Q: What is SELinux?
A: SELinux, or Security-Enhanced Linux, is a security framework designed to enhance the security of Linux systems.

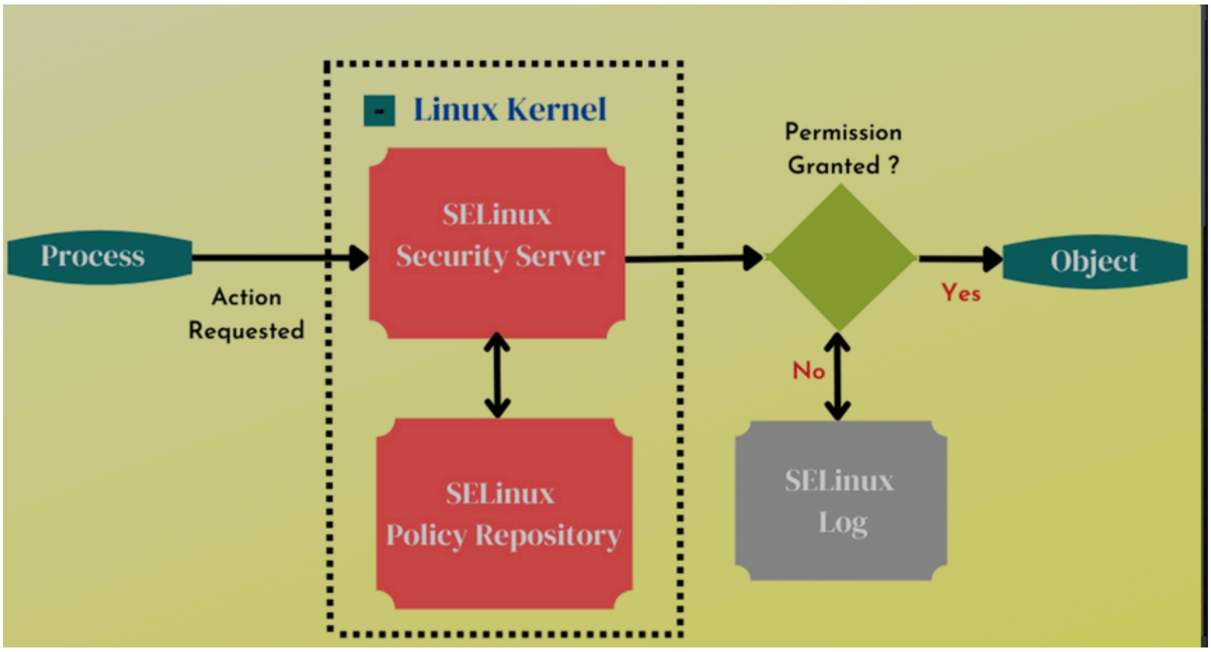
Q: What problem does SELinux solve?
A: SELinux addresses issues related to traditional UNIX permissions by providing fine-grained access control and confinement of processes to specific domains. It prevents unauthorized access and mitigates privilege escalation attacks, thus significantly enhancing system security.

Q: What was the issue before SELinux, and how does it work?
A: Before SELinux, traditional UNIX permissions lacked the granularity and control provided by SELinux. Users had to rely on discretionary access control based on user IDs and group IDs, which could lead to security vulnerabilities. SELinux works by enforcing system-wide administratively-defined policies that dictate how processes interact with files and other processes. It labels all processes and files, separating them into domains and restricting their access based on policies to ensure data confidentiality, integrity, and protection from untrusted inputs.

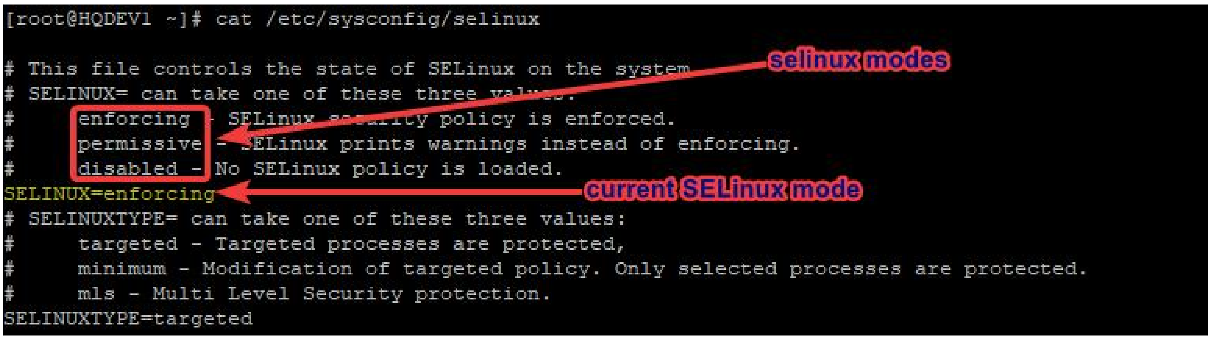
Key Terms:

1. **Mandatory Access Control (MAC)**: A security model where access controls are defined and enforced by the operating system kernel, independent of user actions. SELinux implements MAC.
2. **Policies:** Rules and configurations that define how SELinux controls access to resources such as files, processes, and network ports.
3. **Labels:** SELinux uses labels to identify and enforce access controls on various system resources. Labels are attached to files, processes, and network ports to determine their permissions.
4. **Context:** Refers to the combination of labels associated with a resource. For example, file context includes security context information such as user, role, type, and sensitivity level.
5. **Types:** Refers to the classification of resources (files, processes, etc.) based on their purpose or function. SELinux assigns types to resources to control their interactions.
6. **Users, Roles, and Domains:** SELinux extends the traditional UNIX security model by introducing additional concepts such as roles and domains. Users are associated with roles, and roles are associated with domains. Domains represent contexts in which processes operate and interact with system resources.
7. **Booleans:** SELinux provides Boolean settings that allow administrators to toggle specific SELinux behaviors on or off, providing flexibility in security configurations.

How SELinux Works in Real-Time:



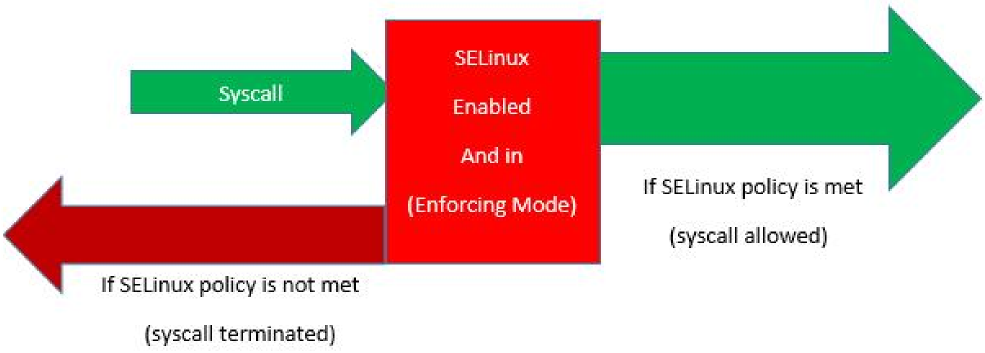
How do i know if SELinux is Enabled: $ cat /etc/sysconfig/selinux or sestatus or getenforce



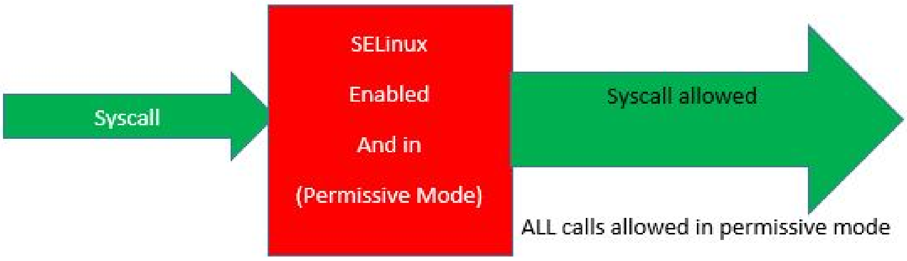
```
[root@HQDEV1 ~]# cat /etc/sysconfig/selinux

# 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=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

How does SELinux Works :

- **Enforcing Mode**



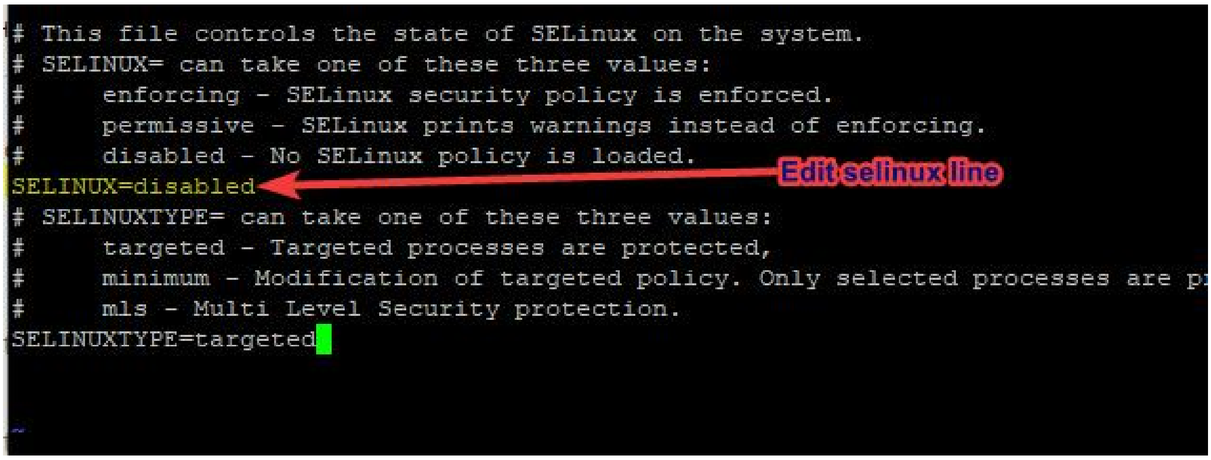
- **Permissive Mode**



How do I switch from enforcing to permissive mode ? : $ setenforce permissive

How do I switch from permissive to enforcing mode?: $ setenforce enforcing

How to disable SELinux (Not recommended in Prod environment)
$ vi /etc/sysconfig/selinux
Edit the Selinux line to disable
Save and exit
Reboot the machine



```
# 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=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are p
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


~
```

What is SELinux Context?

SELinux context is simply the labels that are associated with objects(files, directories, ports, processes, etc).

Everything on a Linux system, including objects such as (files, directories, ports, processes/services, devices, etc) have context, i.e, they are all labeled or associated with context.

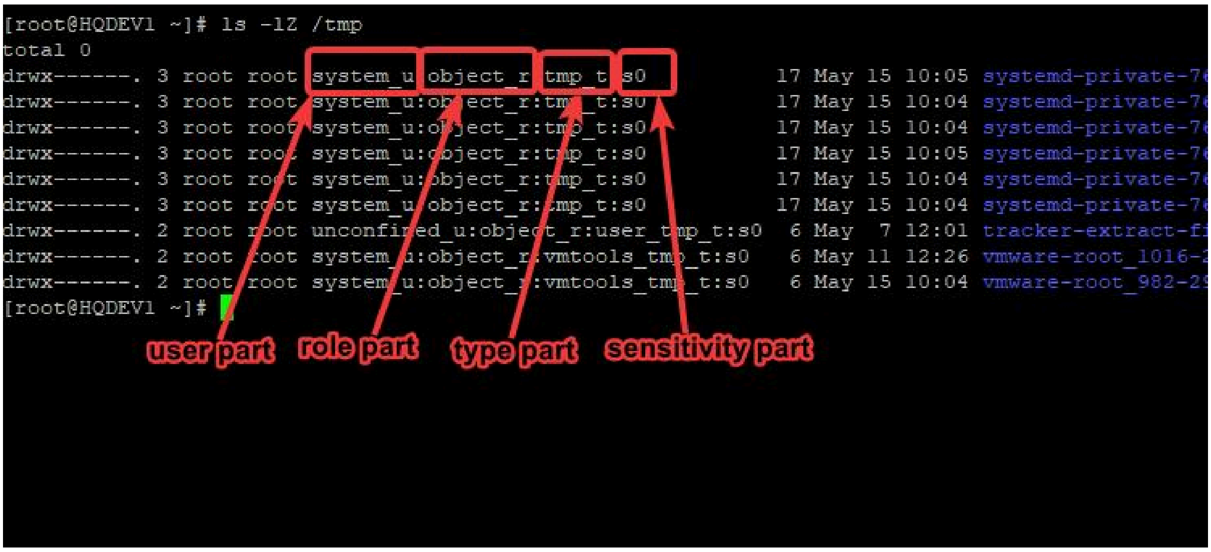
Context is used to make access control decisions, i.e, allow this subject(syscall) to go through if the object's context/label is correct.

Context is divided into four parts. They are the user part, role part, type part, and the sensitivity part

To see the context of an object (files, directories, ports, processes/services, devices, etc), we use the "-Z" option with their simple listing commands

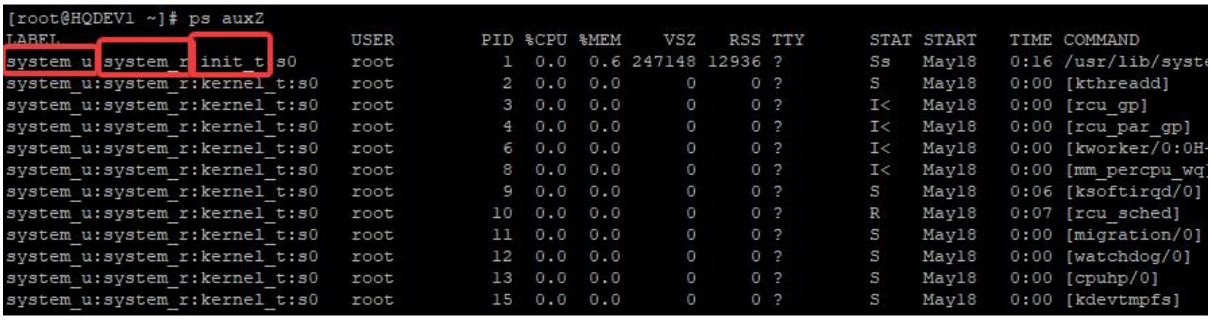
For example, to see the context of the files in "/tmp" directory, you will run the command,

$ ls -lZ /tmp



```
[root@HQDEV1 ~]# ls -lZ /tmp
total 0
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:05 systemd-private-7
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:04 systemd-private-7
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:04 systemd-private-7
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:05 systemd-private-7
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:04 systemd-private-7
drwx------. 3 root root system_u:object_r:tmp_t:s0        17 May 15 10:04 systemd-private-7
drwx------. 2 root root unconfined_u:object_r:user_tmp_t:s0  6 May  7 12:01 tracker-extract-fi
drwx------. 2 root root system_u:object_r:vmtools_tmp_t:s0   6 May 11 12:26 vmware-root_1016-
drwx------. 2 root root system_u:object_r:vmtools_tmp_t:s0   6 May 15 10:04 vmware-root_982-2
[root@HQDEV1 ~]#
```

To see the context of a service or process, you run the command: $ ps auxZ



```
[root@HQDEV1 ~]# ps auxZ
LABEL                           USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
system_u:system_r:init_t:s0     root          1  0.0  0.6 247148 12936 ?        Ss   May18   0:16 /usr/lib/syst
system_u:system_r:kernel_t:s0   root          2  0.0  0.0      0     0 ?        S    May18   0:00 [kthreadd]
system_u:system_r:kernel_t:s0   root          3  0.0  0.0      0     0 ?        I<   May18   0:00 [rcu_gp]
system_u:system_r:kernel_t:s0   root          4  0.0  0.0      0     0 ?        I<   May18   0:00 [rcu_par_gp]
system_u:system_r:kernel_t:s0   root          6  0.0  0.0      0     0 ?        I<   May18   0:00 [kworker/0:0H
system_u:system_r:kernel_t:s0   root          8  0.0  0.0      0     0 ?        I<   May18   0:00 [mm_percpu_wq
system_u:system_r:kernel_t:s0   root          9  0.0  0.0      0     0 ?        S    May18   0:06 [ksoftirqd/0]
system_u:system_r:kernel_t:s0   root         10  0.0  0.0      0     0 ?        R    May18   0:07 [rcu_sched]
system_u:system_r:kernel_t:s0   root         11  0.0  0.0      0     0 ?        S    May18   0:00 [migration/0]
system_u:system_r:kernel_t:s0   root         12  0.0  0.0      0     0 ?        S    May18   0:00 [watchdog/0]
system_u:system_r:kernel_t:s0   root         13  0.0  0.0      0     0 ?        S    May18   0:00 [cpuhp/0]
system_u:system_r:kernel_t:s0   root         15  0.0  0.0      0     0 ?        S    May18   0:00 [kdevtmpfs]
```

For example, to see the contexts of nginx service, run the command: $ ps auxZ |grep nginx

To see the context of a port, use the command: $ netstat -Ztulpen

Very Important:

Key1: when you copy a file/directory to a location, the file automatically inherits the SELinux security context and attributes of the location it was copied to

However;

Key2: When you move a file/directory to a location, the file/directory does not inherit the SELinux security context and attributes of the new location, instead, it moves with its old location's context.

Key3: Most times, problems with SELinux is as a result of filesystems being mislabeled with the wrong context, and booleans not being enabled.

Most Important:
Selinux troubleshooting guide
What is SELinux
A sysadmin's guide to SELinux: 42 answers to the big questions
What Is SELinux (Security-Enhanced Linux)?