SELinux

Security-Enhanced Linux (SELinux) is a solution that incorporates a strong, flexible Mandatory Access Control (MAC) architecture into Cisco IOS-XE platforms through a combination of a Linux kernel security module and system utilities.

SELinux provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. This approach helps prevent tampering and bypassing of application security mechanisms while limiting damage from malicious or flawed applications.

SELinux Modes

SELinux can operate either in **Permissive mode** or **Enforcing mode** when enabled on a system.

- **Permissive mode** : SELinux does not enforce the policy and only generates system logs for any denials caused by policy violations. Operations are logged for resource access policy violations but not denied.
- **Enforcing mode:** SELinux policy is enabled and enforced. It denies resource access based on the access policy rules, and generates system logs.

SELinux is enabled in **Enforcing mode** by default on supported Cisco IOS XE platforms. In the Enforcing mode, any system resource access that does not have the necessary allow policy is treated as a violation, and the operation is denied. The violating operation fails when a denial occurs, and system logs are generated. In Enforcing mode, the solution works in access-violation prevention mode.

Prerequisites

There are no specific prerequisites for this feature.

Restrictions

There are no specific restrictions for this feature.

Configure SELinux in EXEC Mode

Use this example to configure SELinux in EXEC mode:

SUMMARY STEPS

1. **set platform software selinux** {**default** | **enforcing** | **permissive**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**set platform software selinux** {**default** | **enforcing** | **permissive**}	

Example

```
Device# set platform software selinux ?

default     Set SELinux mode to default
enforcing   Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

Configure SELinux in CONFIG Mode

Use this example to configure SELinux in configuration mode:

SUMMARY STEPS

1. **platform security selinux** {**enforcing** | **permissive**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**platform security selinux** {**enforcing** | **permissive**}	

Example

```
Device(config)# platform security selinux

enforcing   Set SELinux policy to Enforcing mode
permissive  Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

SYSLOG message reference

This section covers details about syslog messages.

Facility-Severity-Mnemonic	**%SELINUX-1-VIOLATION**
Severity-Meaning	Alert Level Log
Message	N/A
Message Explanation	Resource access was made by the process for which a resource access policy does not exist. The operation was flagged, and resource access was denied. A system log was generated with information that process resource access has been denied.
Component	SELINUX
Recommended Action	Contact Cisco TAC with the following relevant information as attachments: • The exact message as it appears on the console or in the system • Output of the **show tech-support** command (text file) • Archive of Btrace files from the box using the following command: **request platform software trace archive target <URL>** • Output of the **show platform software selinux** command

This example shows sample syslog messages:

Example 1:

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

Example 2:

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

Verify SELinux enablement

Use the **show platform software selinux** command to view the SELinux configuration mode:

```
Device# show platform software selinux
========================================
IOS-XE SELINUX STATUS
========================================
SElinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

Troubleshoot SELinux

If there is an instance of an SELinux violation on your device or network, please reach out to Cisco TAC with these details:

- The message exactly as it appears on the console or in the system log. For example:

  ```
  device#request platform software trace archive target
      flash:selinux_btrace_logs
  ```

- Output of the **show tech-support** command (text file)
- Archive of Btrace files from the box using this command:

  request platform software trace archive target <URL>

- Output of the **show platform software selinux** command