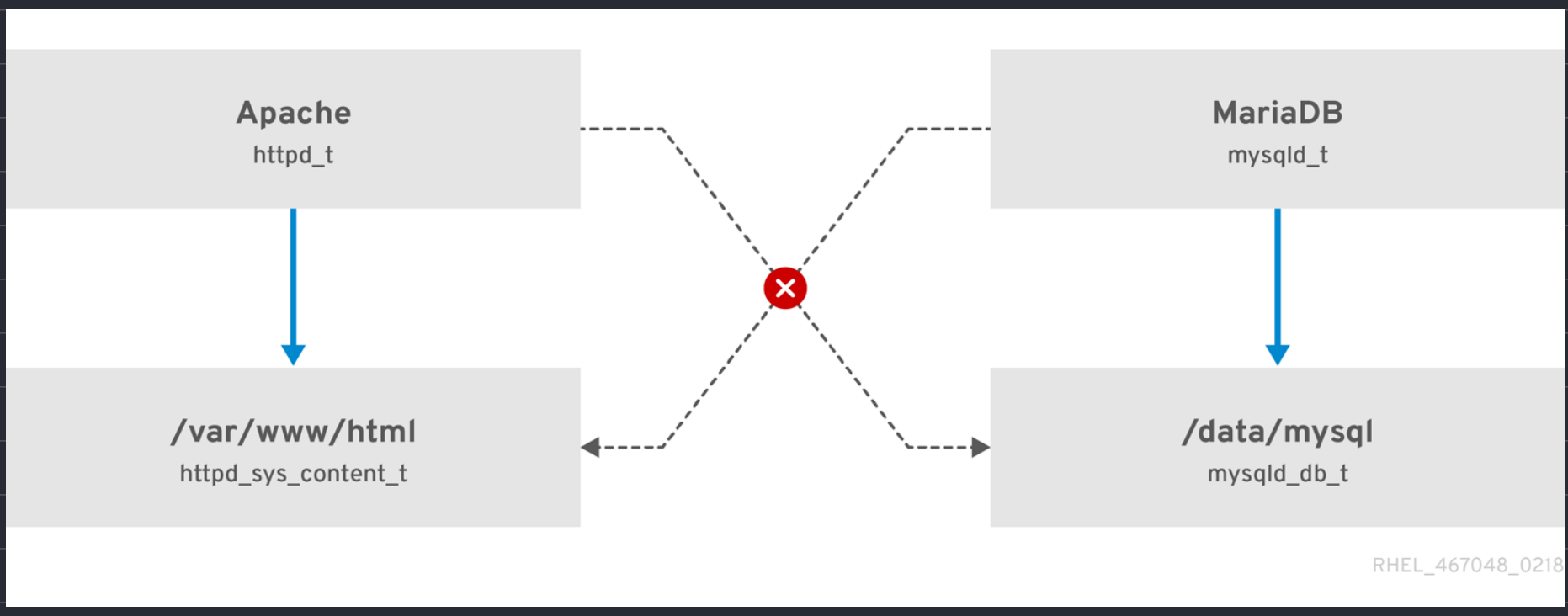
The standard access policy based on the user, group, and other permissions, known as Discretionary Access Control (DAC), does not enable system administrators to create comprehensive and fine-grained security policies, such as restricting specific applications to only viewing log files, while allowing other applications to append new data to the log files.

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called a SELinux context. A SELinux context, sometimes referred to as a SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods; for example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.
Note : It is important to remember that SELinux policy rules are checked after DAC rules. SELinux policy rules are not used if DAC rules deny access first, which means that no SELinux denial is logged if the traditional DAC rules prevent the access.

SELinux contexts have several fields: user, role, type, and security level. The SELinux type information is perhaps the most important when it comes to the SELinux policy, as the most common policy rule which defines the allowed interactions between processes and system resources uses SELinux types and not the full SELinux context. SELinux types usually end with _t. For example, the type name for the web server is httpd_t. The type context for files and directories normally found in /var/www/html/ is httpd_sys_content_t. The type contexts for files and directories normally found in /tmp and /var/tmp/ is tmp_t. The type context for web server ports is http_port_t.

For example, there is a policy rule that permits Apache (the web server process running as httpd_t) to access files and directories with a context normally found in /var/www/html/ and other web server directories (httpd_sys_content_t). There is no allow rule in the policy for files normally found in /tmp and /var/tmp/, so access is not permitted. With SELinux, even if Apache is compromised, and a malicious script gains access, it is still not able to access the /tmp directory.



Create and Manage RAID Devices :

With Raid, we can take multiple storage devices and combine them into a single storage area.

- LVM offers a flexible way to manage storage with features like resizing, snapshots, and easier administration.

- RAID focuses on data redundancy and performance gains through striping or mirroring techniques.

Types :

Level 0 or Stripe array : A bunch of disks are grouped in level zero raid and then Linux sees them as a single storage area.

this type of ray is risky to use because if we lose one disk, then the data on the entire array is lost.

- Advantages: Increased read and write speed.

- Disadvantages: No fault tolerance; if one disk fails, all data is lost.

Level 1 raid or a Mirrored array. Level 1 is a Redundant Array of Independent Disks : keep the same data in multiple places.

If one place fails, then we can recover data from some other place where a copy exists.

When we write a file to this array, the same file actually gets written to all three disks.

- Advantages: High fault tolerance; data remains accessible if one disk fails.

- Disadvantages: Storage capacity is halved; performance may be slightly reduced.

RAID 5 (Striping with Parity) : this requires a minimum of three disks in a level five array.
Data and parity information are striped across three or more disks. Parity allows recovery of data in case of a single disk failure.

- Advantages: Fault tolerance and efficient use of disk space.
- Disadvantages: Write performance can be affected due to parity calculation; one disk failure is tolerable, but not more.

We can lose one disk and our data will still be saved. That's because a raid five array will keep something called parity on each disk.

The parity information is distributed across all the disks, not stored on a single disk.

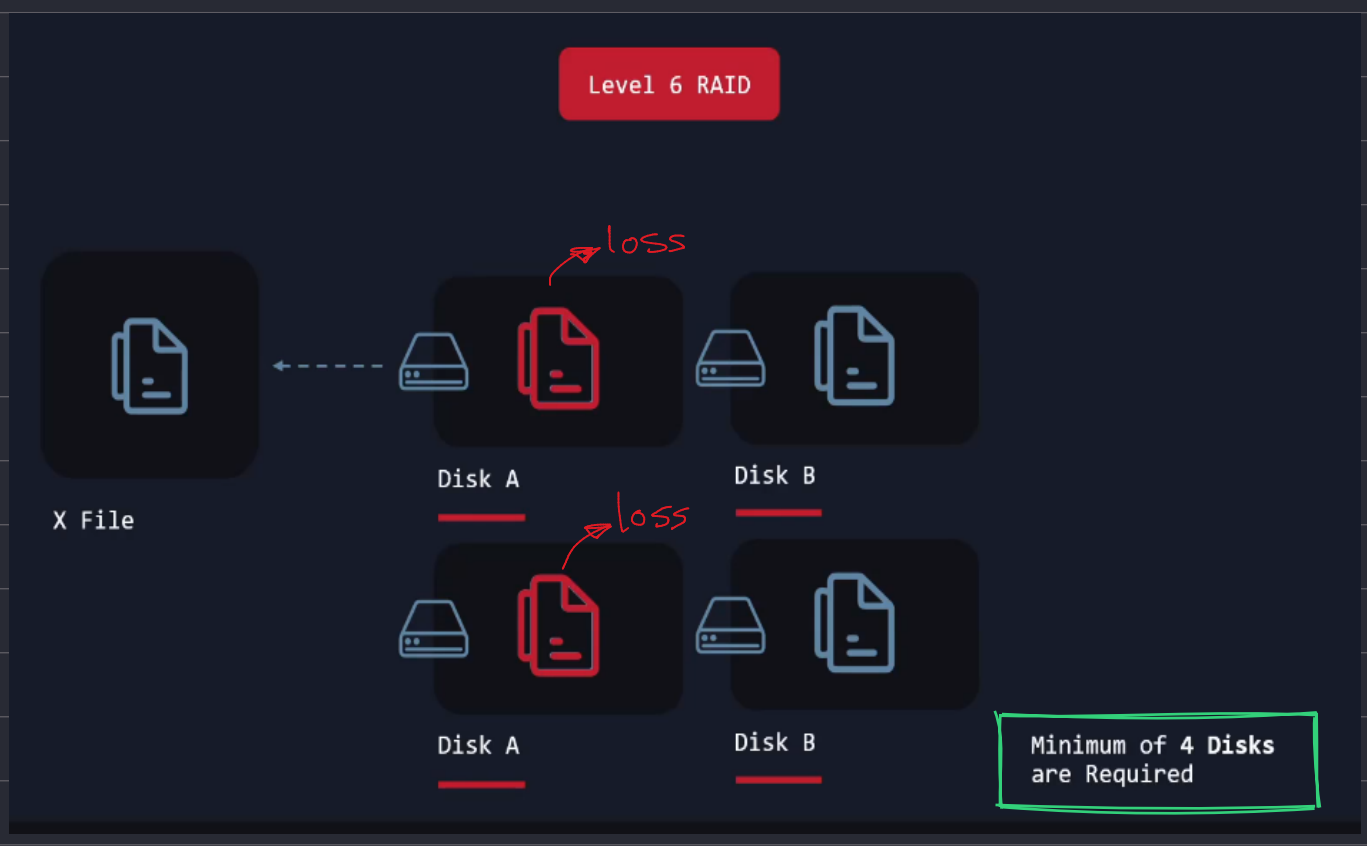
We can think of this parity as some sort of extra information, a small backup that can be used to rebuild in lost information.

if we lose one disk, we'll still have some parity on the other two disks. And parity on these disks can be used to rebuild the data loss from the first disk.

If we have three disks of one terabyte, we'll get two terabytes of usable space because one terabyte will be used to prepare it. Basically 0.33 terabytes of parity will be stored on the first disk, 0.33 terabytes on the second and 0.33 on the third.

If we have ten disks of one terabyte instead, we'd get nine terabytes of usable space.

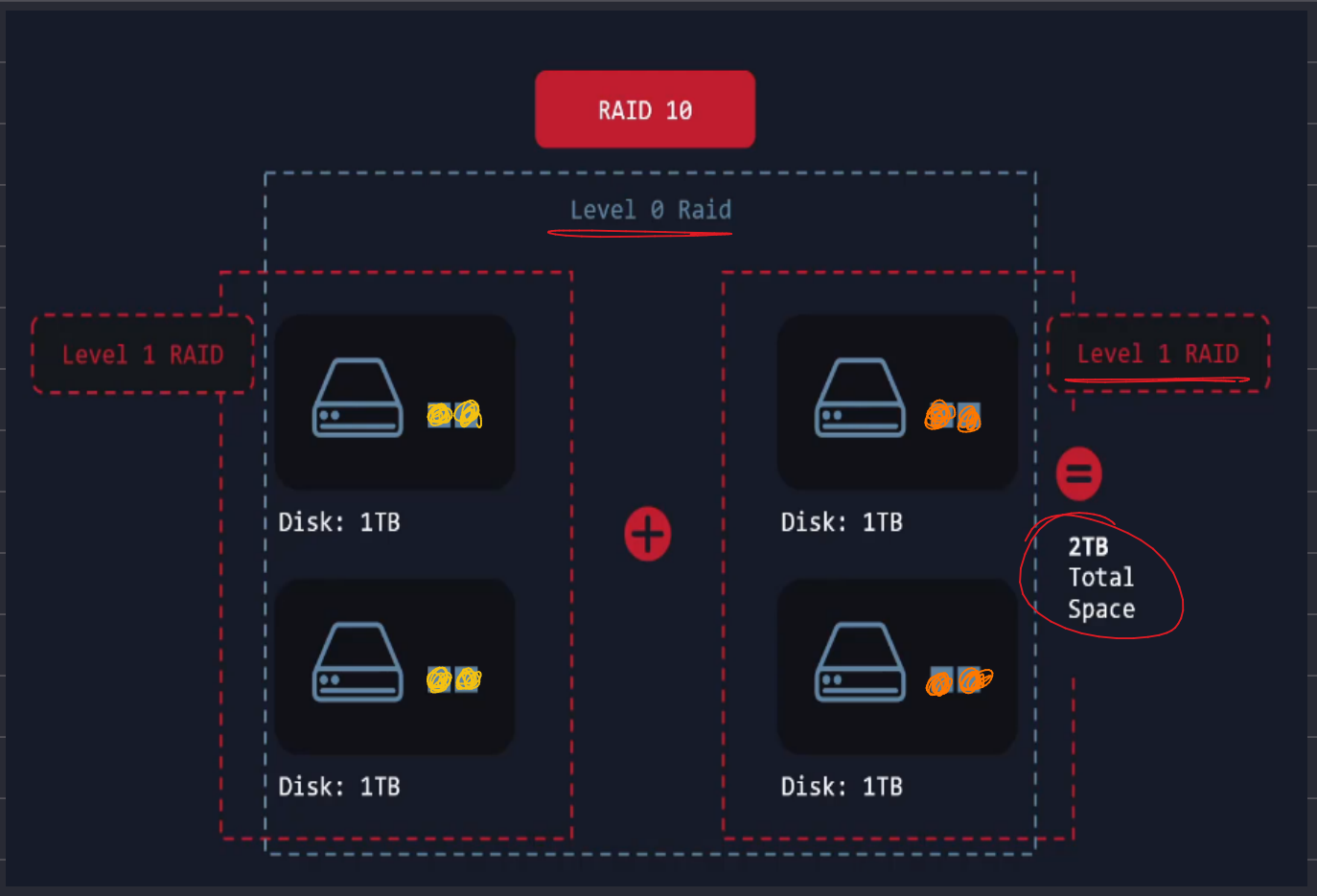
One disk can be lost and data should still be recoverable.



RAID 6 (Striping with Double Parity) :
Similar to RAID 5 but with two parity blocks for each data block, requiring at least four disks.

this level is as level five, but we can lose two disks instead of one

RAID 10 (1+0, Striping and Mirroring)
Combines RAID 0 and RAID 1 by mirroring data across pairs of disks, then striping across these mirrored pairs.




```
$ sudo vgremove --force my_volume

$ sudo pvremove /dev/vdc /dev/vdd /dev/vde

$ sudo mdadm --create /dev/md0 --level=0 --raid-devices=3 /dev/vdc /dev/vdd /dev/vde

$ sudo mkfs.ext4 /dev/md0
# if you want to delete raid:
$ sudo mdadm --stop /dev/md0   ① → stop
```

When you use --zero-superblock, you are clearing any RAID metadata from the specified disks. This is useful when you want to repurpose the disks for a new RAID array or other uses and need to remove any existing RAID configuration:

```
$ sudo mdadm --zero-superblock /dev/vdc /dev/vdd /dev/vde
```
② → delete super block

```
$ sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/vdc /dev/vdd --spare-devices=1 /dev/vde

$ sudo mdadm --stop /dev/md0

$ sudo mdadm --zero-superblock /dev/vdc /dev/vdd /dev/vde
```

This command will set up a RAID 1 array named /dev/md0 with two active devices (/dev/vdc and /dev/vdd) and one spare device (/dev/vde). The RAID 1 configuration ensures that all data is mirrored across the two active disks, providing redundancy. The spare device will automatically take over in case one of the active devices fails, maintaining the RAID 1 array's redundancy.

let's say that /dev/vdc fails. The operating system can detect this and then automatically add /dev/vde the spare device to the mirrored array.

```
$ sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/vdc /dev/vdd

$ sudo mdadm --manage /dev/md0 --add /dev/vde
```
add this device to this array

looking at the status of the arrays on our system, and you can find that information :

```
$ cat /proc/mdstat
Personalities : [raid0] [raid1]
md0 : active raid1 vde[2](S) vdd[1] vdc[0]
      5237760 blocks super 1.2 [2/2] [UU]

unused devices: <none>
```
→ Raid types
→ device name

if we want to remove a device from an array:

```
$ sudo mdadm --manage /dev/md0 --remove /dev/vde
```