Sri Lanka Institute of Information Technology
BSc Honors in Information Technology
Specializing in Cyber Security

IE3062-Data and Operating Systems Security

Student Name	Student ID Number
A A I Nethmika	IT23209534
Mendis W V A	IT23236028
Dissanayake Y Y	IT23238794
C L D Jayawardhana	IT23325296

Table of Contents

Task 01

01.Compare and contrast 5 Linux distribution

1. Ubuntu

- ***Features***: Built on Debian, available in Desktop and Server versions, easily installable and frequently updated.
- ***Strengths:*** Huge community, long-term support (5 years) versions, lots of packages, lots of documentation.
- ***Weaknesses***: Frequent releases can mean a little more up down time than Debian sometimes, uses more resources than Debian

2. Debian

- ***Features***: Known for stability, a base for others including Ubuntu.
- ***Strengths***: Super stable, secure, and lightweight - great for servers with high uptime.
- ***Weaknesses***: Older software packages - it prioritizes stability over always having the latest versions.

3.CentOS Stream

- ***Features***: A rolling-release version of the next release version of Red Hat Enterprise Linux (RHEL).
- ***Strengths***: Enterprise approach has SELinux built in, many people are using it in production.
- ***Weaknesses***: Less stable than traditional CentOS due to pre-releases being accepted before the release of the last version of RHEL.

4. Oracle Linux

- ***Features***: Fully compatible with RHEL, maintained by Oracle, offers RHCK and UEK kernel options.
- ***Strengths***: Free to use, optimized for Oracle products, enterprise options for support.
- ***Weaknesses***: Small community tied to Oracle's commercial ecosystem.

5. Fedora

- ***Features***: Community-driven called an upstream distribution for RHEL, believes in innovation.
- ***Strengths***: Most up-to-date software, active developer community, great for use in testing.
- ***Weaknesses***: Short lifespan of latest releases (13 months) and not suitable for servers for long-term usage.

Justify the most suitable one

Oracle Linux is a powerful, enterprise-centric distribution that focuses on providing stability, speed, and compatibility with enterprise software. It has incorporated all the reliability of Red Hat Enterprise Linux with optimizations made specifically for Oracle products. This makes it an easy solution for servers that need dependable performance to be consistent, secure, and scalable. Here are some of the reasons, Oracle Linux is perfect for this server ecosystem

1.RHEL Compatibility

Oracle Linux is a fully compatible clone of Red Hat Enterprise Linux (RHEL) which gives users of Oracle Linux access to various amounts of enterprise grade software and tools enhancing ease of deployment in production organizations.

2.Enterprise Optimization

The Unbreakable Enterprise Kernel (UEK) and Red Hat Compatible Kernel (RHCK) are both optimized for performance and reliability for enterprise applications, databases or anything that requires the same kind of stable server workloads.

3.Cost Effectiveness

Oracle Linux is free to download and use, without having to pay any subscription fees to have an enterprise level product available to them, which is beneficial to those organizations that are looking for a stable server OS with low license costs.

4.Security and Support

As with most enterprise-grade Linux kernel OS they have several different security features like SELinux and enterprise style patch management. If an organization wants guaranteed support they can, although it is optional, get enterprise level assistance when required, but they are very flexible.

5.Integration with Oracle Products

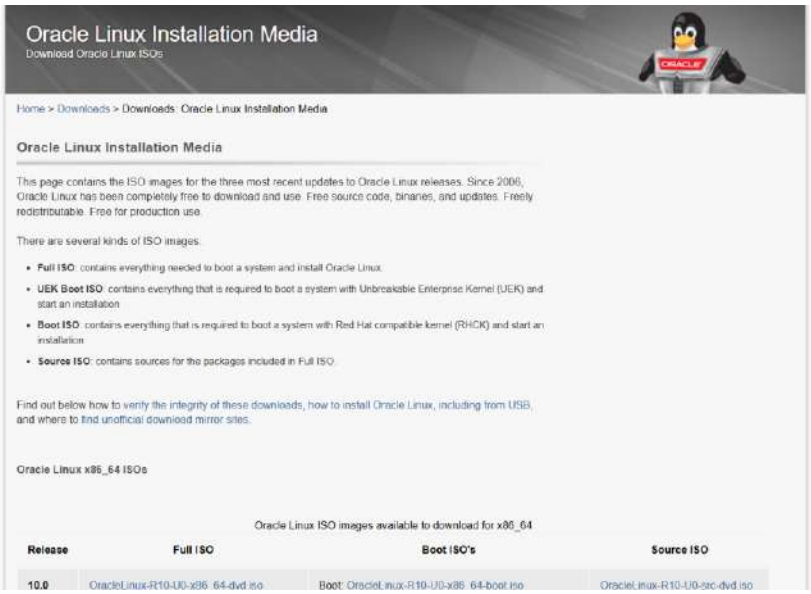
Oracle Linux is tailored and optimized for their intensive databases, middleware products, and cloud services. Providing assurance of performance, stability, and support when systems are based on Oracle products.

6.Stability and Reliability

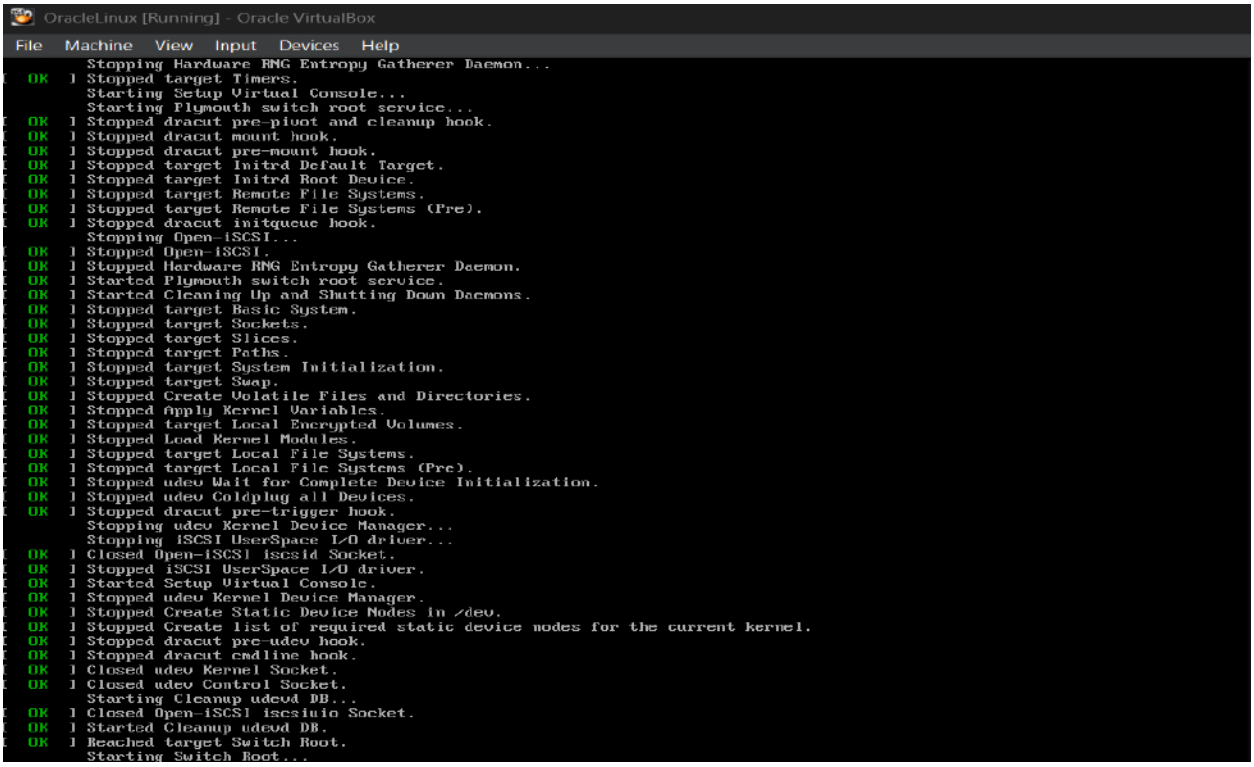
The OS is well known for its excellent uptime and reliability which are only a few characteristics one desires to have in a critical server environment.

02. Oracle Linux Installation

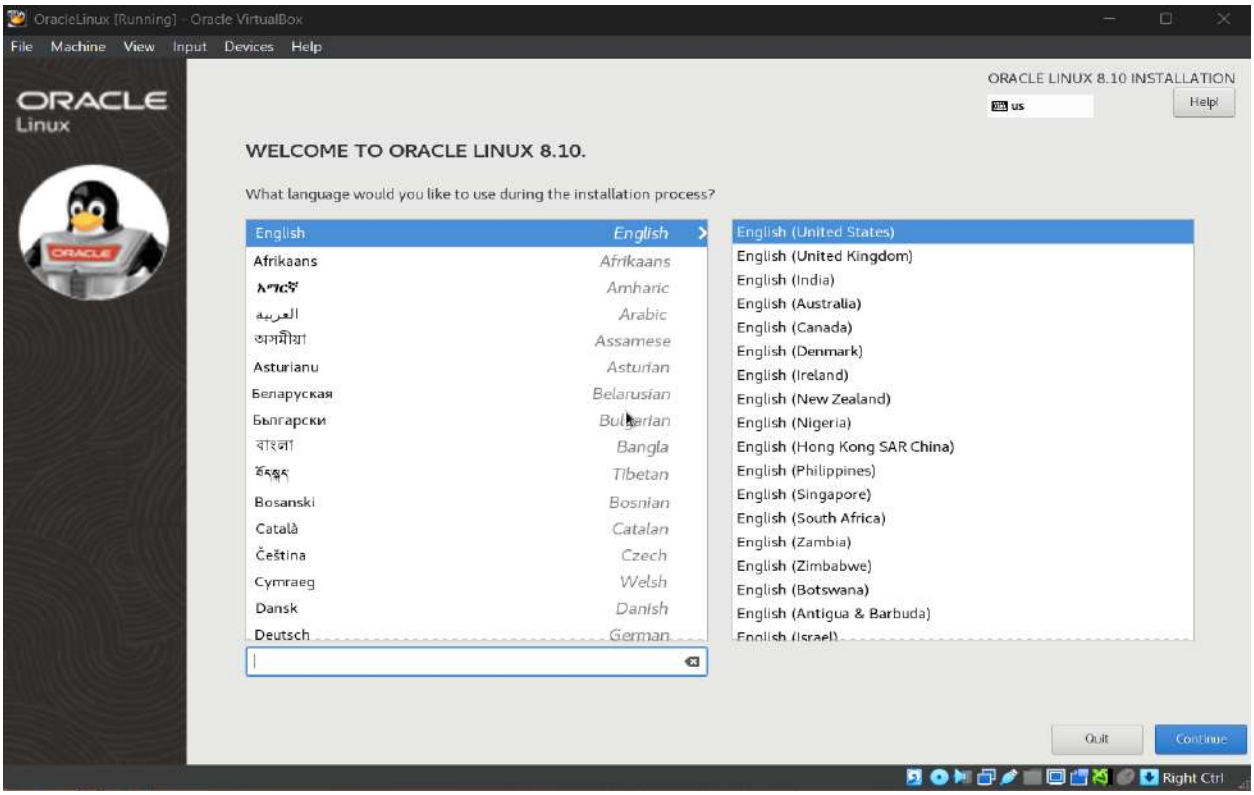
1. Download Oracle Linux image file from https://yum.oracle.com/oracle-linux-isos.html



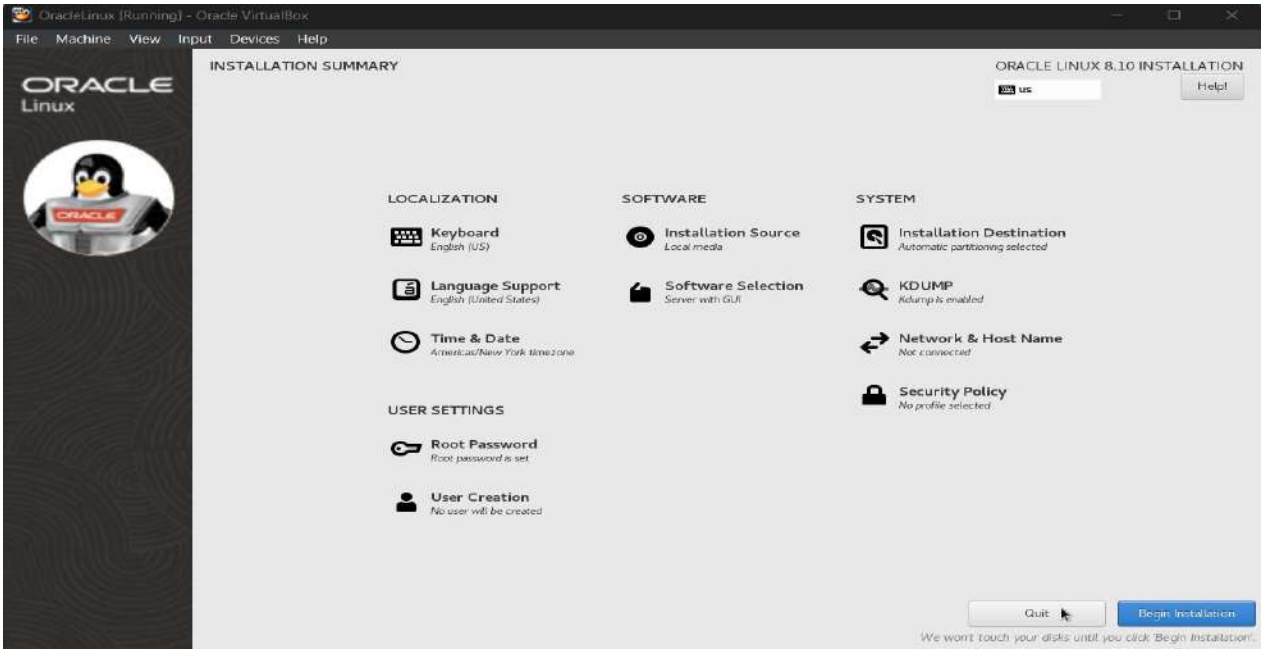
2. Add the downloaded ISO file to Virtual box and run the VM. Then install Oracle Linux.



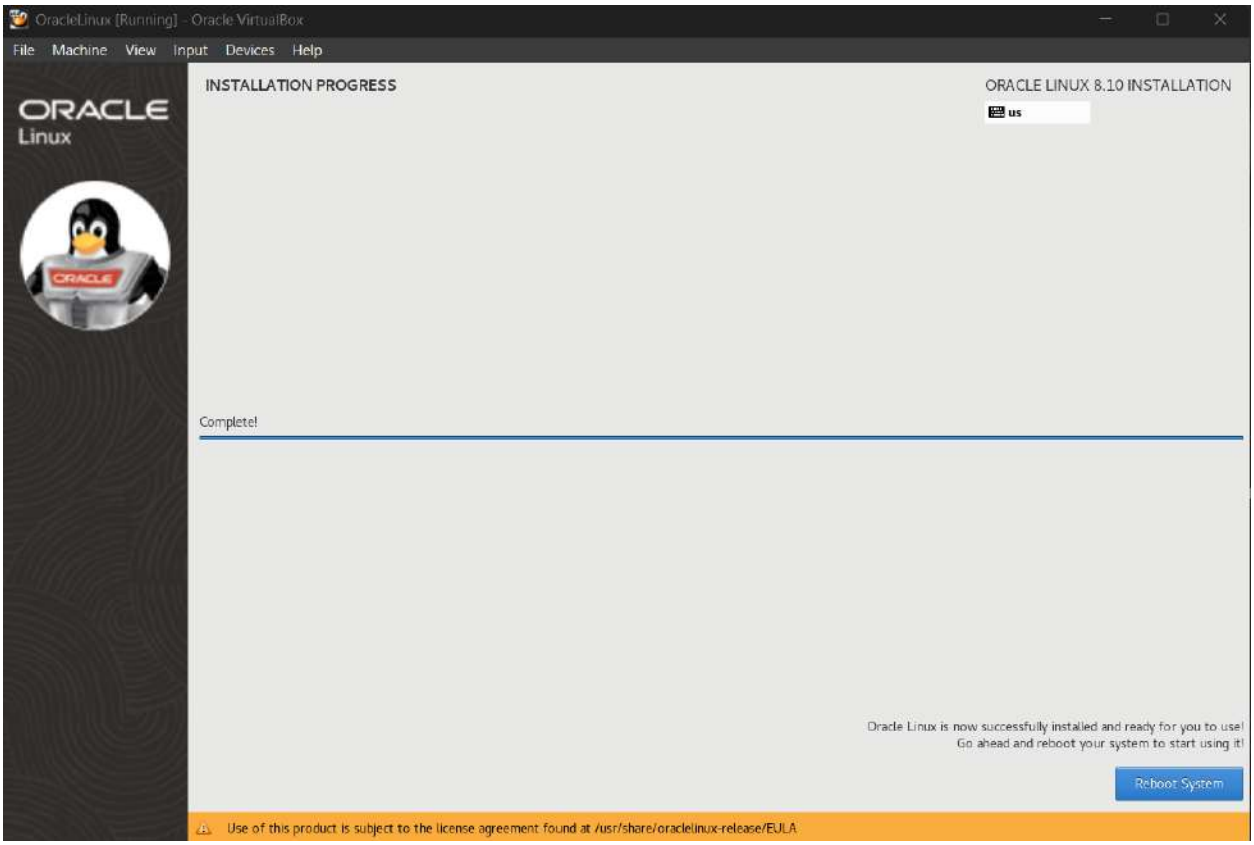
3. Then select the language and press continue



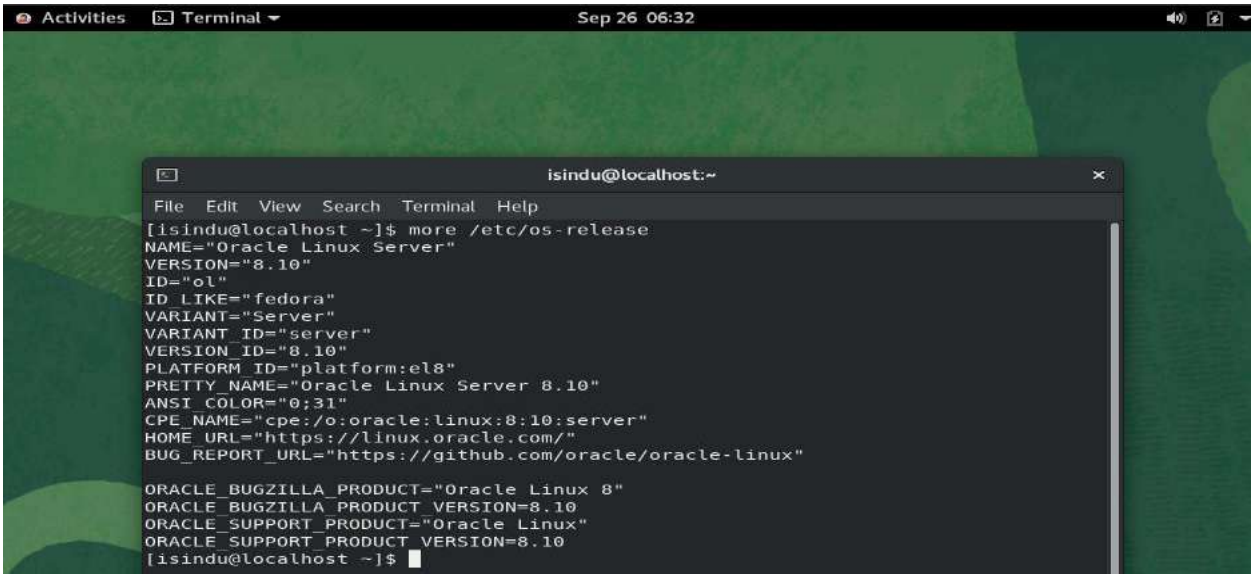
4. Then set a root password and begin installation

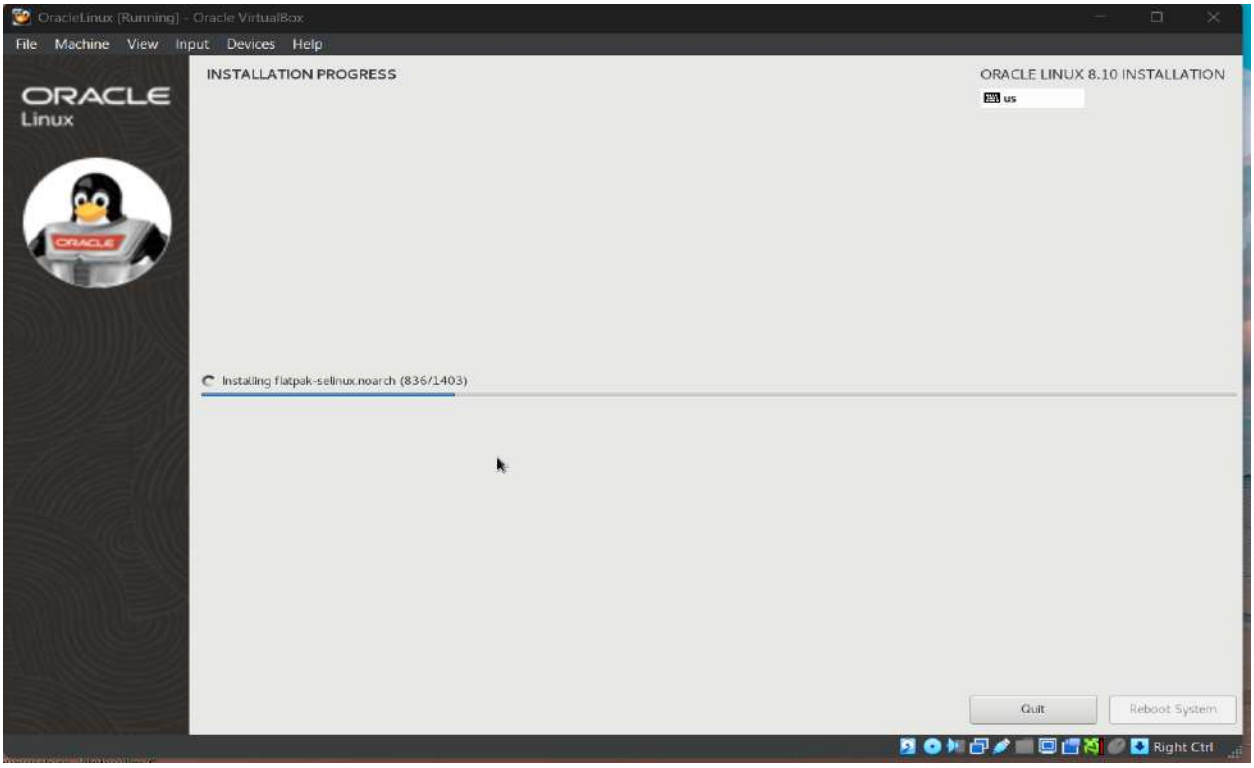


5. After the installation process completed click on Reboot System



6. Then complete the set up and continue using.




OracleLinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
ORACLE
Linux
INSTALLATION PROGRESS
ORACLE LINUX 8.10 INSTALLATION
us
Installing flatpak-selinux.noarch (836/1403)
Quit
Reboot System
Right Ctrl

03.Analyze the security risks and Harden the Distribution

Security Risks Facing the Server

1.Unauthorised access

Weakness or default credentials can allow unauthorized users to gain administrative or database access.

2.SQL injection

Web applications and/or backend services using a database can be forced to create queries that are malicious with respect to that data, which can expose or change sensitive data.

3.Denial-of-Service attacks

High traffic or deliberately crafted requests can overwhelm services either putting them down or exhausting resources.

4.Unpatched vulnerabilities

Without maintaining the operating system and software with updates, leave targets open for known exploits.

5.Firewall configuration

Open or misconfigured firewall rules can create a security issue creating a backdoor on the web service protecting a server.

6.Malware and rootkits

Microsoft Windows, Linux, or Mac systems typically lack monitoring tools that detect malicious software that can hijack the operating system by corrupting its integrity or remaining hidden on the operating system.

7.Data Leakage

Sensitive files and/or credentials are at risk of exposure by users not employing appropriate access controls.

8.Privilege escalation

Unnecessary permissions for users or services can be exploited to gain root access to the server.

9.Misconfigured services

Services often come with default SSH, database, or web server installed. This default configuration may expose servers or resources to vulnerabilities and attacks without appropriate training in their use

10.Insufficient encryption

Encryption encrypting sensitive files at rest or in transit can be intercepted or compromised.

Hardening Oracle

1.Automatic Security Updates

Rolling updates on the OS and software you create with yum update or dnf update update will patch vulnerabilities, bugs, and security risk on the system.

2.Firewall Properly Configured

Using firewall or iptables rules to limit services and ports will restrict unauthorized network traffic and the use of potentially exploited services.

3.SELinux Enabled

Set SELinux to enforcing mode, with a long-term goal of moving to targeted mode and type enforcement. SELinux provides mandatory access to the OS files and processes only to the access and actions that are acceptable - even if the user or any application is exploited.

4.Disable Unused Services

Use the systemctl list-units command to identify running or unneeded services, which you can stop or disable--thus reducing attack surface area and compromise points.

5.Harden SSH Access

Disable root access, use key-only access and restricted logons, and change the default SSH service port to lower brute-force attempts and increase protection against unwanted login.

6.Implement Strong Password Policies

Edit and define password complexity, expiration, and reuse policy in /etc/security/pwquality.conf, to harden user accounts against guessing and brute-force attacks.

7.Enable Auditing and Logging

The audit application can utilize monitoring and logging of critical system events. Audit logs can be forwarded to a central server and gives you the opportunity to detect any suspicious activity or potential compromise.

8.Protect Database from SQL Injection

Help to protect applications from SQL injection vulnerabilities by using parameterized SQL queries, validating user input, and granting critical least privileges to database user access.

9.Mitigating DoS Attacks

Implement rate-limiting rules in iptables or those implemented in your firewall, along with server-layer and database-layer settings to prevent resource consumption hacks as well keep servers available during loading attacks that would lead to a normal life cycle acceptance.

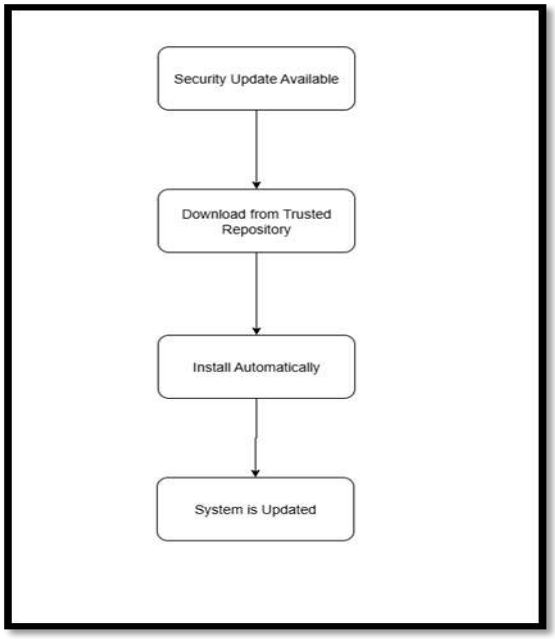
10.Encryption of Data and Communications

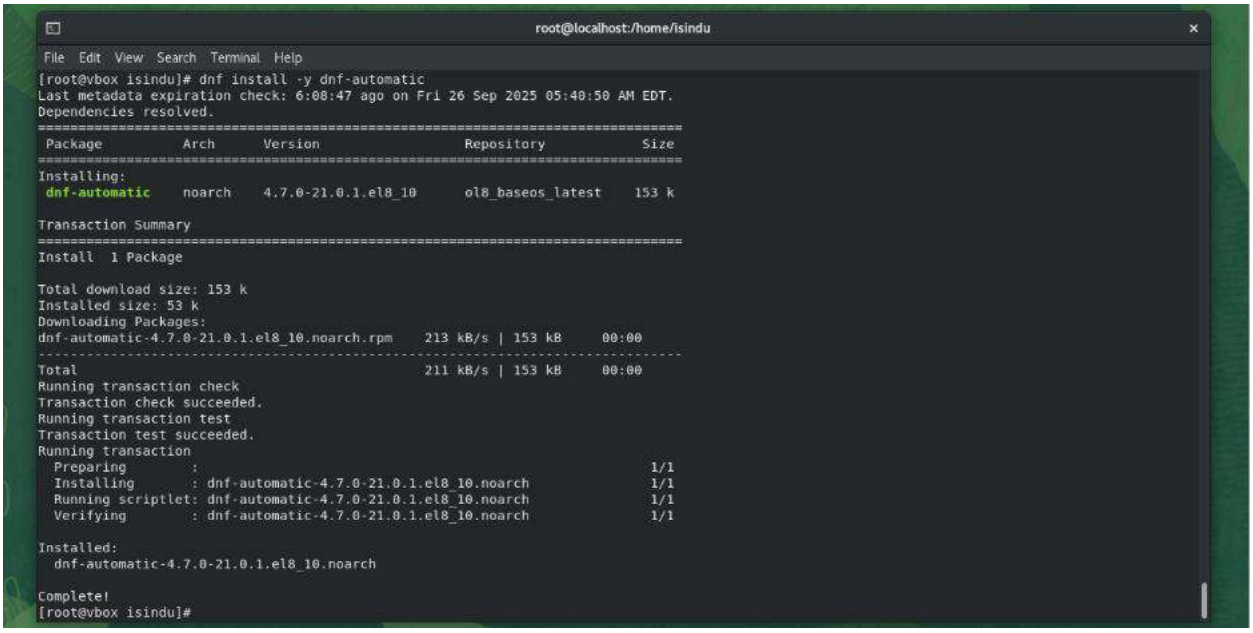
Make sure you protect sensitive data through disk encryption like LUKS, for all your communications use TLS/SSL, and keep data at rest or in transit protected.

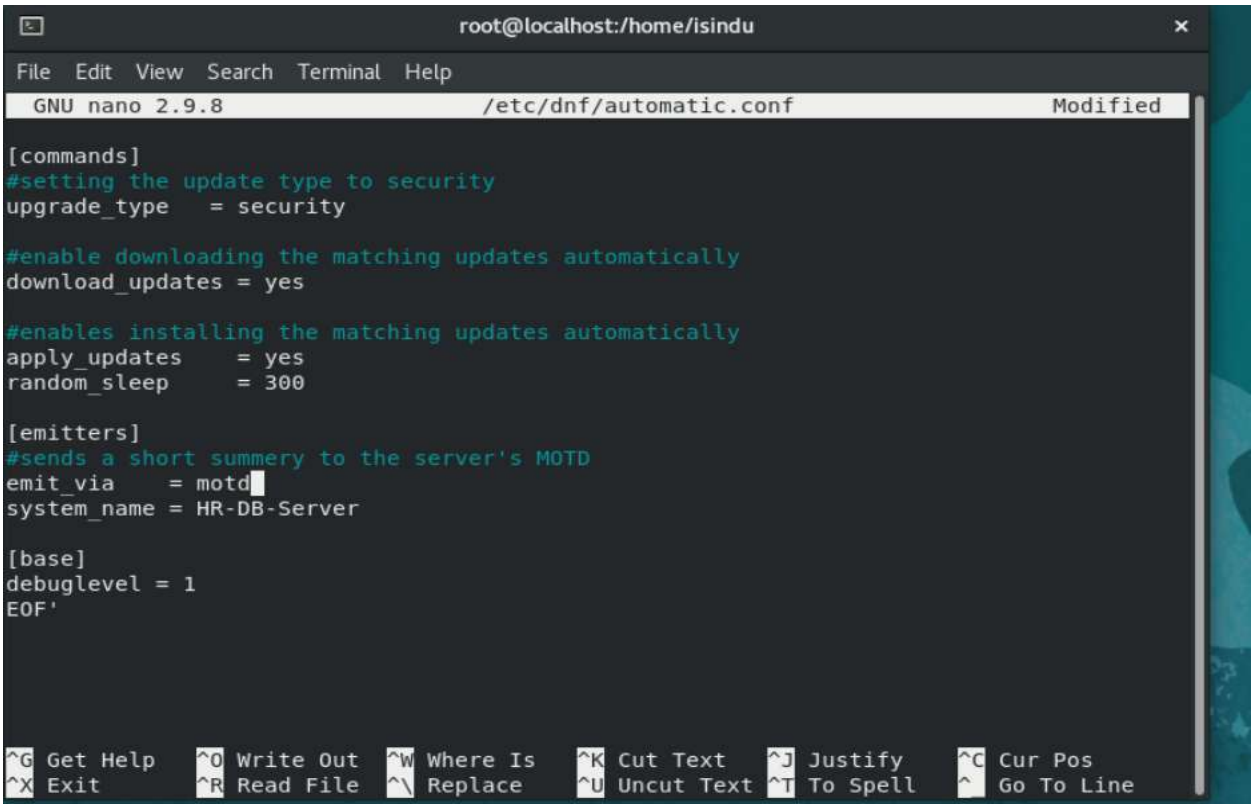
04.Diagrams to Document Configurations

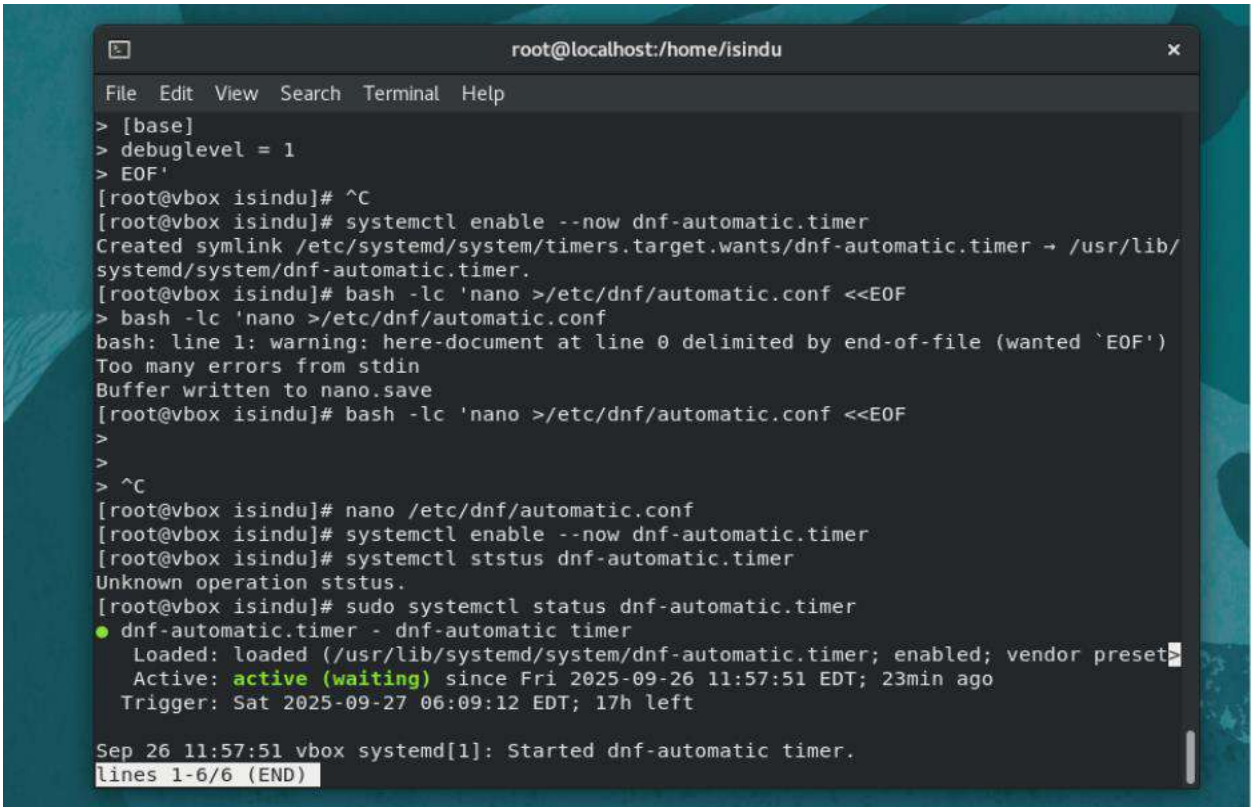
1.Automatic Security Updates

- By downloading and installing updates, you can keep your software up to date automatically.
- Security patches are applied at once with automatic updates.
- Hackers have more difficulties to take advantage of software vulnerabilities in older versions.
- Protects against: Incidents targeting vulnerable software areas Unlawful access to zero-day vulnerabilities.



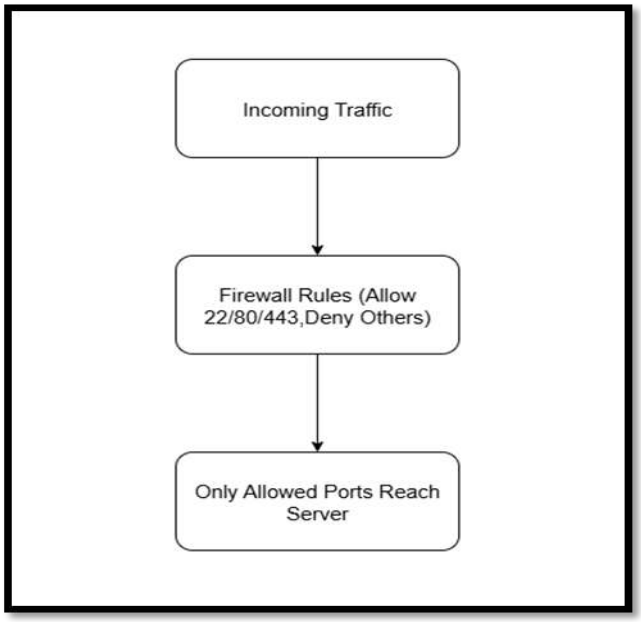


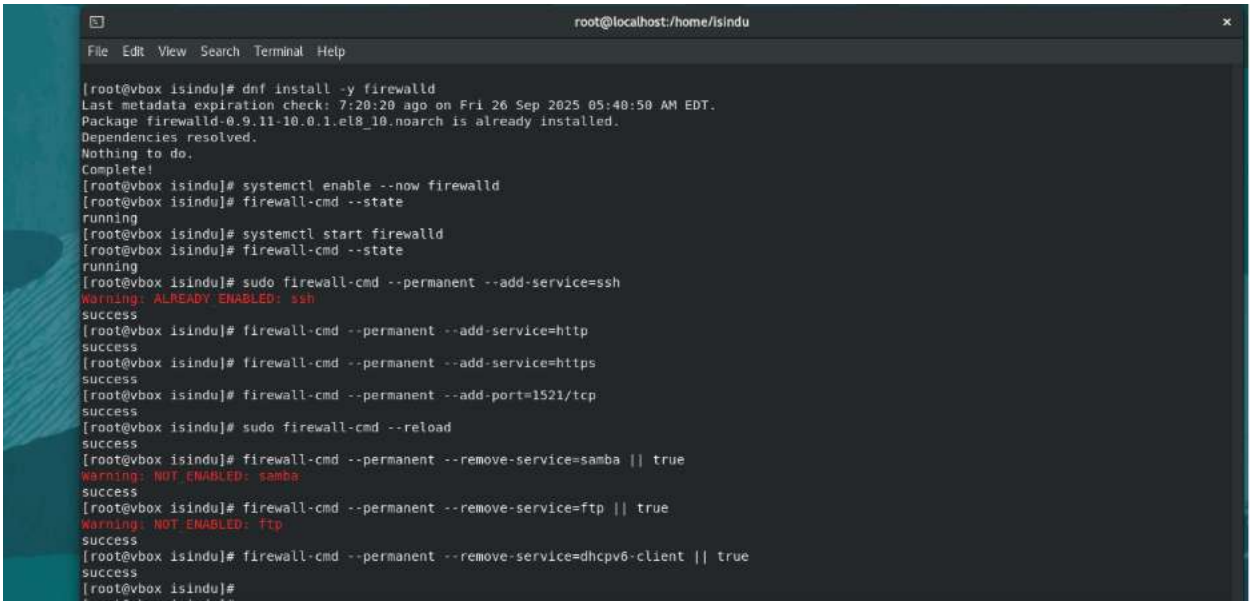

root@localhost:/home/isindu
File Edit View Search Terminal Help
GNU nano 2.9.8 /etc/dnf/automatic.conf Modified
[commands]
#setting the update type to security
upgrade_type = security
#enable downloading the matching updates automatically
download_updates = yes
#enables installing the matching updates automatically
apply_updates = yes
random_sleep = 300
[emitters]
#sends a short summery to the server's MOTD
emit_via = motd
system_name = HR-DB-Server
[base]
debuglevel = 1
EOF'
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line


root@localhost:/home/isindu
File Edit View Search Terminal Help
> [base]
> debuglevel = 1
> EOF'
[root@vbox isindu]# ^C
[root@vbox isindu]# systemctl enable --now dnf-automatic.timer
Created symlink /etc/systemd/system/timers.target.wants/dnf-automatic.timer → /usr/lib/systemd/system/dnf-automatic.timer.
[root@vbox isindu]# bash -lc 'nano >/etc/dnf/automatic.conf <<EOF
> bash -lc 'nano >/etc/dnf/automatic.conf
bash: line 1: warning: here-document at line 0 delimited by end-of-file (wanted `EOF')
Too many errors from stdin
Buffer written to nano.save
[root@vbox isindu]# bash -lc 'nano >/etc/dnf/automatic.conf <<EOF
>
>
> ^C
[root@vbox isindu]# nano /etc/dnf/automatic.conf
[root@vbox isindu]# systemctl enable --now dnf-automatic.timer
[root@vbox isindu]# systemctl ststus dnf-automatic.timer
Unknown operation ststus.
[root@vbox isindu]# sudo systemctl status dnf-automatic.timer
● dnf-automatic.timer - dnf-automatic timer
Loaded: loaded (/usr/lib/systemd/system/dnf-automatic.timer; enabled; vendor preset>
Active: active (waiting) since Fri 2025-09-26 11:57:51 EDT; 23min ago
Trigger: Sat 2025-09-27 06:09:12 EDT; 17h left
Sep 26 11:57:51 vbox systemd[1]: Started dnf-automatic timer.
lines 1-6/6 (END)

2.Firewall Properly Configured

- Firewalls decide which information can go into or out of the network depending on a set of security rules.
- Only open those ports that are absolutely necessary (e.g., 22 for SSH, 80/443 for web traffic) so that the exposure is minimized.
- Reduces the system's susceptibility to attackers.
- Helps the system against:
    - Unauthorized access
    - Port scanning
    - Network-based attacks

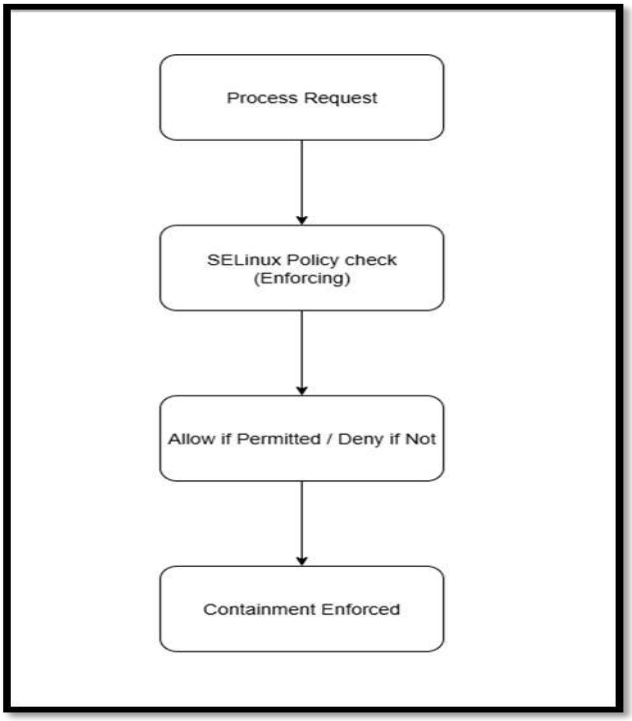




```
root@localhost:/home/isindu
File  Edit  View  Search  Terminal  Help
[root@vbox isindu]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: http https ssh
  ports: 1521/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

3.SELinux Enabled

- Security-Enhanced Linux (SELinux) implements mandatory access control (MAC) policy.
- Such limitations prohibit the functionalities of the processes, thus, even in the case of a security breach, the intruder's capabilities will be minimal.
- SELinux thus forms one more bulwark of security against mistakes on the part of the system or misuse by the user.
- Protection Offered Against: Power increases beyond authorized Access to files or processes without permission

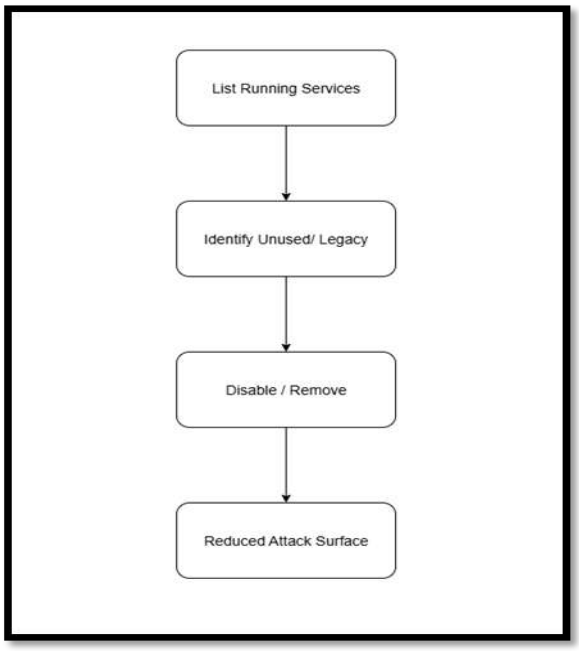


```
[root@localhost ~]# getenforce
Permissive
[root@localhost ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@localhost ~]# sed -i 's/^SELINUX=.*/SELINUX=enforcing/' /etc/selinux/confi
g
[root@localhost ~]# grep ^SELINUX= /etc/selinux/config
SELINUX=enforcing
```

```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[root@localhost ~]# ps -eZ | egrep 'sshd|tnslsnr|pmon|smon|oracle' || true
system_u:system_r:sshd_t:s0-s0:c0.c1023 1155 ?   00:00:00 sshd
```

4.Disable Unused Services

- Security-Enhanced Linux (SELinux) utilizes mandatory access control (MAC) policies.
- Such restrictions limit the actions of processes, therefore, in case a hacker will be able to access the system.
- Moreover, SELinux does not only add a safety fence against hardware or software failures, it also guards the system from the user's incorrect operations.
- Defends the system from: Privilege escalation Access to files or processes without authorization.



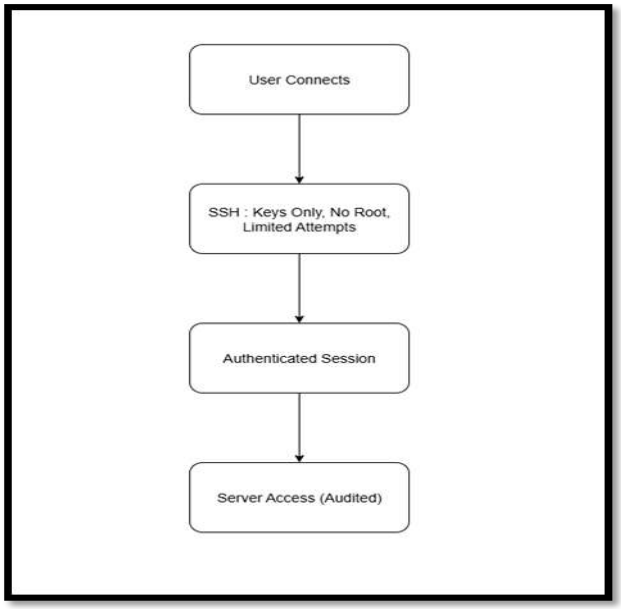

```
[root@localhost ~]# systemctl status sshd firewalld chronyd rsyslog auditd crond NetworkManager dnf-auto
matic.timer
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset>
   Active: active (running) since Sun 2025-10-05 04:11:17 EDT; 1h 10min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1155 (sshd)
    Tasks: 1 (limit: 10362)
   Memory: 2.0M
   CGroup: /system.slice/sshd.service
           └─1155 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-p>

Oct 05 04:11:17 localhost.localdomain systemd[1]: Starting OpenSSH server daemo>
Oct 05 04:11:17 localhost.localdomain sshd[1155]: Server listening on 0.0.0.0 p>
Oct 05 04:11:17 localhost.localdomain sshd[1155]: Server listening on :: port 2>
Oct 05 04:11:17 localhost.localdomain systemd[1]: Started OpenSSH server daemon.

● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor p>
   Active: active (running) since Sun 2025-10-05 04:11:17 EDT; 1h 10min ago
     Docs: man:firewalld(1)
 Main PID: 860 (firewalld)
    Tasks: 2 (limit: 10362)
   Memory: 41.8M
lines 1-23...skipping...
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-10-05 04:11:17 EDT; 1h 10min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1155 (sshd)
    Tasks: 1 (limit: 10362)
   Memory: 2.0M
   CGroup: /system.slice/sshd.service
           └─1155 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes2>

Oct 05 04:11:17 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Oct 05 04:11:17 localhost.localdomain sshd[1155]: Server listening on 0.0.0.0 port 22.
Oct 05 04:11:17 localhost.localdomain sshd[1155]: Server listening on :: port 22.
Oct 05 04:11:17 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
```

```
[root@localhost ~]# virsh net-destroy default && virsh net-autostart default --disable

Network default destroyed

Network default unmarked as autostarted

[root@localhost ~]#
[root@localhost ~]# ss -tupen
Netid    State     Recv-Q     Send-Q         Local Address:Port         Peer Address:Port    Process
[root@localhost ~]# ^C
[root@localhost ~]# ss -tulpen
Failed to find cgroup2 mount
Failed to find cgroup2 mount
Failed to find cgroup2 mount
Failed to find cgroup2 mount
Failed to find cgroup2 mount
Netid State  Recv-Q  Send-Q   Local Address:Port   Peer Address:Port Process

udp   UNCONN 0       0            127.0.0.1:323         0.0.0.0:*     users:(("chronyd",pid=1230,fd=5))
 ino:26831 sk:1 cgroup:unreachable:1 <->
udp   UNCONN 0       0                [::1]:323            [::]:*     users:(("chronyd",pid=1230,fd=6))
 ino:26832 sk:2 cgroup:unreachable:1 v6only:1 <->
tcp   LISTEN 0       128            0.0.0.0:22          0.0.0.0:*     users:(("sshd",pid=1155,fd=3))
 ino:26090 sk:3 cgroup:unreachable:1 <->
tcp   LISTEN 0       128              [::]:22             [::]:*     users:(("sshd",pid=1155,fd=4))
 ino:26104 sk:4 cgroup:unreachable:1 v6only:1 <->
[root@localhost ~]# firewall-cmd --permanent --add-port=1521/tcp
You're performing an operation over default zone ('public'),
but your connections/interfaces are in zone 'libvirt' (see --get-active-zones)
You most likely need to use --zone=libvirt option.

Warning: ALREADY_ENABLED: 1521:tcp
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --remove-service=http
success
[root@localhost ~]# firewall-cmd --permanent --zone=public --remove-service=https
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh
  ports: 1521/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost ~]#
```

5. Harden SSH Access

- Secure Shell (SSH) hardening is a set of measures: Using exclusively key-based authentication Turning off root login Limiting the number of login attempts
- These measures improve the security of remote access.
- By SSH only those allowed connect.
- Preventing the system from becoming the victim of: Brute-force attacks Unauthorized remote access.




```
[root@localhost ~]# sshd -T | egrep '^(permitrootlogin|maxauthtries|passwordauthentication|pubkeyauthent
ication|port|allowusers)\b'
port 22
maxauthtries 6
permitrootlogin yes
pubkeyauthentication yes
passwordauthentication yes
```

```
[root@localhost ~]# sed -i -E \
>    -e 's/^#?PermitRootLogin.*/PermitRootLogin no/' \
>    -e 's/^#?PasswordAuthentication.*/PasswordAuthentication no/' \
>    -e 's/^#?PubkeyAuthentication.*/PubkeyAuthentication yes/' \
>    -e 's/^#?MaxAuthTries.*/MaxAuthTries 3/' \
> /etc/ssh/sshd_config
[root@localhost ~]# sshd -t && echo "sshd config OK"
sshd config OK
[root@localhost ~]# systemctl restart sshd && echo "sshd restarted"
sshd restarted
[root@localhost ~]# sshd -T | egrep '^(permitrootlogin|maxauthtries|passwordauthentication|pubkeyauthenticati
on|port|allowusers)\b'
port 22
maxauthtries 3
permitrootlogin no
pubkeyauthentication yes
passwordauthentication no
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 service name="ss
h" limit value="5/m" accept' && \
> firewall-cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 service name="ssh" drop' && \
> firewall-cmd --reload && \
> firewall-cmd --zone=public --list-rich-rules
success
success
success
rule family="ipv4" service name="ssh" accept limit value="5/m"
rule family="ipv4" service name="ssh" drop
[root@localhost ~]#
```

6.Implement Strong Password Policies

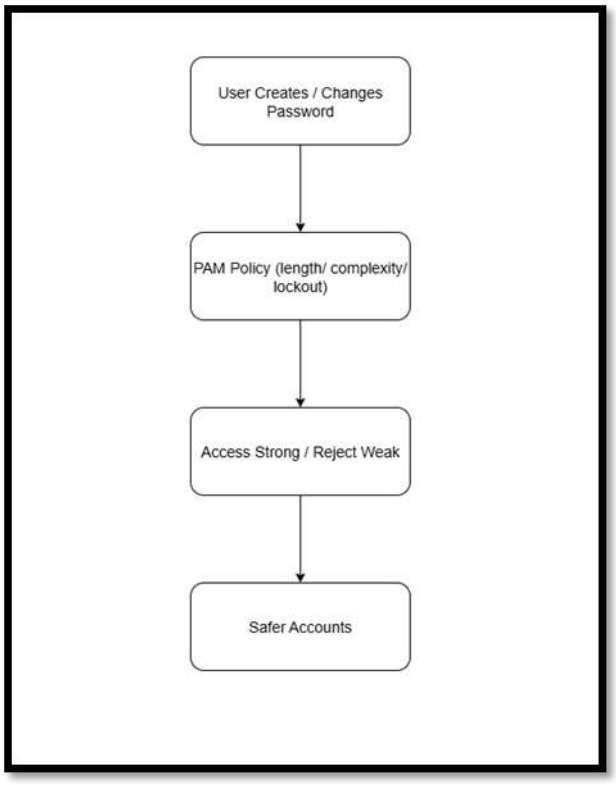
Password policies enforce:

- Complexity requirements
- Minimum length
- Account lockout after failed attempts

These policies encourage users to create strong passwords that are difficult to guess or crack.

Protects Against:

- Unauthorized account access
- Dictionary attacks
- Password guessing



a. Account lockout [faillock]

```
[root@localhost ~]# sed -i -E 's/^\s*#?\s*deny\s*=.*/deny = 5/' /etc/security/faillock.conf
[root@localhost ~]# ed -i -E 's/^\s*#?\s*unlock_time\s*=.*/unlock_time = 900/' /etc/security/faillock.conf
ed: invalid option -- 'i'
Try 'ed --help' for more information.
[root@localhost ~]# sed -i -E 's/^\s*#?\s*unlock_time\s*=.*/unlock_time = 900/' /etc/security/faillock.conf
[root@localhost ~]# sed -i -E 's/^\s*#?\s*fail_interval\s*=.*/fail_interval = 900/' /etc/security/faillock.co
nf
[root@localhost ~]# grep -E '^\s*(deny|unlock_time|fail_interval)\s*=' /etc/security/faillock.conf
deny = 5
fail_interval = 900
unlock_time = 900
[root@localhost ~]#
```

```
[root@localhost ~]# authselect enable-feature with-pwquality 2>/dev/null || true
[root@localhost ~]# sed -i -E 's/^#?\s*minlen\s*=.*/minlen = 12/' /etc/security/pwquality.conf
[root@localhost ~]# sed -i -E 's/^#?\s*minclass\s*=.*/minclass = 3/' /etc/security/pwquality.conf
[root@localhost ~]# grep -E '^\s*(minlen|minclass)\s*=' /etc/security/pwquality.conf
minlen = 12
minclass = 3
[root@localhost ~]# grep -n 'pam_faillock' /etc/pam.d/system-auth /etc/pam.d/password-auth
/etc/pam.d/system-auth:6:auth        required                                    pam_faillock.so preauth silent
/etc/pam.d/system-auth:13:auth        required                                    pam_faillock.so authfail
/etc/pam.d/system-auth:16:account     required                                    pam_faillock.so
/etc/pam.d/password-auth:6:auth       required                                    pam_faillock.so preauth silent
/etc/pam.d/password-auth:12:auth       required                                    pam_faillock.so authfail
/etc/pam.d/password-auth:15:account     required                                    pam_faillock.so
[root@localhost ~]#
```

```
[root@localhost ~]# grep -E '^(deny|fail_interval|unlock_time)\s*=' /etc/security/faillock.conf
deny = 5
fail_interval = 900
unlock_time = 900
[root@localhost ~]# grep -n 'pam_faillock' /etc/pam.d/system-auth /etc/pam.d/password-auth
/etc/pam.d/system-auth:6:auth        required                                    pam_faillock.so preaut
h silent
/etc/pam.d/system-auth:12:auth        required                                    pam_faillock.so authf
ail
/etc/pam.d/system-auth:15:account     required                                    pam_faillock.so
/etc/pam.d/password-auth:6:auth       required                                    pam_faillock.so prea
uth silent
/etc/pam.d/password-auth:12:auth       required                                    pam_faillock.so aut
hfail
/etc/pam.d/password-auth:15:account     required                                    pam_faillock.so
[root@localhost ~]#
```

b. Complexity & length [pwquality]

```
[root@localhost ~]# authselect enable-feature with-pwquality 2>/dev/null || true
[root@localhost ~]# sed -i -E 's/^#?\s*minlen\s*=.*/minlen = 12/' /etc/security/pwquality.conf
[root@localhost ~]# sed -i -E 's/^#?\s*minclass\s*=.*/minclass = 3/' /etc/security/pwquality.conf
[root@localhost ~]# grep -E '^\s*(minlen|minclass)\s*=' /etc/security/pwquality.conf
minlen = 12
minclass = 3
```

```
[root@localhost ~]# grep -E '^(minlen|minclass)\s*=' /etc/security/pwquality.conf
minlen = 12
minclass = 3
[root@localhost ~]# grep -n 'pam_pwquality\.so' /etc/pam.d/system-auth /etc/pam.d/password-auth
/etc/pam.d/system-auth:22:password    requisite                                   pam_pwquality.so loca
l_users_only
/etc/pam.d/password-auth:22:password    requisite                                   pam_pwquality.so lo
cal users only
```

c. Rotation/aging defaults [login.defs + existing users]

```
[root@localhost ~]# sed -i 's/^#\?PASS_MAX_DAYS.*/PASS_MAX_DAYS   90/' /etc/login.defs
[root@localhost ~]# sed -i 's/^#\?PASS_MIN_DAYS.*/PASS_MIN_DAYS   7/'  /etc/login.defs
[root@localhost ~]# sed -i 's/^#\?PASS_WARN_AGE.*/PASS_WARN_AGE   7/'  /etc/login.defs
[root@localhost ~]# grep -E 'PASS_MAX_DAYS|PASS_MIN_DAYS|PASS_WARN_AGE' /etc/login.defs
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   7
[root@localhost ~]# chage -M 90 -m 7 -W 7 isindu
[root@localhost ~]# chage -l isindu
Last password change                                    : Oct 05, 2025
Password expires                                        : Jan 03, 2026
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 7
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
[root@localhost ~]#
```

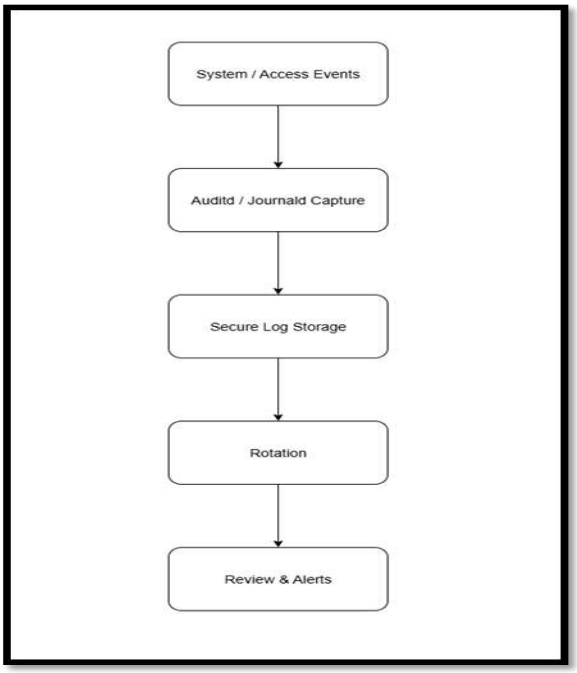
```
[root@localhost ~]# authselect create-profile hardening -b sssd
New profile was created at /etc/authselect/custom/hardening
[root@localhost ~]# for f in /etc/authselect/custom/hardening/system-auth /etc/authselect/custom/hardeni
ng/password-auth; do
>   sed -i '/^password.*pam_pwquality\.so/a password    requisite     pam_pwhistory.so use_authtok remem
ber=5' "$f"
> done && grep -n 'pam_pwhistory.so' /etc/authselect/custom/hardening/system-auth /etc/authselect/custom
/hardening/password-auth
/etc/authselect/custom/hardening/system-auth:32:password    requisite     pam_pwhistory.so use_authtok r
emember=5
/etc/authselect/custom/hardening/system-auth:34:password    requisite
 pam_pwhistory.so use_authtok                          {include if "with-pwhistory"}
/etc/authselect/custom/hardening/password-auth:25:password    requisite     pam_pwhistory.so use_authtok
 remember=5
/etc/authselect/custom/hardening/password-auth:27:password    requisite
   pam_pwhistory.so use_authtok                          {include if "with-pwhistory"}
```

d. Password history [prevent reuse]

```
[root@localhost ~]# authselect select custom/hardening with-faillock && authselect apply-changes
Profile "custom/hardening" was selected.
The following nsswitch maps are overwritten by the profile:
- passwd
- group
- netgroup
- automount
- services

Make sure that SSSD service is configured and enabled. See SSSD documentation for more information.

Changes were successfully applied.
[root@localhost ~]# grep -n 'pam_pwhistory\.so' /etc/pam.d/system-auth /etc/pam.d/password-auth
/etc/pam.d/system-auth:23:password    requisite     pam_pwhistory.so use_authtok remember=5
/etc/pam.d/password-auth:23:password    requisite     pam_pwhistory.so use_authtok remember=5
[root@localhost ~]# grep -n 'pam_pwquality\.so' /etc/pam.d/system-auth /etc/pam.d/password-auth
/etc/pam.d/system-auth:22:password    requisite                                     pam_pwquality.so loca
l_users_only
/etc/pam.d/password-auth:22:password    requisite                                     pam_pwquality.so lo
cal_users_only
[root@localhost ~]#
```

7.Enable Auditing and Logging

- System logs and audit instruments document all significant events or attempts to gain access, even those performed unlawfully.
- As a result of continuous monitoring, abnormal activities can be detected and reacted to at an early stage.
- Thanks to monitoring the system can prevent: Deeply concealed breaches Access without authorization Harmful activities of the already trusted by the system insiders



a. Enabling core logging services

```
File  Edit  View  Search  Terminal  Help
[root@localhost ~]# dnf install -y audit rsyslog
Last metadata expiration check: 2:08:06 ago on Sun 05 Oct 2025 06:57:54 AM EDT.
Package audit-3.1.2-1.el8_10.1.x86_64 is already installed.
Package rsyslog-8.2102.0-15.0.1.el8_10.1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost ~]# systemctl enable --now auditd
[root@localhost ~]# systemctl enable --now rsyslog
[root@localhost ~]# systemctl status auditd --no-pager
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-10-05 04:11:13 EDT; 4h 47min ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
 Main PID: 825 (auditd)
    Tasks: 4 (limit: 10362)
   Memory: 2.0M
   CGroup: /system.slice/auditd.service
           ├─825 /sbin/auditd
           └─827 /usr/sbin/sedispatch

Oct 05 04:11:13 localhost.localdomain augenrules[849]: enabled 1
Oct 05 04:11:13 localhost.localdomain augenrules[849]: failure 1
Oct 05 04:11:13 localhost.localdomain augenrules[849]: pid 825
Oct 05 04:11:13 localhost.localdomain augenrules[849]: rate_limit 0
Oct 05 04:11:13 localhost.localdomain augenrules[849]: backlog_limit 8192
Oct 05 04:11:13 localhost.localdomain augenrules[849]: lost 0
Oct 05 04:11:13 localhost.localdomain augenrules[849]: backlog 4
Oct 05 04:11:13 localhost.localdomain augenrules[849]: backlog_wait_time 60000
Oct 05 04:11:13 localhost.localdomain augenrules[849]: backlog_wait_time_actual 0
Oct 05 04:11:13 localhost.localdomain systemd[1]: Started Security Auditing Service.
[root@localhost ~]# systemctl status rsyslog --no-pager
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-10-05 04:11:19 EDT; 4h 47min ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 1225 (rsyslogd)
    Tasks: 3 (limit: 10362)
   Memory: 1.6M
   CGroup: /system.slice/rsyslog.service
           └─1225 /usr/sbin/rsyslogd -n

Oct 05 04:11:18 localhost.localdomain systemd[1]: Starting System Logging Service...
Oct 05 04:11:19 localhost.localdomain systemd[1]: Started System Logging Service.
Oct 05 04:11:19 localhost.localdomain rsyslogd[1225]: [origin software="rsyslogd" swVersion="8.2102-start
```

b. Make journal persistent (so logs survive reboots) and set sane limits

```
[root@localhost ~]# sed -i -E \
>   -e 's/^#?Storage=.*/Storage=persistent/' \
>   -e 's/^#?SystemMaxUse=.*/SystemMaxUse=200M/' \
>   -e 's/^#?RateLimitIntervalSec=.*/RateLimitIntervalSec=30s/' \
>   -e 's/^#?RateLimitBurst=.*/RateLimitBurst=1000/' \
>   /etc/systemd/journald.conf
[root@localhost ~]# systemctl restart systemd-journald
[root@localhost ~]# grep -E '^(Storage|SystemMaxUse|RateLimitIntervalSec|RateLimitBurst)=' /etc/systemd/
journald.conf
Storage=persistent
RateLimitIntervalSec=30s
RateLimitBurst=1000
SystemMaxUse=200M
[root@localhost ~]#
```

c. Add focused audit rules (watched files & key actions)

```
[root@localhost ~]# cat >/etc/audit/rules.d/10-hardening.rules <<'EOF'
> --loginuid-immutable
> -w /etc/passwd    -p wa -k account_changes
> -w /etc/shadow    -p wa -k account_changes
> -w /etc/group     -p wa -k account_changes
> -w /etc/sudoers   -p wa -k sudo_changes
> -w /etc/ssh/sshd_config -p wa -k ssh_config
> -w /etc/firewalld -p wa -k firewall_changes

> -w /usr/bin/sudo -p x  -k sudo_actions
> -w /etc/systemd/system -p wa -k service_changes
> -w /opt/oracle -p wa -k oracle_config
> EOF
[root@localhost ~]# augenrules --load
No rules
enabled 1
failure 1
pid 825
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 825
rate_limit 0
backlog_limit 8192
lost 0
backlog 4
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 825
rate_limit 0
backlog_limit 8192
lost 0
backlog 26
backlog_wait_time 60000
backlog_wait_time_actual 0
[root@localhost ~]# auditctl -l
-w /etc/passwd -p wa -k account_changes
```

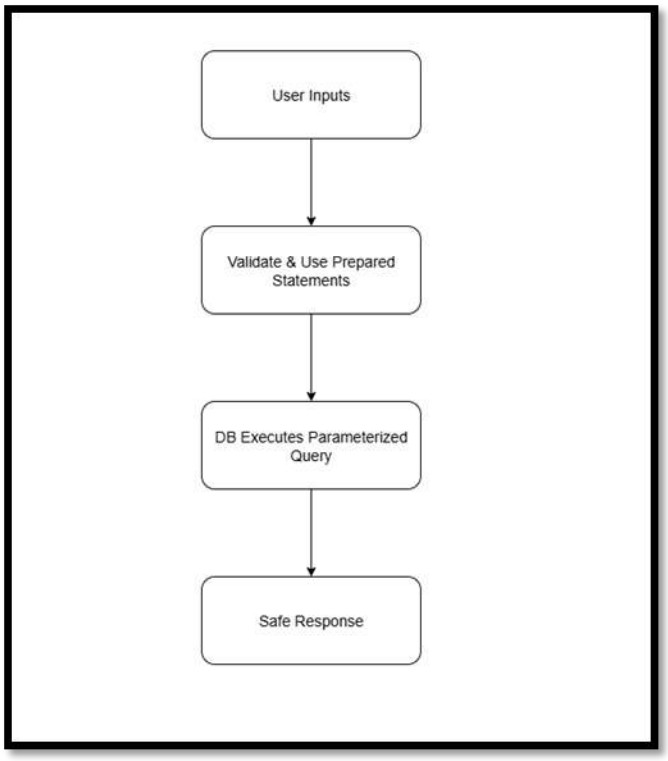
```
backlog_wait_time_actual 0
[root@localhost ~]# auditctl -l
-w /etc/passwd -p wa -k account_changes
-w /etc/shadow -p wa -k account_changes
-w /etc/group -p wa -k account_changes
-w /etc/sudoers -p wa -k sudo_changes
-w /etc/ssh/sshd_config -p wa -k ssh_config
-w /etc/firewalld -p wa -k firewall_changes
-w /usr/bin/sudo -p x -k sudo_actions
-w /etc/systemd/system -p wa -k service_changes
-w /opt/oracle -p wa -k oracle_config
[root@localhost ~]#
```

d. Basic log rotation check (keeps logs from growing unbounded)

```
[root@localhost ~]# ls -1 /etc/logrotate.d | sed -n '1,120p'
bootlog
btmp
chrony
cups
dnf
firewalld
iscsiuiolog
kvm_stat
libvirtd
libvirtd.qemu
numad
psacct
samba
sssd
syslog
up2date
wpa_supplicant
wtmp
[root@localhost ~]# cat /etc/logrotate.conf | sed -n '1,120p'
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
[root@localhost ~]#
```

8.Protect Database from SQL Injection

- Techniques to prevent SQL injection are: Using parameterized queries Validating user inputs Encrypting sensitive data
- Helps stop: SQL injection attacks Unauthorized reading, altering or deletion of database data Compromise of database confidentiality and integrity.

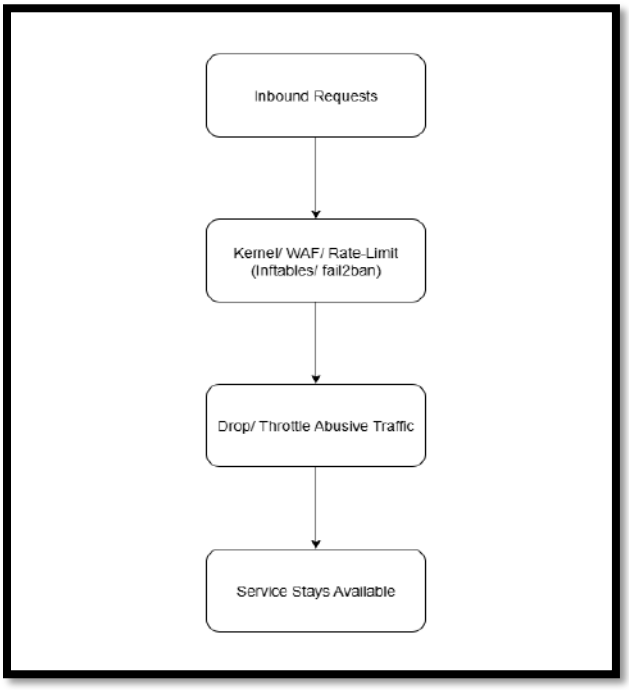



```
[root@localhost ~]# firewall-cmd --zone=public --list-rich-rules
rule family="ipv4" service name="ssh" accept limit value="5/m"
rule family="ipv4" source address="192.168.1.0/24" port port="1521" protocol="tcp" accept
rule family="ipv4" service name="ssh" drop
[root@localhost ~]#
```

```
[root@localhost ~]# mkdir -p /etc/tns_admin
[root@localhost ~]# cat >/etc/tns_admin/sqlnet.ora <<'EOF'
> TCP.VALIDNODE_CHECKING = YES
> TCP.INVITED_NODES = (192.168.1.10,192.168.1.11)  #app host loc
> EOF
[root@localhost ~]# cat /etc/tns_admin/sqlnet.ora
TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODES = (192.168.1.10,192.168.1.11)  #app host loc
[root@localhost ~]#
```

9.Mitigating DoS Attacks

- Rate-limiting tools such as Fail2ban, nftables, and WAFs manage traffic via: Allowing or blocking requests that go beyond a predefined threshold
- Thus, the attackers who bombard the server with too many requests are stopped.
- Helped the system to Avoid: Brute-force attacks Denial-of-Service (DoS) attacks.



a. Add safe kernel/network DoS hardening (sysctl)

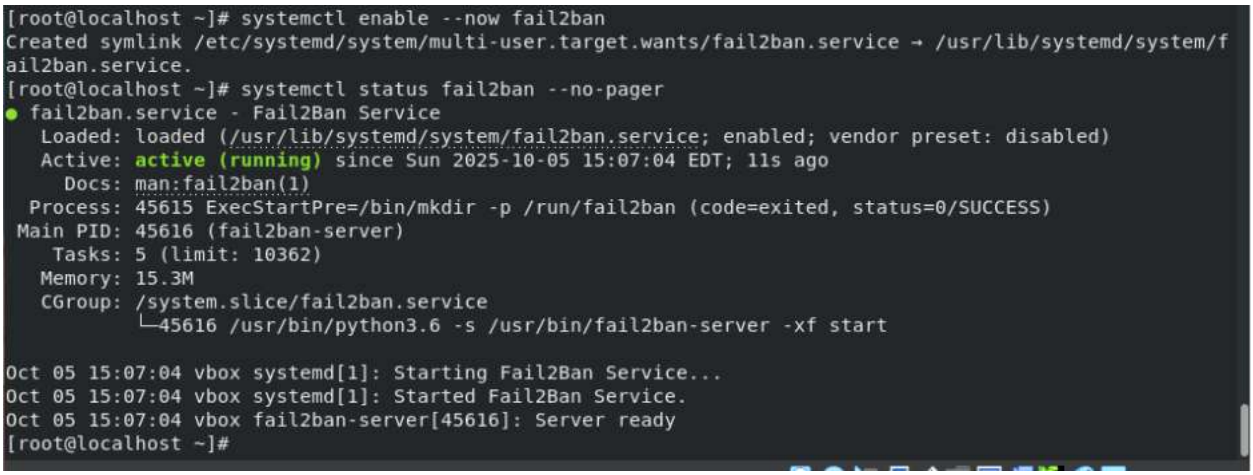
```
> net.ipv4.icmp_ignore_bogus_error_responses = 1
>
> # Queue sizes
> net.core.somaxconn = 1024
> net.core.netdev_max_backlog = 5000
> EOF
[root@localhost ~]# sysctl --system | sed -n '1,200p'
* Applying /usr/lib/sysctl.d/01-unprivileged-bpf.conf ...
kernel.unprivileged_bpf_disabled = 1
* Applying /usr/lib/sysctl.d/10-default-yama-scope.conf ...
kernel.yama.ptrace_scope = 0
* Applying /usr/lib/sysctl.d/50-coredump.conf ...
kernel.core_pattern = |/usr/lib/systemd/systemd-coredump %P %u %g %s %t %c %h %e %d
kernel.core_pipe_limit = 16
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.sysrq = 16
kernel.core_uses_pid = 1
kernel.kptr_restrict = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.promote_secondaries = 1
net.core.default_qdisc = fq_codel
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /usr/lib/sysctl.d/50-libkcapi-optmem_max.conf ...
net.core.optmem_max = 81920
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
kernel.pid_max = 4194304
* Applying /usr/lib/sysctl.d/60-libvirtd.conf ...
fs.aio-max-nr = 1048576
* Applying /usr/lib/sysctl.d/60-qemu-postcopy-migration.conf ...
* Applying /etc/sysctl.d/99-dos-hardening.conf ...
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 8192
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_rfc1337 = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.core.somaxconn = 1024
net.core.netdev_max_backlog = 5000
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.conf ...
[root@localhost ~]#
```

b. Rate-limit Oracle listener (1521) at the firewall

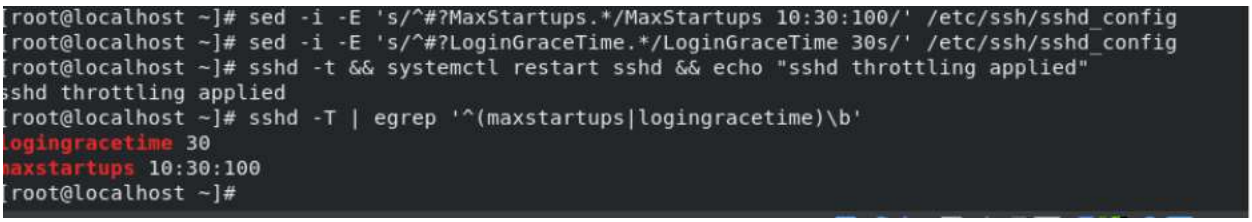
```
[root@localhost ~]# firewall-cmd --permanent --zone=public \
>   --add-rich-rule='rule family=ipv4 port protocol="tcp" port="1521" limit value="60/m" accept'
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" service name="ssh" accept limit value="5/m"
        rule family="ipv4" port port="1521" protocol="tcp" accept limit value="60/m"
        rule family="ipv4" source address="192.168.1.0/24" port port="1521" protocol="tcp" accept
        rule family="ipv4" service name="ssh" drop
[root@localhost ~]#
```

c. Install + enable Fail2ban for SSH

Why ?: Bans IPs that brute-force SSH based on log entries.

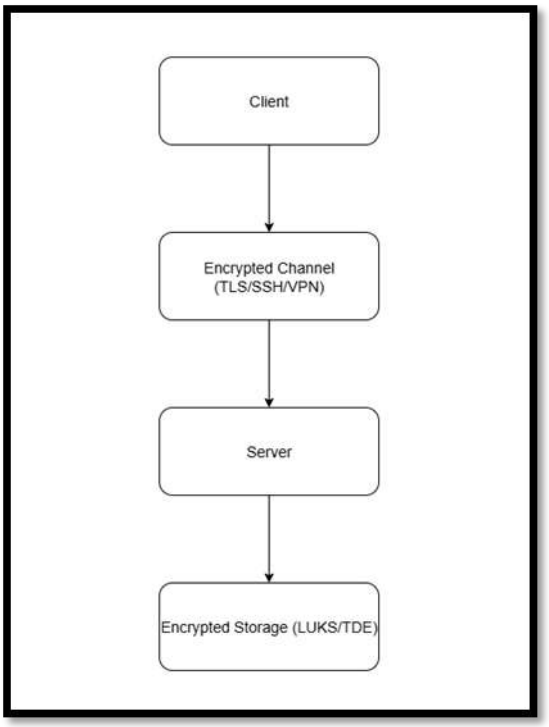


d. Throttle SSH daemon



10.Encryption of Data and Communications

- Encrypting network traffic with the use of protocols such as SSH, VPN or TLS.
- Protecting data at rest mainly by using solutions such as LUKS and TDE.
- Contributes to data confidentiality and integrity in cases of interception or theft of data.
- Offers security from: Data breaches Sniffing Man-in-the-middle attacks.



a. Encrypt data in transit

```
[root@localhost ~]# mkdir -p /etc/tns_admin
[root@localhost ~]# cat >/etc/tns_admin/sqlnet.ora <<'EOF'
> # Require encryption & crypto checksums on server side
> SQLNET.ENCRYPTION_SERVER = required
> SQLNET.CRYPTO_CHECKSUM_SERVER = required
>
> # Strong algorithms (clients will negotiate these)
> SQLNET.ENCRYPTION_TYPES_SERVER = (AES256,AES192)
> SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256,SHA1)
> EOF
[root@localhost ~]# cp /etc/tns_admin/sqlnet.ora /etc/tns_admin/sqlnet.client.template
[root@localhost ~]#
```

b. Encrypt data **at rest**

i. Encrypted backup “vault” with LUKS

```
[root@localhost ~]# cryptsetup luksFormat /secure/db_backups.img

WARNING!
========
This will overwrite data on /secure/db_backups.img irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /secure/db_backups.img:
Verify passphrase:


[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# cryptsetup open /secure/db_backups.img dbvault
Enter passphrase for /secure/db_backups.img:

[root@localhost ~]#
[root@localhost ~]# mkfs.ext4 /dev/mapper/dbvault
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 1306624 4k blocks and 327040 inodes
Filesystem UUID: 42509fcf-e2a5-4c80-aa34-b58d68111a79
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

[root@localhost ~]# mkdir -p /secure/db_backups
[root@localhost ~]# mount /dev/mapper/dbvault /secure/db_backups
[root@localhost ~]# df -h /secure/db_backups
Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/dbvault  4.9G   24K  4.6G   1% /secure/db_backups
[root@localhost ~]#
```

Task 02

01.Implement 5 Configurations to Harden Oracle DBMS

1.Enforce Strong Auth & Lockout

```
SQL> CREATE PROFILE C##STRONG_PROFILE LIMIT
  2  PASSWORD_VERIFY_FUNCTION ORA12C_STRONG_VERIFY_FUNCTION
  3  PASSWORD_LIFE_TIME 90
  4  PASSWORD_GRACE_TIME  7
  5  FAILED_LOGIN_ATTEMPTS 5
  6  PASSWORD_LOCK_TIME
  7  1/24
  8  SESSIONS_PER_USER 3
  9  CONTAINER=ALL;

Profile created.

SQL> SELECT con_id, profile, resource_name, limit
  2  FROM   cdb_profiles
  3  WHERE  profile = 'C##STRONG_PROFILE'
  4  ORDER  BY con_id, resource_name;

    CON_ID
----------
PROFILE
--------------------------------------------------------------------------------
RESOURCE_NAME
--------------------------------
LIMIT
--------------------------------------------------------------------------------
         1
C##STRONG_PROFILE
COMPOSITE_LIMIT
DEFAULT


    CON_ID
----------
PROFILE
--------------------------------------------------------------------------------
RESOURCE_NAME
--------------------------------
LIMIT
--------------------------------------------------------------------------------
         1
C##STRONG_PROFILE
CONNECT_TIME
DEFAULT
```

→ **Running 5 bad logins to confirm the lockout**

```
[oracle@vbox ~]$ for i in {1..5}; do echo "Attempt $i"; sqlplus "app1/Wrong#Pass@FREEPDB1" <<< "" || tru
e; echo; done
Attempt 1

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Oct 7 03:44:42 2025
Version 23.9.0.25.07

Copyright (c) 1982, 2025, Oracle.  All rights reserved.

ERROR:
ORA-01017: invalid credential or not authorized; logon denied
Help: https://docs.oracle.com/error-help/db/ora-01017/


Enter user-name: ERROR:
ORA-01017: invalid credential or not authorized; logon denied
Help: https://docs.oracle.com/error-help/db/ora-01017/


Enter user-name:
Attempt 2

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Oct 7 03:44:44 2025
Version 23.9.0.25.07

Copyright (c) 1982, 2025, Oracle.  All rights reserved.

ERROR:
ORA-01017: invalid credential or not authorized; logon denied
Help: https://docs.oracle.com/error-help/db/ora-01017/


Enter user-name: ERROR:
ORA-01017: invalid credential or not authorized; logon denied
Help: https://docs.oracle.com/error-help/db/ora-01017/


Enter user-name:
Attempt 3

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Oct 7 03:44:45 2025
Version 23.9.0.25.07
```

```
[oracle@vbox ~]$ sqlplus / as sysdba

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Oct 7 03:47:59 2025
Version 23.9.0.25.07

Copyright (c) 1982, 2025, Oracle.  All rights reserved.


Connected to:
Oracle Database 23ai Free Release 23.0.0.0.0 - Develop, Learn, and Run for Free
Version 23.9.0.25.07

SQL> alter session set container=FREEPDB1;

Session altered.

SQL> select username, account_status, lock_date, expiry_date, profile
  2  from   dba_users
  3  where  username='APP1';

USERNAME
--------------------------------------------------------------------------------
ACCOUNT_STATUS                   LOCK_DATE EXPIRY_DA
-------------------------------- --------- ---------
PROFILE
--------------------------------------------------------------------------------
APP1
LOCKED(TIMED)                    07-OCT-25 05-JAN-26
C##STRONG_PROFILE


SQL>
```

→ **Testing Strong Password Rule**

```
SQL> alter user app1 identified by "password";
alter user app1 identified by "password"
*
ERROR at line 1:
ORA-28003: The password chosen did not meet the required complexity rules set
by your organization.
ORA-20000: password length less than 9 characters
Help: https://docs.oracle.com/error-help/db/ora-28003/


SQL> alter user app1 identified by "ApP1!2025-long#Pwd";

User altered.
```

```
[oracle@vbox ~]$ sqlplus 'app1/ApP1!2025-long#Pwd@FREEPDB1'

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Oct 7 03:56:45 2025
Version 23.9.0.25.07

Copyright (c) 1982, 2025, Oracle.  All rights reserved.

Last Successful login time: Tue Oct 07 2025 02:40:36 -04:00

Connected to:
Oracle Database 23ai Free Release 23.0.0.0.0 - Develop, Learn, and Run for Free
Version 23.9.0.25.07

SQL>
```

2.Least Privilege + Outbound Network Whitelisting

→ **Deny by Default(before ACL)**

```
SQL> conn app1/"ApP1!2025-long#Pwd"@FREEPDB1
Connected.
SQL> set serveroutput on
SQL> declare
  2  req  utl_http.req;
  3  resp utl_http.resp;
  4  line varchar2(200);
  5  begin
  6  req  := utl_http.begin_request('http://127.0.0.1:80/');
  7  resp := utl_http.get_response(req);
  8  utl_http.read_line(resp, line, true);
  9  dbms_output.put_line(line);
 10   utl_http.end_response(resp);
 11  end;
 12  /
declare
*
ERROR at line 1:
ORA-29273: HTTP request failed
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at "SYS.UTL_HTTP", line 380
ORA-06512: at "SYS.UTL_HTTP", line 1189
ORA-06512: at line 6
Help: https://docs.oracle.com/error-help/db/ora-29273/
```

→ **Creating and Assigning ACL**

```
SQL> Begin
  2  DBMS_NETWORK_ACL_ADMIN.CREATE_ACL(
  3  acl         => 'app1_acl.xml',
  4  description => 'Outbound allowlist for APP1',
  5  principal   => 'APP1',
  6  is_grant    => TRUE,
  7  privilege   => 'connect'
  8  );
  9
 10  DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL(
 11  acl  => 'app1_acl.xml',
 12  host => '127.0.0.1'
 13  );
 14  END;
 15  /

PL/SQL procedure successfully completed.

SQL> SELECT host, lower_port, upper_port, acl FROM dba_network_acls ORDER BY host;

HOST
--------------------------------------------------------------------------------
LOWER_PORT UPPER_PORT
---------- ----------
ACL
--------------------------------------------------------------------------------
*

NETWORK_ACL_3AB400E76C8A13EEE063C6845E646CD0

127.0.0.1

/sys/acls/app1_acl.xml

HOST
--------------------------------------------------------------------------------
LOWER_PORT UPPER_PORT
---------- ----------
ACL
--------------------------------------------------------------------------------
```

→ **ACL Privilege Entry**

```
SQL> SELECT acl, principal, privilege, is_grant, start_date, end_date
  2  FROM   dba_network_acl_privileges
  3  ORDER  BY principal, acl;

ACL
--------------------------------------------------------------------------------
PRINCIPAL
--------------------------------------------------------------------------------
PRIVILEGE
--------------------------------------------------------------------------------
IS_GR
-----
START_DATE
---------------------------------------------------------------------------
END_DATE
---------------------------------------------------------------------------
/sys/acls/app1_acl.xml

ACL
--------------------------------------------------------------------------------
PRINCIPAL
--------------------------------------------------------------------------------
PRIVILEGE
--------------------------------------------------------------------------------
IS_GR
-----
START_DATE
---------------------------------------------------------------------------
END_DATE
---------------------------------------------------------------------------
APP1

ACL
--------------------------------------------------------------------------------
PRINCIPAL
--------------------------------------------------------------------------------
PRIVILEGE
--------------------------------------------------------------------------------
IS_GR
-----
START_DATE
---------------------------------------------------------------------------
END_DATE
---------------------------------------------------------------------------
connect
```

After ACL Creation — Outbound to 127.0.0.1 Allowed; HTTP/80 Fails (Connection Refused, no ORA-24247)

```
SQL> conn app1/"ApP1!2025-long#Pwd"@FREEPDB1
Connected.
SQL> set serveroutput on
SQL> declare
  2  req  utl_http.req;
  3
  4  resp utl_http.resp;
  5  line varchar2(200);
  6  begin
  7  req  := utl_http.begin_request('http://127.0.0.1:80/');
  8  resp := utl_http.get_response(req);
  9  utl_http.read_line(resp, line, true);
 10  dbms_output.put_line(line);
 11  utl_http.end_response(resp);
 12  end;
 13  /
declare
*
ERROR at line 1:
ORA-29273: HTTP request failed
ORA-30698: network connection failed: connection refused
ORA-06512: at "SYS.UTL_HTTP", line 380
ORA-06512: at "SYS.UTL_HTTP", line 1189
ORA-06512: at line 7
Help: https://docs.oracle.com/error-help/db/ora-29273/
```

→ **Restrict ACL to Port 1521**

```
SQL> SELECT host, lower_port, upper_port, acl
  2  FROM   dba_network_acls
  3  ORDER  BY host, lower_port;

HOST
--------------------------------------------------------------------------------
LOWER_PORT UPPER_PORT
---------- ----------
ACL
--------------------------------------------------------------------------------
*

NETWORK_ACL_3AB400E76C8A13EEE063C6845E646CD0

127.0.0.1
      1521       1521
/sys/acls/app1_acl.xml

HOST
--------------------------------------------------------------------------------
LOWER_PORT UPPER_PORT
---------- ----------
ACL
--------------------------------------------------------------------------------
```

→ **Testing Allowed Path**

```
SQL> set serveroutput on
SQL> declare
  2  c utl_tcp.connection;
  3  begin
  4  c := utl_tcp.open_connection(remote_host => '127.0.0.1', remote_port => 1521, tx_timeout => 2);
  5  utl_tcp.close_connection(c);
  6  dbms_output.put_line('TCP OK to 127.0.0.1:1521');
  7  end;
  8  /
TCP OK to 127.0.0.1:1521

PL/SQL procedure successfully completed.
```

→ **Post-Restriction Negative Test**

```
SQL> set serveroutput on
SQL> declare
  2  req  utl_http.req;
  3  resp utl_http.resp;
  4  begin
  5  req  := utl_http.begin_request('http://127.0.0.1:80/');
  6  resp := utl_http.get_response(req);
  7  utl_http.end_response(resp);
  8  end;
  9  /
declare
*
ERROR at line 1:
ORA-29273: HTTP request failed
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at "SYS.UTL_HTTP", line 380
ORA-06512: at "SYS.UTL_HTTP", line 1189
ORA-06512: at line 5
Help: https://docs.oracle.com/error-help/db/ora-29273/
```

→ **Listener Service**

```
SQL> host lsnrctl status

LSNRCTL for Linux: Version 23.0.0.0.0 - Production on 07-OCT-2025 05:44:57

Copyright (c) 1991, 2025, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 23.0.0.0.0 - Production
Start Date                07-OCT-2025 03:37:15
Uptime                    0 days 2 hr. 7 min. 41 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Default Service           FREE
Listener Parameter File   /opt/oracle/product/23ai/dbhomeFree/network/admin/listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/vbox/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "408c1428db5418b1e065000000000001" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "FREE" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "FREEXDB" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "freepdb1" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
The command completed successfully
```

3.Turn on (and tighten) Unified Auditing

→ Enabling Unified Auditing(CDB$ROOT) – Baseline

```
SQL> AUDIT POLICY ORA_SECURECONFIG;

Audit succeeded.

SQL> AUDIT POLICY ORA_LOGON_FAILURES;

Audit succeeded.

SQL> AUDIT POLICY ORA_ACCOUNT_MGMT;

Audit succeeded.

SQL> SET LINES 200 PAGES 100
SQL> SELECT policy_name, entity_type, entity_name, success, failure
  2  FROM   audit_unified_enabled_policies
  3  ORDER  BY policy_name, entity_name;

POLICY_NAME                                                                                                      ENTITY_
---------------------------------------------------------------------------------------------------------------- -------
ENTITY_NAME                                                                                                      SUC FAI
---------------------------------------------------------------------------------------------------------------- --- ---
ORA$DICTIONARY_SENS_COL_ACCESS                                                                                   USER
ALL USERS                                                                                                        YES YES

ORA_ACCOUNT_MGMT                                                                                                 USER
ALL USERS                                                                                                        YES YES

ORA_DV_DEFAULT_PROTECTION                                                                                        USER
ALL USERS                                                                                                        YES YES

ORA_DV_SCHEMA_CHANGES                                                                                            USER
ALL USERS                                                                                                        YES YES

ORA_LOGIN_LOGOUT                                                                                                 USER
ALL USERS                                                                                                        NO  YES

ORA_LOGON_FAILURES                                                                                               USER
ALL USERS                                                                                                        YES YES

ORA_SECURECONFIG                                                                                                 USER
ALL USERS                                                                                                        YES YES


7 rows selected.
```

Unified Auditing: DDL_CHANGES Policy — CREATE/ALTER/DROP captured for APP1

```
SQL> conn / as sysdba
Connected.
SQL> alter session set container=FREEPDB1;

Session altered.

SQL> SET LINES 200 PAGES 100
SQL> SELECT to_char(event_timestamp,'YYYY-MM-DD HH24:MI:SS') AS ts,
  2  dbusername, action_name, object_schema, object_name, return_code
  3  FROM   unified_audit_trail
  4  WHERE dbusername = 'APP1'
  5  AND action_name IN ('CREATE TABLE','ALTER TABLE','DROP TABLE')
  6  AND object_name LIKE 'AUDIT_DEMO%'
  7  ORDER BY event_timestamp DESC
  8  FETCH FIRST 10 ROWS ONLY;

TS                  DBUSERNAME
------------------- ------------------------------------------------------------------------------------------------
----------------------------------------
ACTION_NAME                                                      OBJECT_SCHEMA
---------------------------------------------------------------- --------------------------------
--------------------------------------------------------------------------------
OBJECT_NAME
RETURN_CODE
------------------------------------------------------------------------------------------------------------------
---------------------- -----------
2025-10-07 06:06:27 APP1
DROP TABLE                                                       APP1
AUDIT_DEMO
  0

2025-10-07 06:06:14 APP1
ALTER TABLE                                                      APP1
AUDIT_DEMO
  0

2025-10-07 06:06:08 APP1
CREATE TABLE                                                     APP1
AUDIT_DEMO
  0


SQL>
```

→ **Unified Auditing – Failed Login (ORA-01017) Capture**

```
SQL> SELECT to_char(event_timestamp,'YYYY-MM-DD HH24:MI:SS') AS ts,
  2  dbusername, action_name, return_code, os_username, userhost
  3  FROM unified_audit_trail
  4  WHERE action_name IN ('LOGON','LOGOFF')
  5  AND return_code IN (1017)
  6  ORDER BY event_timestamp DESC
  7  FETCH FIRST 5 ROWS ONLY;

TS                  DBUSERNAME
------------------- ------------------------------------------------------------------------------------
----------------------------------------
ACTION_NAME                                                      RETURN_CODE
---------------------------------------------------------------- -----------
OS_USERNAME
------------------------------------------------------------------------------------------------------
------------------------
USERHOST
------------------------------------------------------------------------------------------------------
------------------------
2025-10-07 06:13:27 APP1
LOGON                                                                  1017
oracle
vbox
```

→ **Unified Auditing – ALTER USER events (ock/unlock/password) Event capture**

```
SQL> alter user app1 account unlock;

User altered.

SQL>
SQL> alter user app1 identified by "ApP1!2025-long#Pwd";

User altered.

SQL> set lines 200 pages 100
SQL> SELECT to_char(event_timestamp,'YYYY-MM-DD HH24:MI:SS') AS ts,
  2  dbusername, action_name, object_name, return_code
  3  FROM unified_audit_trail
  4  WHERE action_name IN ('ALTER USER')
  5  AND object_name = 'APP1'
  6  ORDER BY event_timestamp DESC
  7  FETCH FIRST 10 ROWS ONLY;

TS                  DBUSERNAME
------------------- ------------------------------------------------------------------------------------
----------------------------------------
ACTION_NAME                                                      OBJECT_NAME
---------------------------------------------------------------- ------------------------------------
--------------------------------------------------------------------------------
RETURN_CODE
-----------
2025-10-07 06:20:53 SYS
ALTER USER                                                       APP1
         0

2025-10-07 06:20:42 SYS
ALTER USER                                                       APP1
         0

2025-10-07 06:20:35 SYS
ALTER USER                                                       APP1
         0
```

4.Encrypt and Lockdown Network Traffic + Listener

→ Hardened Server SQL*Net Settings (AES256, SHA512, Valid Node Check

```
[oracle@vbox ~]$ echo "==> New sqlnet.ora:"
==> New sqlnet.ora:
[oracle@vbox ~]$ sed -n '1,200p' $ORACLE_HOME/network/admin/sqlnet.ora
SQLNET.ENCRYPTION_SERVER = REQUIRED
SQLNET.CRYPTO_CHECKSUM_SERVER = REQUIRED
SQLNET.ENCRYPTION_TYPES_SERVER = (AES256)
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA512)
SQLNET.ALLOW_WEAK_CRYPTO = FALSE

TCP.VALIDNODE_CHECKING = YES
TCP.INVITED_NODES = (127.0.0.1,10.0.2.15)
```

→ Listener Admin Restrictions Enabled

```
[oracle@vbox ~]$ printf "\n# Harden: disallow remote admin changes\nADMIN_RESTRICTIONS_LISTENER = ON\n"
| tee -a $ORACLE_HOME/network/admin/listener.ora

# Harden: disallow remote admin changes
ADMIN_RESTRICTIONS_LISTENER = ON
[oracle@vbox ~]$ echo "==> New listener.ora:"
==> New listener.ora:
[oracle@vbox ~]$ sed -n '1,200p' $ORACLE_HOME/network/admin/listener.ora
# listener.ora Network Configuration File: /opt/oracle/product/23ai/dbhomeFree/network/admin/listener.or
a
# Generated by Oracle configuration tools.

DEFAULT_SERVICE_LISTENER = FREE

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )


# Harden: disallow remote admin changes
ADMIN_RESTRICTIONS_LISTENER = ON
[oracle@vbox ~]$ lsnrctl stop
```

→ **Listener Restart & Status — LISTENER running on 127.0.0.1:1521 (No Services Registered Yet)**

```
[oracle@vbox ~]$ lsnrctl start

LSNRCTL for Linux: Version 23.0.0.0.0 - Production on 07-OCT-2025 07:13:10

Copyright (c) 1991, 2025, Oracle.  All rights reserved.

Starting /opt/oracle/product/23ai/dbhomeFree/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 23.0.0.0.0 - Production
System parameter file is /opt/oracle/product/23ai/dbhomeFree/network/admin/listener.ora
Log messages written to /opt/oracle/diag/tnslsnr/vbox/listener/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PORT=1521)))
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 23.0.0.0.0 - Production
Start Date                07-OCT-2025 07:13:10
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Default Service           FREE
Listener Parameter File   /opt/oracle/product/23ai/dbhomeFree/network/admin/listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/vbox/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
The listener supports no services
The command completed successfully
[oracle@vbox ~]$ lsnrctl status

LSNRCTL for Linux: Version 23.0.0.0.0 - Production on 07-OCT-2025 07:13:18

Copyright (c) 1991, 2025, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 23.0.0.0.0 - Production
Start Date                07-OCT-2025 07:13:10
Uptime                    0 days 0 hr. 0 min. 8 sec
Trace Level               off
```

→ **Listener Status — Services Registered (FREE / freepdb1 READY)**

```
SQL> host lsnrctl status;

LSNRCTL for Linux: Version 23.0.0.0.0 - Production on 07-OCT-2025 07:21:12

Copyright (c) 1991, 2025, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 23.0.0.0.0 - Production
Start Date                07-OCT-2025 07:13:10
Uptime                    0 days 0 hr. 8 min. 1 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Default Service           FREE
Listener Parameter File   /opt/oracle/product/23ai/dbhomeFree/network/admin/listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/vbox/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=127.0.0.1)(PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "408c1428db5418b1e065000000000001" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "FREE" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "FREEXDB" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
Service "freepdb1" has 1 instance(s).
  Instance "FREE", status READY, has 1 handler(s) for this service...
The command completed successfully
```

→ **SQL*Net Encryption & Integrity Negotiated — AES256 + SHA512 (Session Banner)**

```
SQL> SET LINES 200
SQL> SELECT network_service_banner
  2  FROM v$session_connect_info
  3  WHERE sid = (SELECT DISTINCT sid FROM v$mystat);

NETWORK_SERVICE_BANNER
----------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------
Oracle Bequeath NT Protocol Adapter for Linux: Version 23.0.0.0.0 - Production
Authentication service for Linux: Version 23.0.0.0.0 - Production
Encryption service for Linux: Version 23.0.0.0.0 - Production
AES256 Encryption service adapter for Linux: Version 23.0.0.0.0 - Production
Crypto-checksumming service for Linux: Version 23.0.0.0.0 - Production
SHA512 Crypto-checksumming service adapter for Linux: Version 23.0.0.0.0 - Production

6 rows selected.
```

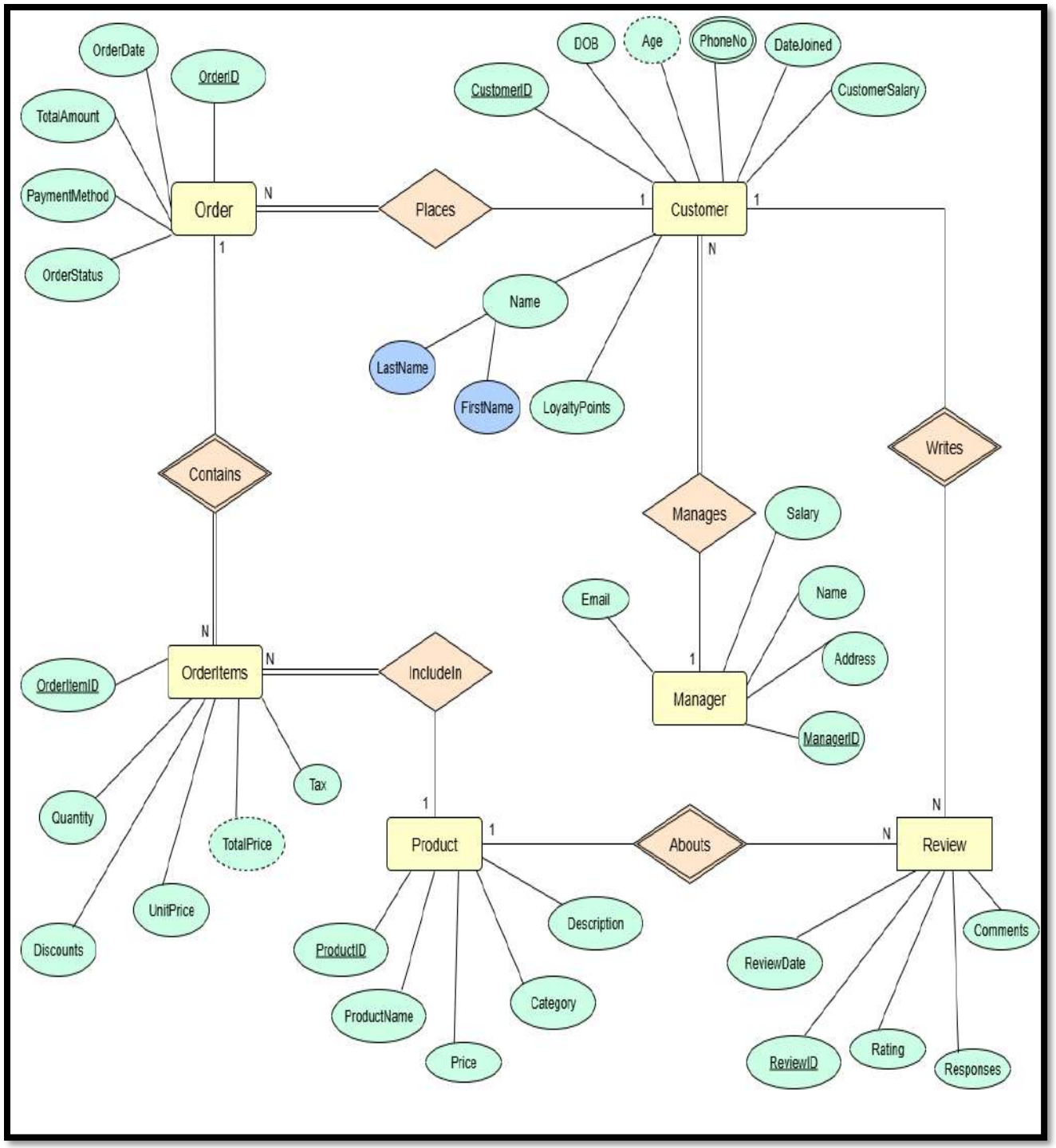
5.PDB Lockdown Profile (Cut Attack Surface)

```
SQL> ALTER LOCKDOWN PROFILE C##SAFER_PDB
  2   DISABLE FEATURE = ('NETWORK_ACCESS');

Lockdown Profile altered.

SQL> ALTER LOCKDOWN PROFILE C##SAFER_PDB
  2
SQL>
SQL> ALTER LOCKDOWN PROFILE C##SAFER_PDB
  2  DISABLE STATEMENT = ('CREATE DIRECTORY');

Lockdown Profile altered.

SQL> ALTER LOCKDOWN PROFILE C##SAFER_PDB
  2  DISABLE STATEMENT = ('CREATE LIBRARY');

Lockdown Profile altered.

SQL> SHOW PDBS;

    CON_ID CON_NAME                       OPEN MODE  RESTRICTED
---------- ------------------------------ ---------- ----------
         2 PDB$SEED                       READ ONLY  NO
         3 FREEPDB1                       READ WRITE NO
```

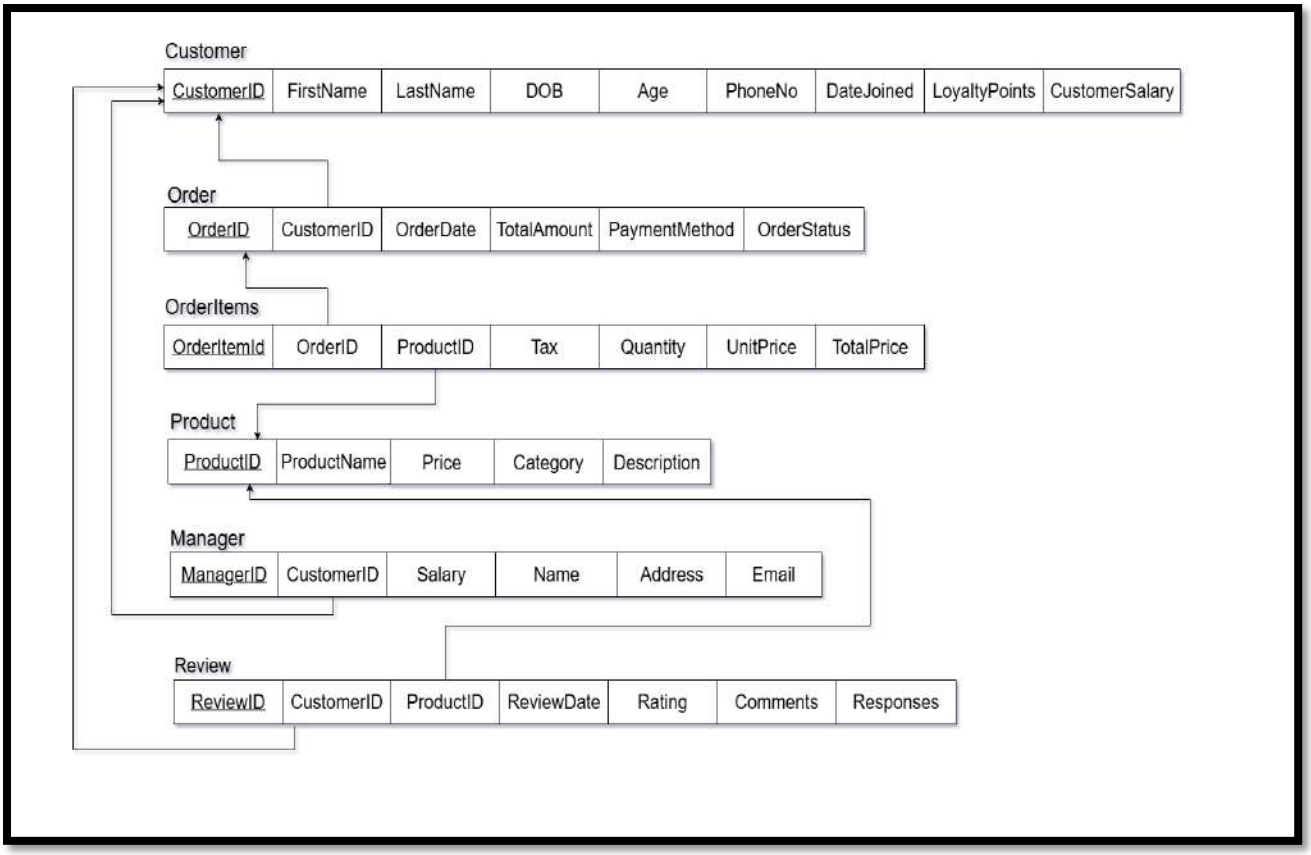
```
SQL> ALTER SESSION SET CONTAINER = FREEPDB1;

Session altered.

SQL> CREATE DIRECTORY T_DEMO AS '/tmp';
CREATE DIRECTORY T_DEMO AS '/tmp'
*
ERROR at line 1:
ORA-01031: insufficient privileges
Help: https://docs.oracle.com/error-help/db/ora-01031/
```

```
SQL>
SQL> CREATE DATABASE LINK d_test CONNECT TO scott IDENTIFIED BY tiger USING 'loopback';
CREATE DATABASE LINK d_test CONNECT TO scott IDENTIFIED BY tiger USING 'loopback'
                      *
ERROR at line 1:
ORA-02011: duplicate database link name
Help: https://docs.oracle.com/error-help/db/ora-02011/


SQL> DECLARE
  2  resp CLOB;
  3  BEGIN
  4  resp := UTL_HTTP.REQUEST('http://example.com');
  5  DBMS_OUTPUT.PUT_LINE(DBMS_LOB.SUBSTR(resp, 100, 1));
  6  END;
  7  /
DECLARE
*
ERROR at line 1:
ORA-29273: HTTP request failed
ORA-06512: at "SYS.UTL_HTTP", line 1594
ORA-12545: Connect failed because target host or object does not exist
ORA-06512: at "SYS.UTL_HTTP", line 380
ORA-06512: at "SYS.UTL_HTTP", line 1534
ORA-06512: at line 4
Help: https://docs.oracle.com/error-help/db/ora-29273/
```

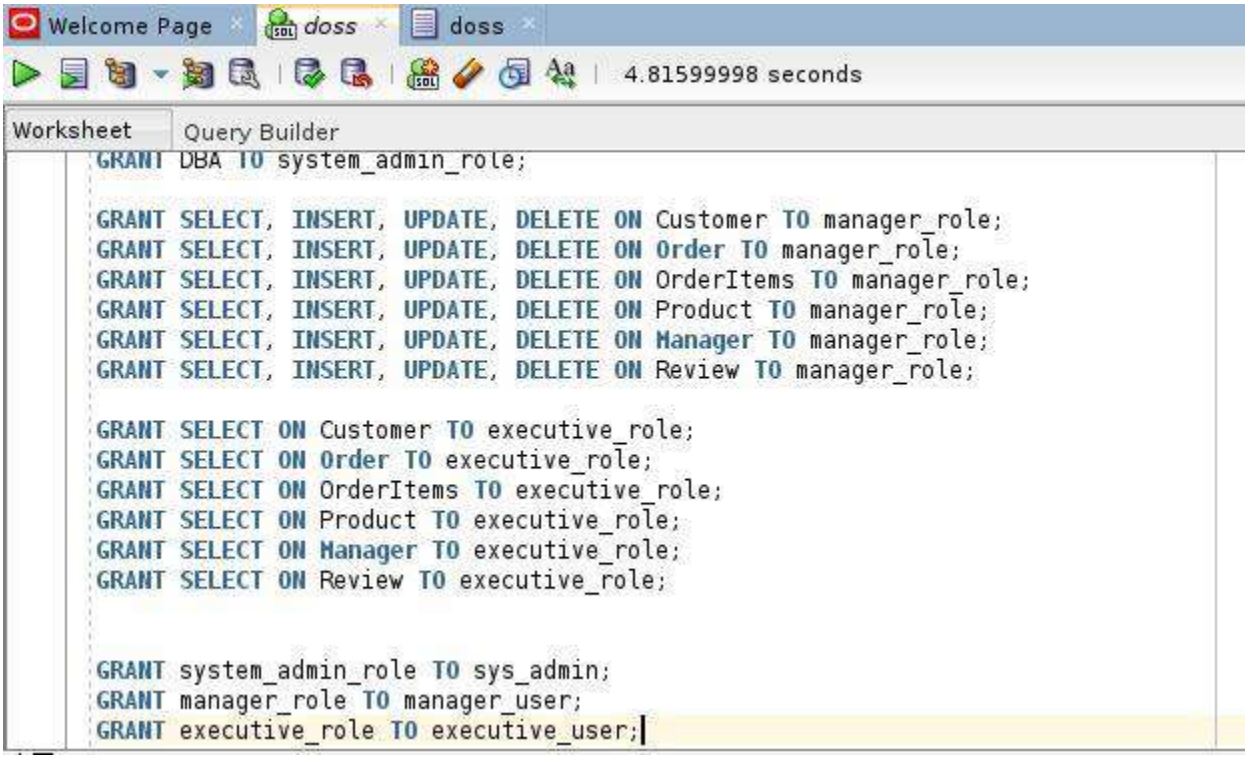
02.ER Diagram



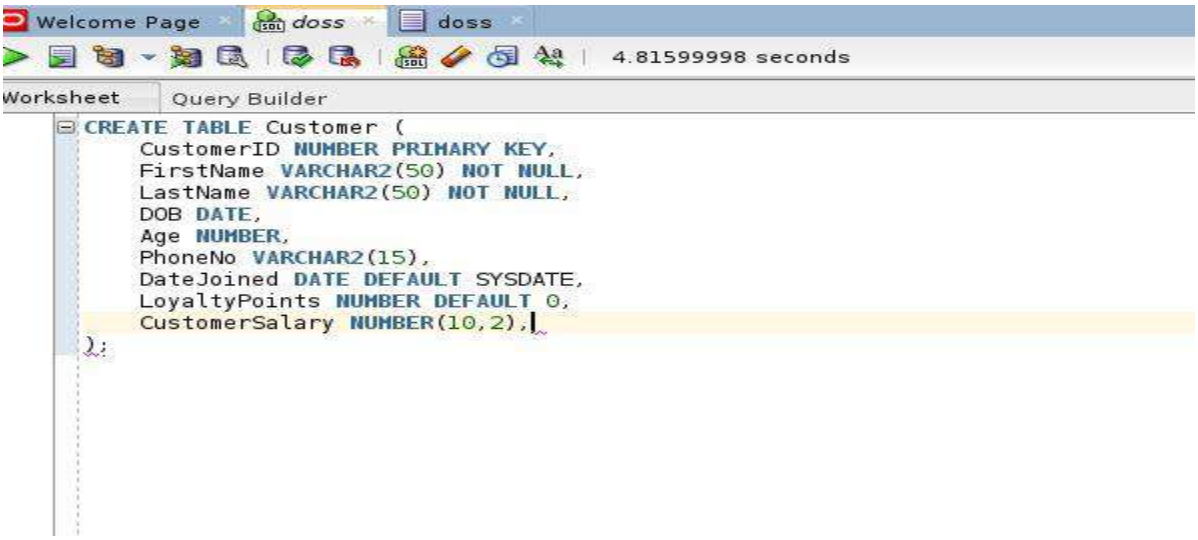
03.Relational Schema

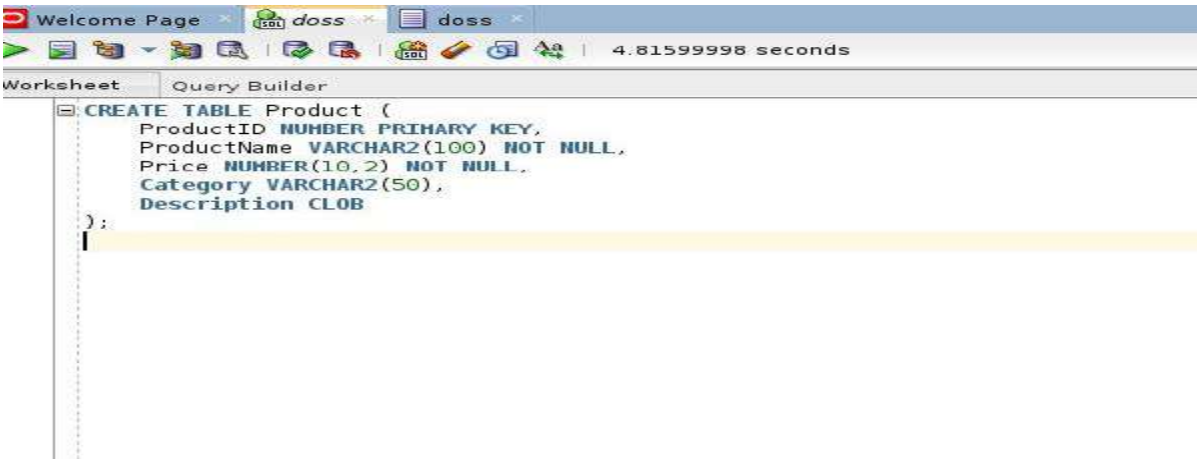


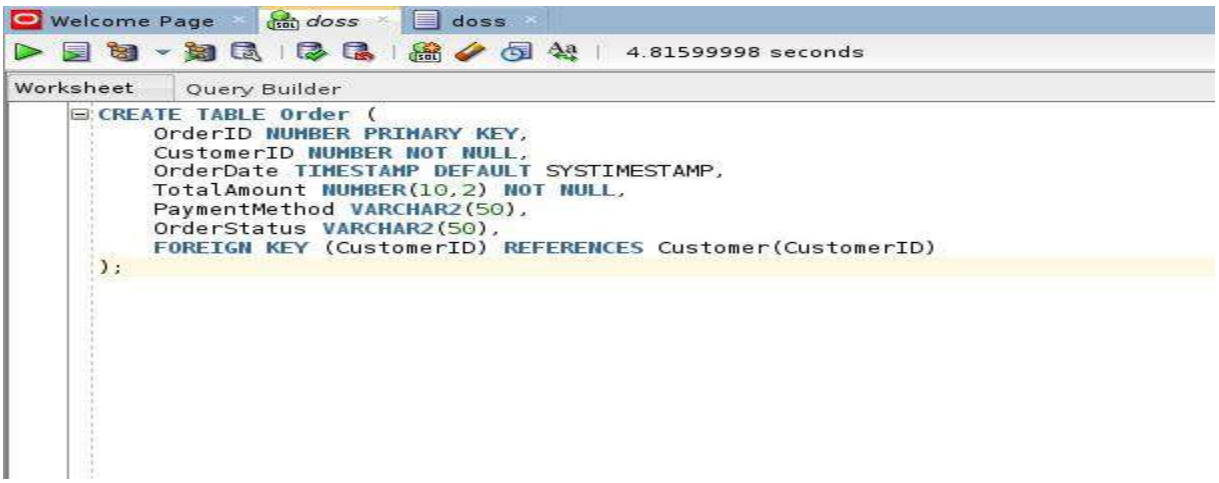
04. Create Roles and Grant Permissions

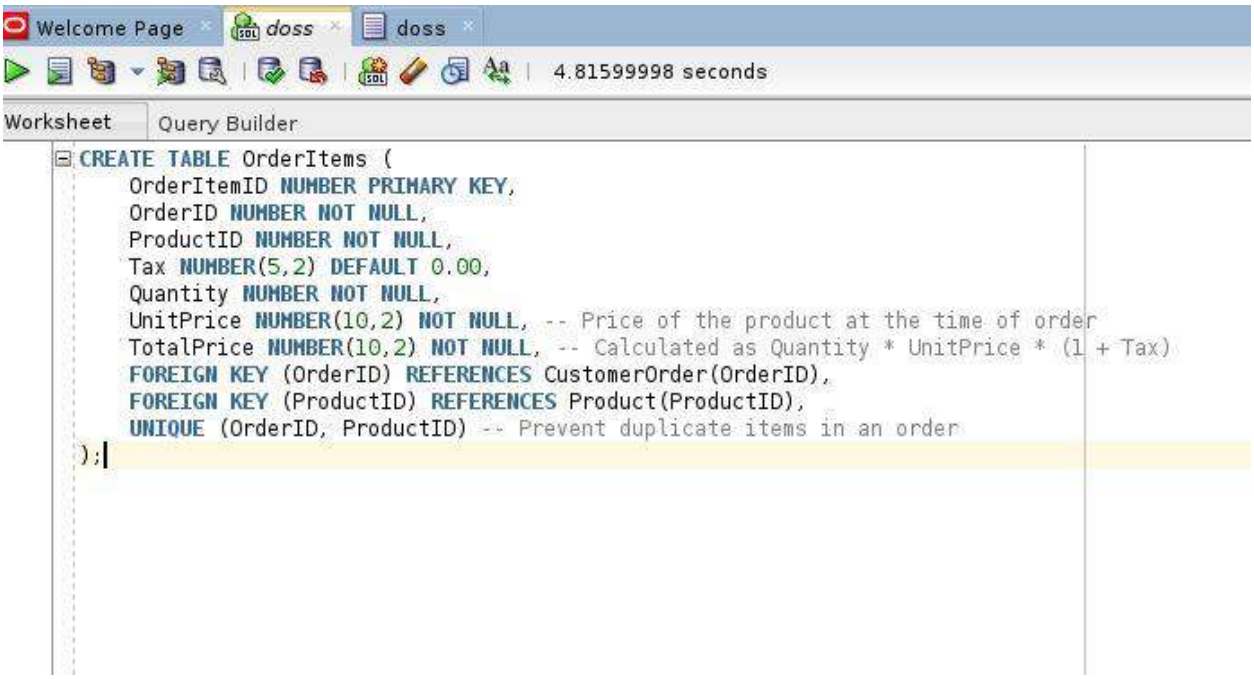


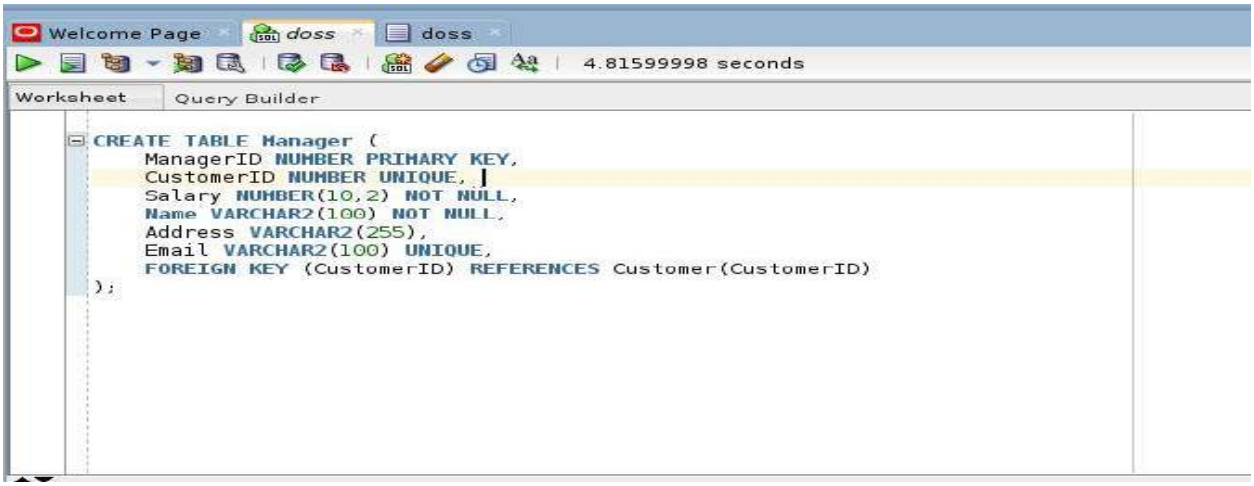
05. Create Table

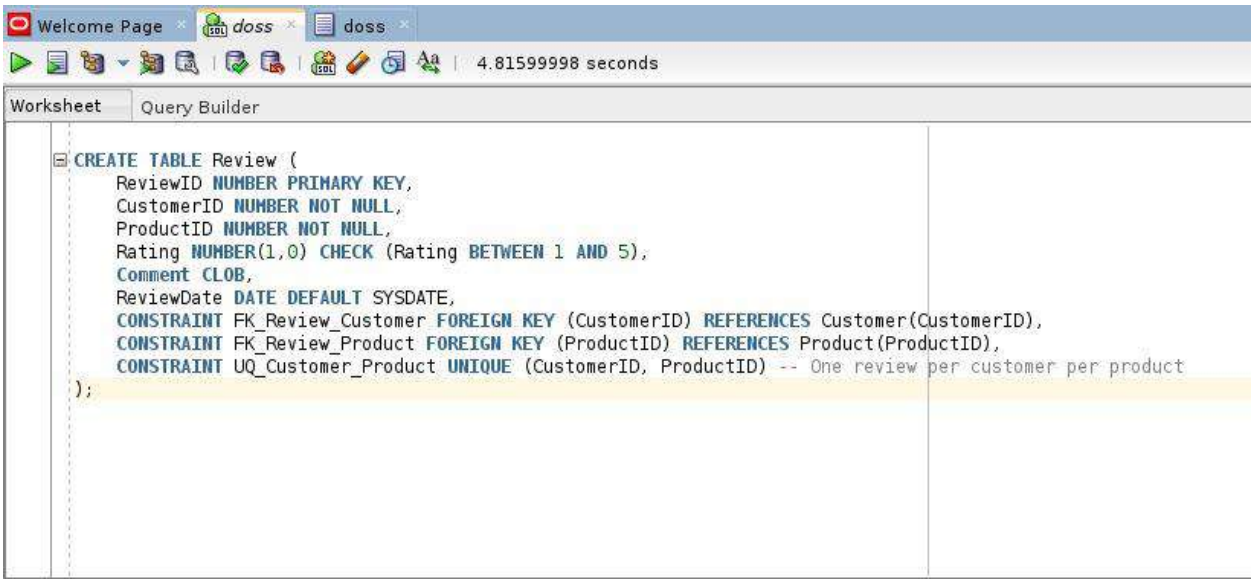



Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
CREATE TABLE Product (
ProductID NUMBER PRIMARY KEY,
ProductName VARCHAR2(100) NOT NULL,
Price NUMBER(10,2) NOT NULL,
Category VARCHAR2(50),
Description CLOB
);

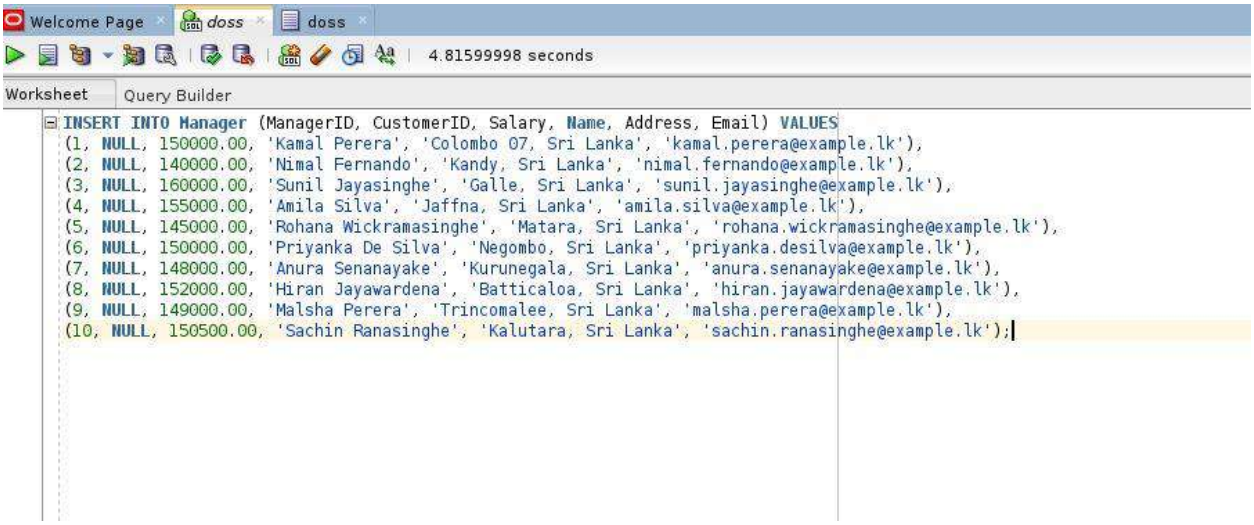

Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
CREATE TABLE Order (
OrderID NUMBER PRIMARY KEY,
CustomerID NUMBER NOT NULL,
OrderDate TIMESTAMP DEFAULT SYSTIMESTAMP,
TotalAmount NUMBER(10,2) NOT NULL,
PaymentMethod VARCHAR2(50),
OrderStatus VARCHAR2(50),
FOREIGN KEY (CustomerID) REFERENCES Customer(CustomerID)
);

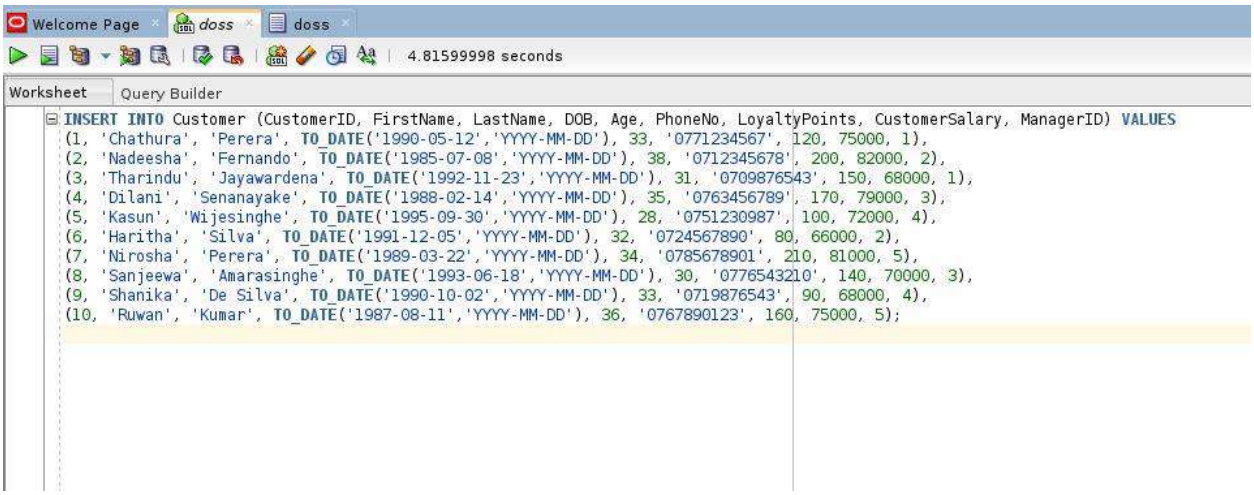

Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
CREATE TABLE OrderItems (
OrderItemID NUMBER PRIMARY KEY,
OrderID NUMBER NOT NULL,
ProductID NUMBER NOT NULL,
Tax NUMBER(5,2) DEFAULT 0.00,
Quantity NUMBER NOT NULL,
UnitPrice NUMBER(10,2) NOT NULL, -- Price of the product at the time of order
TotalPrice NUMBER(10,2) NOT NULL, -- Calculated as Quantity * UnitPrice * (1 + Tax)
FOREIGN KEY (OrderID) REFERENCES CustomerOrder(OrderID),
FOREIGN KEY (ProductID) REFERENCES Product(ProductID),
UNIQUE (OrderID, ProductID) -- Prevent duplicate items in an order
);

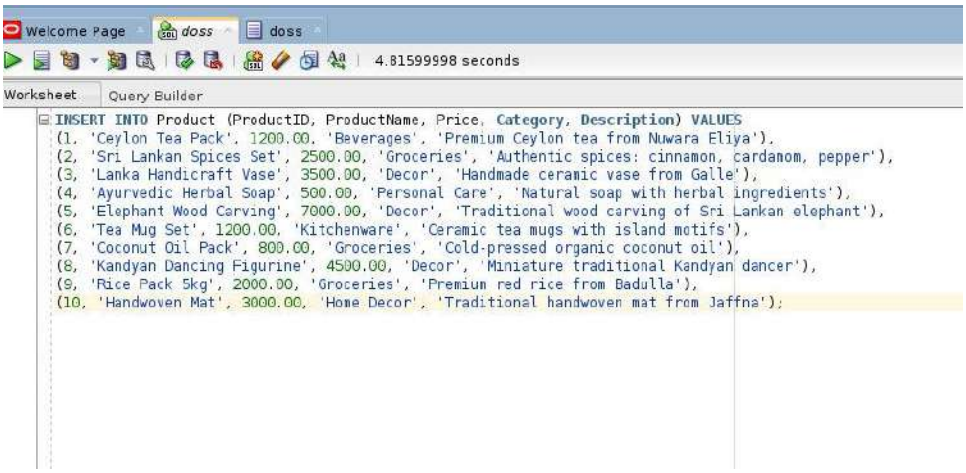

Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
CREATE TABLE Manager (
ManagerID NUMBER PRIMARY KEY,
CustomerID NUMBER UNIQUE,
Salary NUMBER(10,2) NOT NULL,
Name VARCHAR2(100) NOT NULL,
Address VARCHAR2(255),
Email VARCHAR2(100) UNIQUE,
FOREIGN KEY (CustomerID) REFERENCES Customer(CustomerID)
);

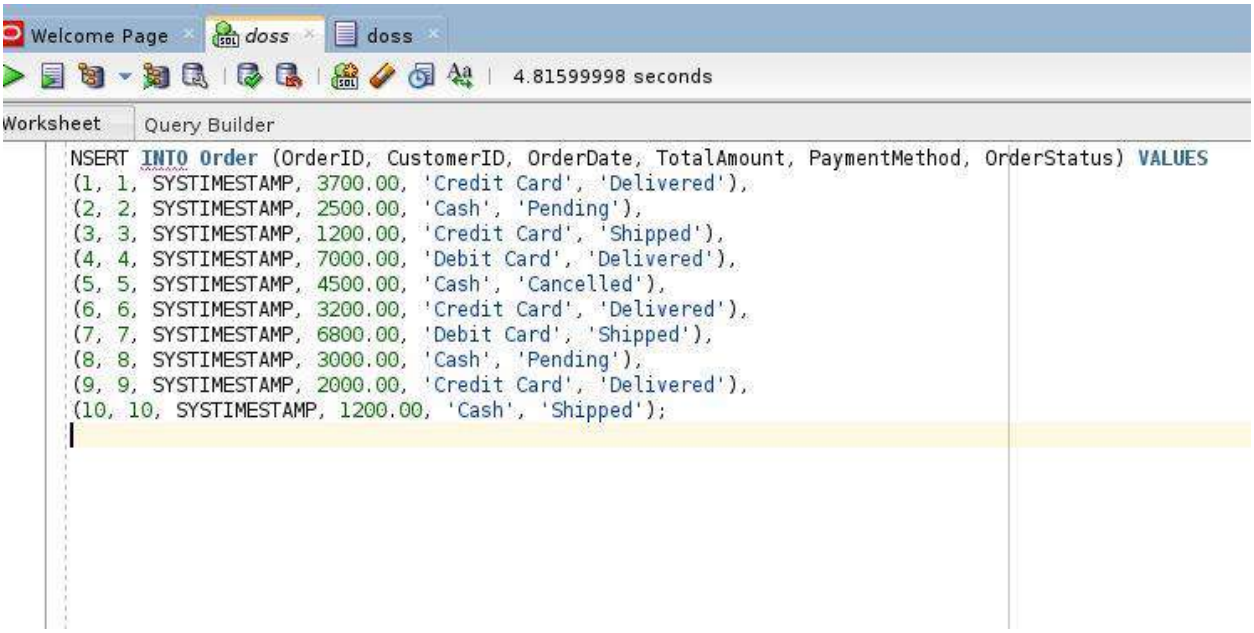


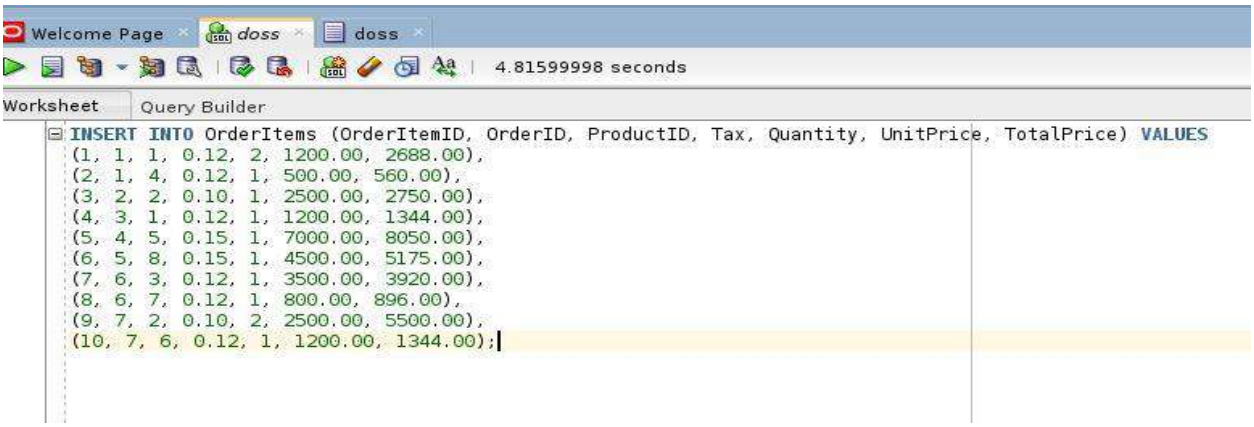
06. Insert Data

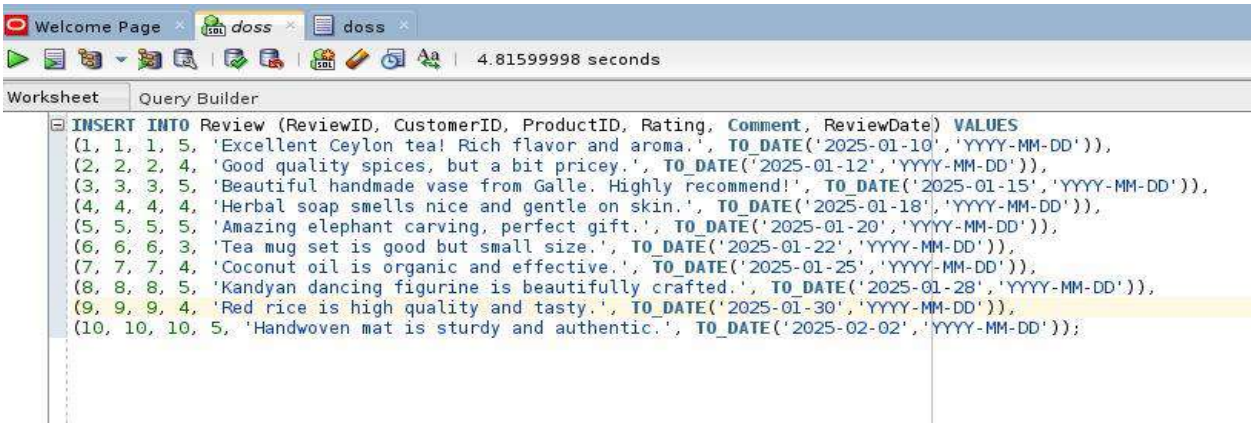



Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
INSERT INTO Customer (CustomerID, FirstName, LastName, DOB, Age, PhoneNo, LoyaltyPoints, CustomerSalary, ManagerID) VALUES
(1, 'Chathura', 'Perera', TO_DATE('1990-05-12','YYYY-MM-DD'), 33, '0771234567', 120, 75000, 1),
(2, 'Nadeesha', 'Fernando', TO_DATE('1985-07-08','YYYY-MM-DD'), 38, '0712345678', 200, 82000, 2),
(3, 'Tharindu', 'Jayawardena', TO_DATE('1992-11-23','YYYY-MM-DD'), 31, '0709876543', 150, 68000, 1),
(4, 'Dilani', 'Senanayake', TO_DATE('1988-02-14','YYYY-MM-DD'), 35, '0763456789', 170, 79000, 3),
(5, 'Kasun', 'Wijesinghe', TO_DATE('1995-09-30','YYYY-MM-DD'), 28, '0751230987', 100, 72000, 4),
(6, 'Haritha', 'Silva', TO_DATE('1991-12-05','YYYY-MM-DD'), 32, '0724567890', 80, 66000, 2),
(7, 'Nirosha', 'Perera', TO_DATE('1989-03-22','YYYY-MM-DD'), 34, '0785678901', 210, 81000, 5),
(8, 'Sanjeewa', 'Amarasinghe', TO_DATE('1993-06-18','YYYY-MM-DD'), 30, '0776543210', 140, 70000, 3),
(9, 'Shanika', 'De Silva', TO_DATE('1990-10-02','YYYY-MM-DD'), 33, '0719876543', 90, 68000, 4),
(10, 'Ruwan', 'Kumar', TO_DATE('1987-08-11','YYYY-MM-DD'), 36, '0767890123', 160, 75000, 5);

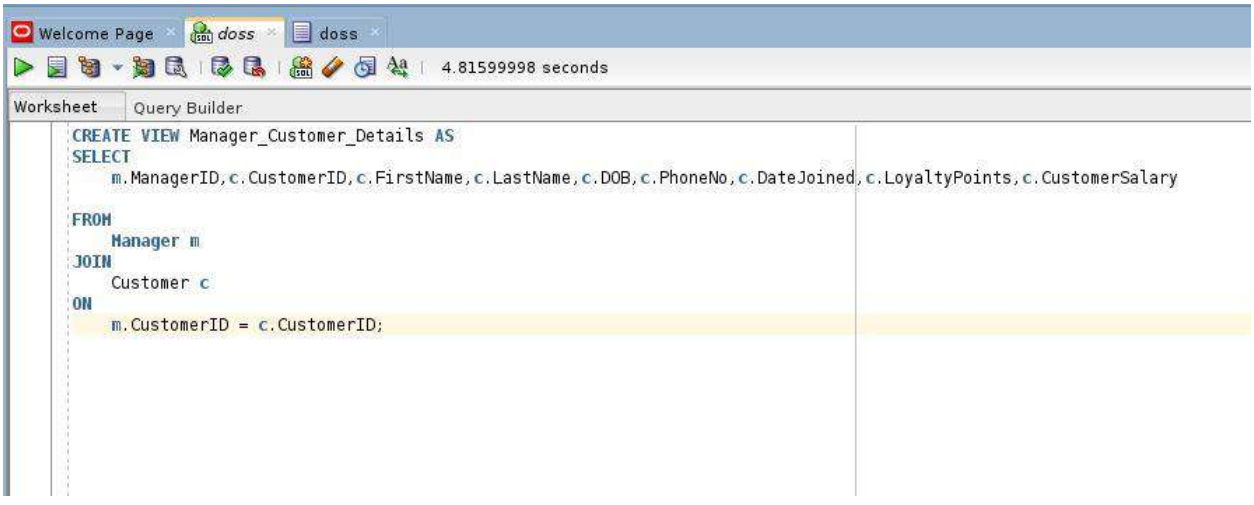

Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
INSERT INTO Product (ProductID, ProductName, Price, Category, Description) VALUES
(1, 'Ceylon Tea Pack', 1200.00, 'Beverages', 'Premium Ceylon tea from Nuwara Eliya'),
(2, 'Sri Lankan Spices Set', 2500.00, 'Groceries', 'Authentic spices: cinnamon, cardamom, pepper'),
(3, 'Lanka Handicraft Vase', 3500.00, 'Decor', 'Handmade ceramic vase from Galle'),
(4, 'Ayurvedic Herbal Soap', 500.00, 'Personal Care', 'Natural soap with herbal ingredients'),
(5, 'Elephant Wood Carving', 7000.00, 'Decor', 'Traditional wood carving of Sri Lankan elephant'),
(6, 'Tea Mug Set', 1200.00, 'Kitchenware', 'Ceramic tea mugs with island motifs'),
(7, 'Coconut Oil Pack', 800.00, 'Groceries', 'Cold-pressed organic coconut oil'),
(8, 'Kandyan Dancing Figurine', 4500.00, 'Decor', 'Miniature traditional Kandyan dancer'),
(9, 'Rice Pack 5kg', 2000.00, 'Groceries', 'Premium red rice from Badulla'),
(10, 'Handwoven Mat', 3000.00, 'Home Decor', 'Traditional handwoven mat from Jaffna');


Welcome Page
doss
doss
4.81599998 seconds
Worksheet
Query Builder
NSERT INTO Order (OrderID, CustomerID, OrderDate, TotalAmount, PaymentMethod, OrderStatus) VALUES
(1, 1, SYSTIMESTAMP, 3700.00, 'Credit Card', 'Delivered'),
(2, 2, SYSTIMESTAMP, 2500.00, 'Cash', 'Pending'),
(3, 3, SYSTIMESTAMP, 1200.00, 'Credit Card', 'Shipped'),
(4, 4, SYSTIMESTAMP, 7000.00, 'Debit Card', 'Delivered'),
(5, 5, SYSTIMESTAMP, 4500.00, 'Cash', 'Cancelled'),
(6, 6, SYSTIMESTAMP, 3200.00, 'Credit Card', 'Delivered'),
(7, 7, SYSTIMESTAMP, 6800.00, 'Debit Card', 'Shipped'),
(8, 8, SYSTIMESTAMP, 3000.00, 'Cash', 'Pending'),
(9, 9, SYSTIMESTAMP, 2000.00, 'Credit Card', 'Delivered'),
(10, 10, SYSTIMESTAMP, 1200.00, 'Cash', 'Shipped');



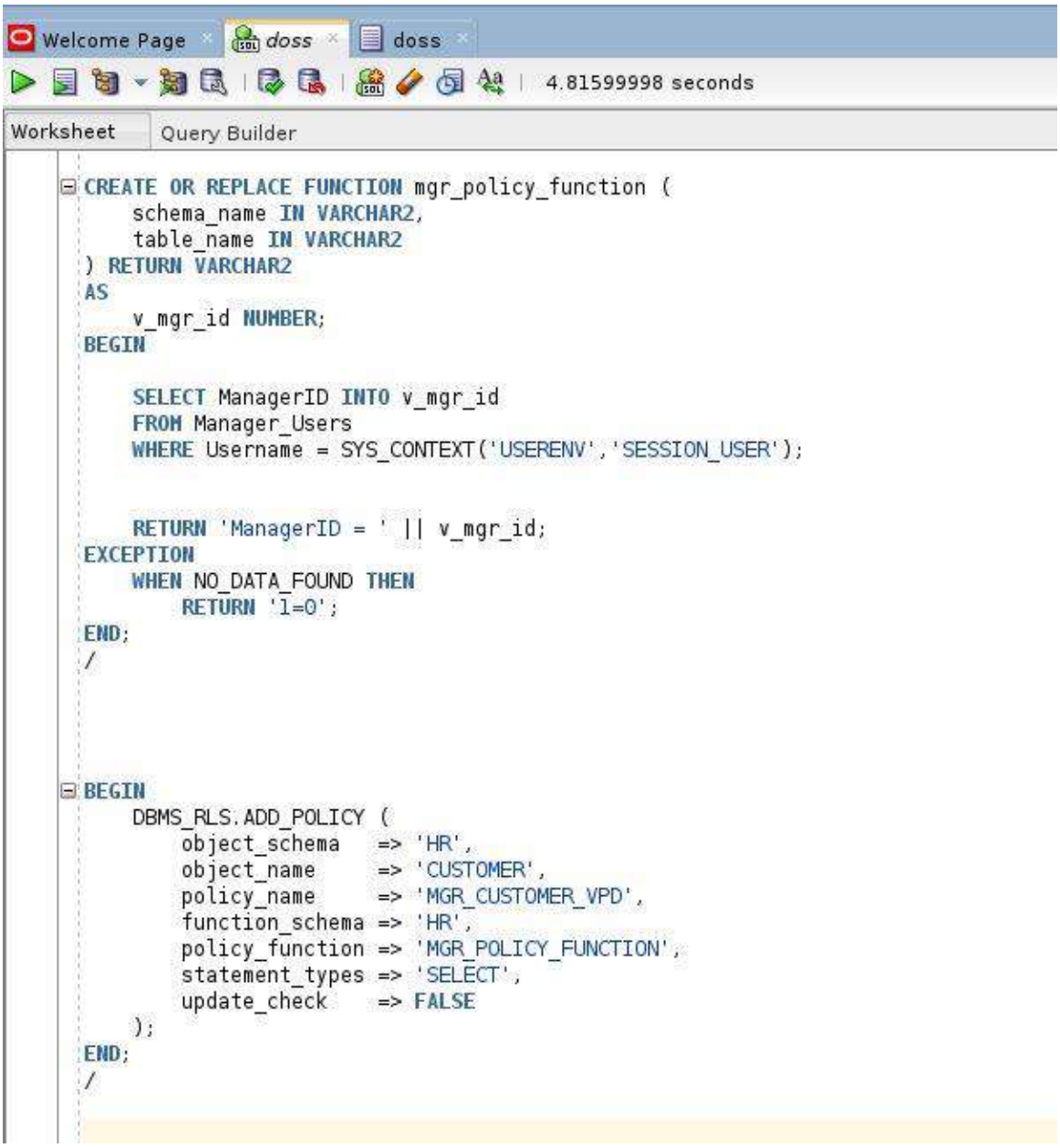


07. Create View

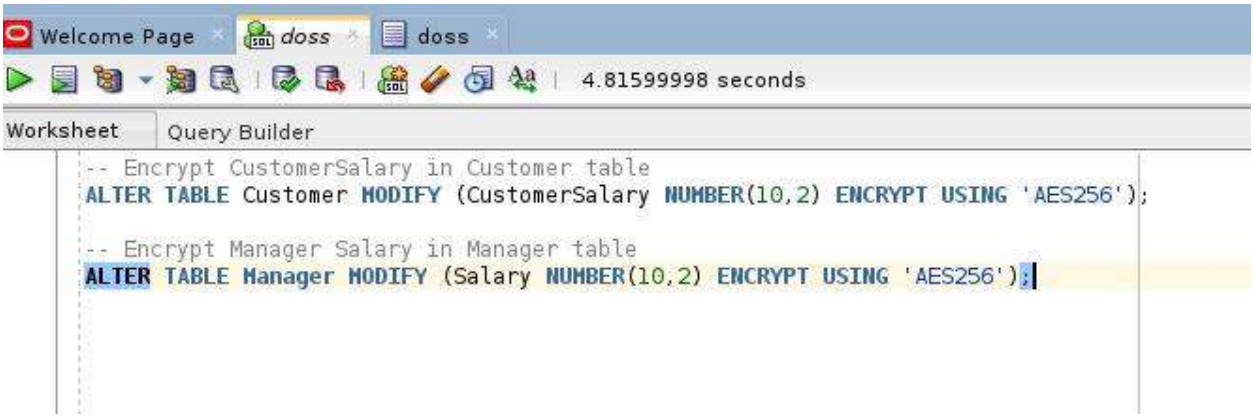


08. Create VPD

Dynamically filters the data of the CUSTOMER table based on the currently logged-in manager.

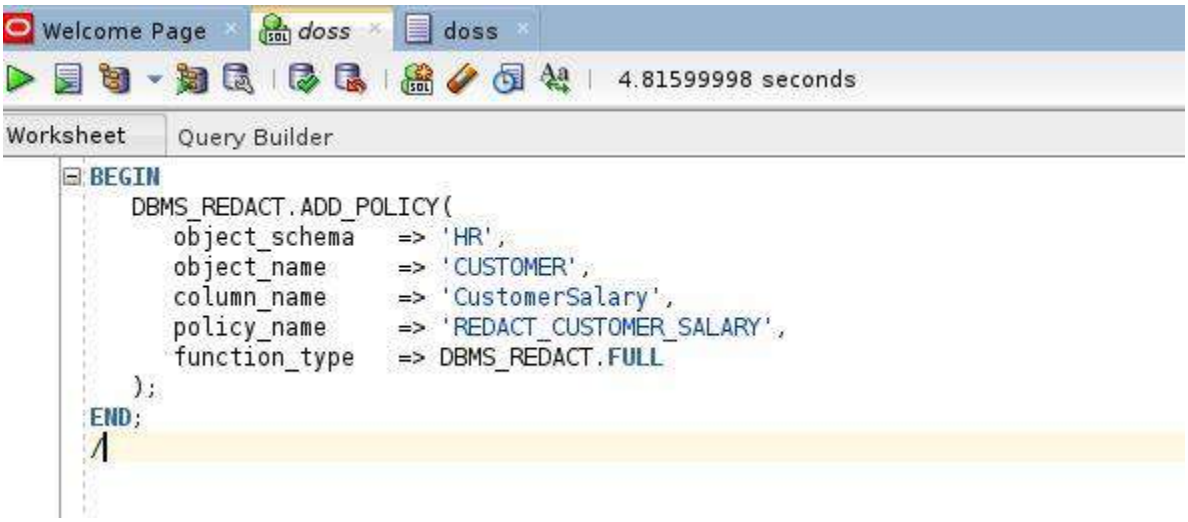


09. Data Encryption

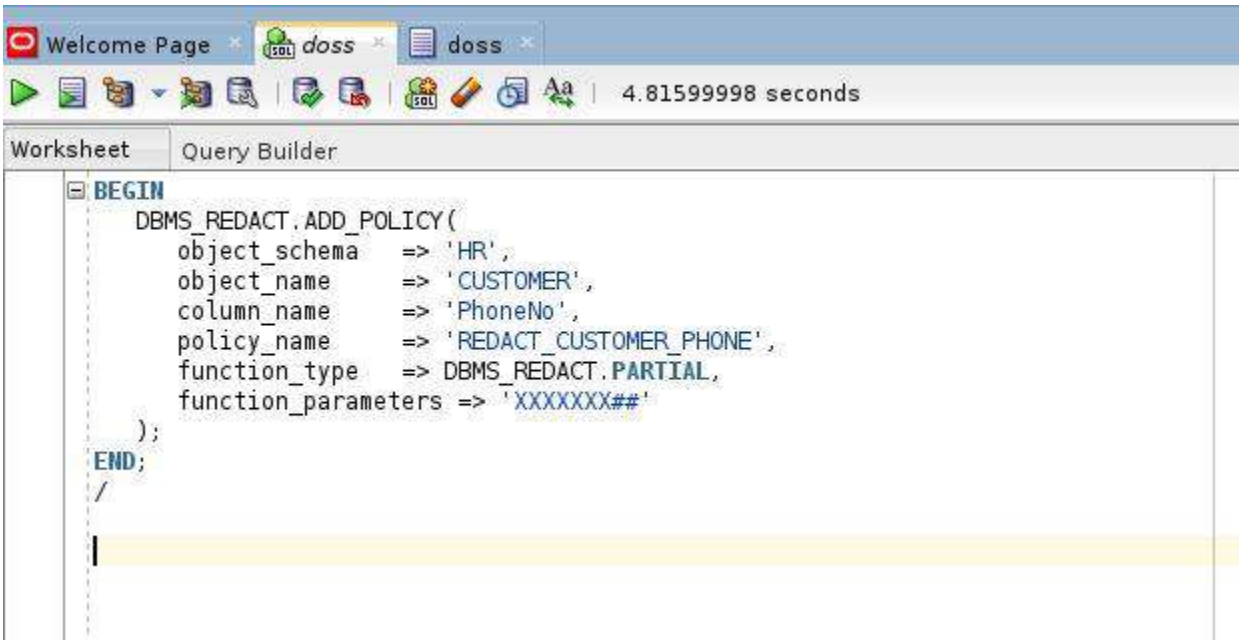


10. Data Masking

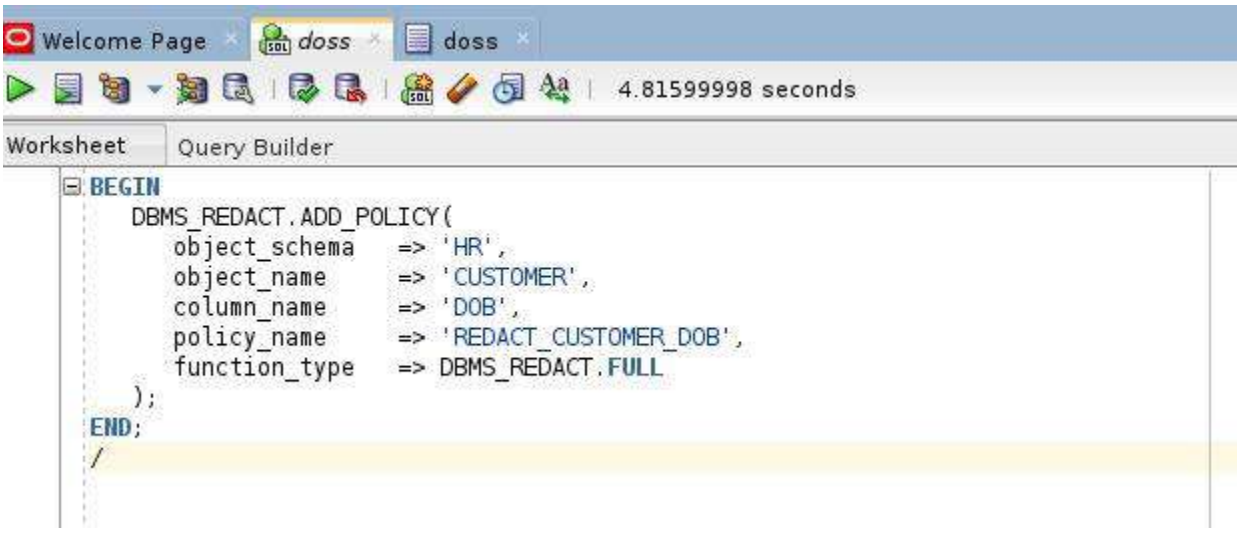
Mask Customer Salary completely



Mask Customer PhoneNo partially (show last 2 digits)

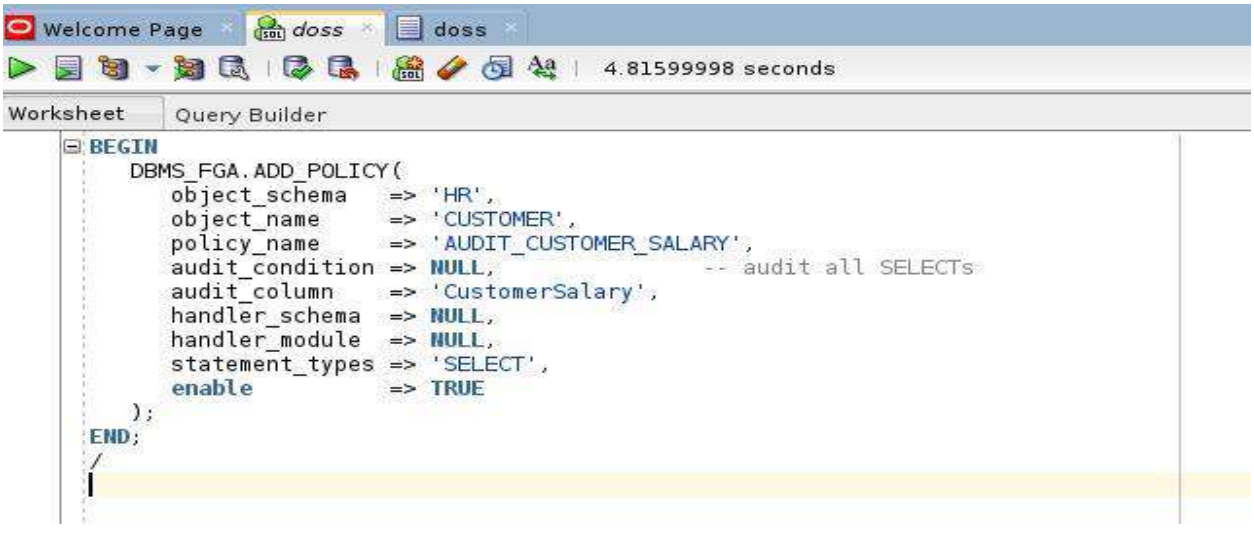


Mask Customer DOB completely



11. Implement FGA Policy

Create an FGA policy to audit access to CustomerSalary



Task 03

Big Data Security vs Traditional Data Security

a.) Big Data Security

Big data security entails protecting large and complex datasets that are growing quickly using strategies that provide confidentiality, integrity, and availability. Big data security is also contingent on analytics and machine-learning for threat detection, and provenance tracking of data—not necessary in traditional database security.

The main security requirements of big data

1. Data Confidentiality

Safeguard sensitive data from unauthorized access , during storage and communication, with encryption, anonymization, and access control tools.

2. Data Integrity

Maintain the accuracy and trustworthiness of data, by using hashing, checksums, and signatures, to enable detection of unauthorized modifications and corruptions.

3. Data Availability

Maintain data and its services in ways to assure continuous availability using means like redundancy, backups, load balancing, and resilient architecture to mitigate failures or attacks.

4. Authentication and Access Control

Verify user action and identity, using multifactor authentication, and implement role-based permissions with the lowest minimum privileges for access to a secure data system.

5. Accountability and Auditing

Capture, log, and monitor every change to data to detect misconduct, support compliance, and facilitate an audit trail of system activities and transparency.

6. Privacy Preservation

To assure the privacy of individuals in big data, we use techniques such as differential privacy, techniques like pseudonymization, and tools by strong governance protocols to comply with regulatory frameworks during the collection and processing stages.

7. Secure Data Sharing and Interoperability

Encourage safe, secure collaboration among organizations using secure sharing methods, interoperability of standards, and organization wide policies, with minimal exposure of sensitive data and information.

Difference Between Traditional Data and Big Data

Requirement	Traditional Systems	Big Data Systems
Data Confidentiality	Focuses on structured databases with basic encryption and basic access.	Handles diverse datasets on distributed nodes with scalable encryption.
Data Integrity	Does verification through monitoring or manual checks on one database or application?	Verification via distributed integrity checks and streams.
Data Availability	Availability ensured via backup and failover.	High availability is needed for clustered systems and continuous analytics.
Authentication & Access Control	Usually provides a single application login with basic type roles.	Multi-site authentication via APIs and cloud services.
Accountability & Auditing	Usually provides centralized monitoring and logging within a single system.	Distributed logging for traceability in multi-type cloud environments.
Privacy Preservation	Data is usually just masked or anonymized within databases.	Advanced techniques reduce re-identification risks in multiple datasets.
Secure Data Sharing & Interoperability	Data typically stays within the organization, unshared.	Enables secure data sharing, interoperability, and risk mitigation in organizations.

b.) Common Attacks on Big Data Security

1.SQL Injection

SQL Injections are attacks that exploit vulnerabilities in an input field to insert malicious code into an SQL query. Attackers use SQL Injection attacks to manipulate the backend SQL databases to access, modify or even delete sensitive organizational records.

Impact: Loss of sensitive data; unauthorized changes; removing or bypassing authentication norms; regulatory violations; financial losses, harmed reputation due to exposed or corrupt organizational databases.

2. Unauthorized Access / Data Breaches

Attackers take advantage of low authentication/poorly configured big data platform access to exploit access points to gain unauthorized entry to exfiltrate confidential records from NoSQL or distributed collaborative environments often in a massive scale.

Impact: Regulatory fines/losses, financial losses due to stolen identities/losses due to reputation loss, personal data exposure, and operational losses due to huge exposure of sensitive personal data.

3. Ransomware / Malware Injections

Malicious software corrupts or encrypts critical organization repositories of data making large datasets globally inaccessible, to regain access, attackers demand ransom thereby crippling analytics and operations across distributed big data systems.

Impact: Downtime costs, ransom demand costs, corrupt datasets, reduced productivity (often hours to days), and damaged trust threaten long-term data integrity and business continuity.

4. Denial-of-Service (DoS / DDoS) Attacks against big data infrastructure with extreme traffic overload on services drain network and computer power thereby disrupting distributed customers and denying legitimate customers from accessing essential resources.

Impact: Revenue losses, lost service, frustrated customers, and failures stemming from failures of mandated critical services ensure infrastructure is heavily unavailable or considered degraded.

5. Inference Attacks

Adversaries can take the query results and query patterns of analysis to extract inferred information out of revealed information exploiting the restricted privacy protections of the analytics pipeline without necessarily needing access to the system.

Impact: Breaches of privacy, theft of intellectual property, noncompliance with legal or regulatory obligations, and reputational harm to the organization if information that is sensitive can be inferred from aggregate queries.

c.) Security Controls to Mitigate Attacks

Mitigating attacks on big data systems requires several types of security controls. To mitigate these attacks security teams must install one or more of the security controls below.

1. SQL Injection

→ ***Input Validation and Parameterized Queries -*** Validate ALL user input and use prepared statements with parameterized queries in your code to arbitrarily add user input SQL code.
→ ***Web Application Firewall (WAF) -*** WAFs can identify and block suspicious query patterns before it makes it to the database engine.

2. Unauthorized Access / Data Breaches

→ ***Role-Based Access Control (RBAC) -*** Use strict access control, establishing user roles and privileges to limit access to your big data to expose less sensitive data.
→ ***Data Encryption -*** Encrypt sensitive data at rest and during transfer to keep information unreadable after being stolen.

3. Ransomware / Malicious Software Injections

→ ***Secure, Immutable, and Regular Backups -*** Consistently establishing secure and immutable backups that function as a backup method, allowing for recovery of data without ransom (or critical data loss).
→ ***Endpoint Detection and Other Anti-Malware Software -*** Using detection and monitoring solutions to detect and quarantine Malware so it would not infect the the rest of the system.

4. Denial-of-Service (DoS / DDoS)

→ ***Filtering / Network Level Rate Limiting*** -Stop malicious traffic surges from overwhelming big data services.

→ ***Redundant Infrastructure / Load Balancing -*** Having multiple nodes and data centers to handle bad actor attempts to overwhelm that availability in those services.

5. Inference Attacks

→ ***Query Restrictions & Aggregation Controls -*** Limit highly precise queries and/or repeated queries that could have predisposed adversaries to deduce sensitive information through aggregated results.

→ ***Differential Privacy Techniques -*** Add systematic noise or anonymization to the outputs of queries to protect the identity of individual records while maintaining the analytical utility of the records.

References

1. **What is Oracle Linux?**
   https://en.wikipedia.org/wiki/Oracle_Linux

2. **Understanding big data security**
   https://www.redzonetech.net/blog-posts/big-data-security

3. **Big Data Security Concerns**
   https://www.integrate.io/blog/big-data-security-concerns/?

4. **Big Data Analytics Versus Traditional Data Analytics**
   https://infomineo.com/blog/big-data-analytics-versus-traditional-data-analytics/

5. **Attacks on Big Data Security**
   https://www.bcs.org/articles-opinion-and-research/top-ten-database-attacks/

   https://www.buchanan.com/database-security-risks-and-threats/

   https://dl.acm.org/doi/abs/10.3103/S0146411620080271

6. **Security Controls to Mitigate Attacks**
   https://www.researchgate.net/publication/301277002_Database_Security_-_Attacks_and_Control_Methods

   https://www.datasunrise.com/potential-db-threats/mitigating-db-threats/

   https://www.twingate.com/blog/glossary/inference-attack