Security-Enhanced Linux

Information About Security-Enhanced Linux

Security-Enhanced Linux (SELinux)

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

Purpose of SELinux

SELinux provides an enhanced mechanism to enforce the separation of information, based on confidentiality and integrity requirements, which addresses threats of tampering and bypassing of application security mechanisms and enables the confinement of damage that malicious or flawed applications can cause.

SELinux Mechanism

SELinux enforces mandatory access control policies that confine user programs and system services to the minimum privilege required to perform their assigned functionality. This reduces or eliminates the ability of these programs and daemons to cause harm when compromised (for example, through buffer overflows or misconfigurations). This is a practical implementation of principle of least privilege by enforcing MAC on Cisco IOS XE platforms. This confinement mechanism works independently of the traditional Linux access control mechanisms. SELinux allows you to define policies to control the access from an application process to any resource object, thereby allowing for the clear definition and confinement of process behavior.

SELinux Modes in Cisco IOS XE

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

- **Permissive Mode**: In Permissive mode, SELinux does not enforce the policy, and only generates system logs for any denials caused by violation of the resource access policy. The operation is not denied, but only logged for resource access policy violation.
- **Enforcing Mode**: In Enforcing mode, the SELinux policy is enabled and enforced. The Enforcing mode denies resource access based on the access policy rules, and generates system logs.

  SELinux is enabled in the 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.

Note By default, SELinux is in the Enforcing mode.

Configuring SELinux in the EXEC Mode

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service internal** **Example:** `Device(config)# service internal`	Enables the internal commands of the network-based services.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits from the global configuration mode.
Step 5	**set platform software selinux** {**default** | **enforcing** | **permissive**} **Example:** `Device# set platform software selinux enforcing`	Configures SELinux in the EXEC mode.

Configuring SELinux in the Global Configuration Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**service internal** **Example:** `Device(config)# service internal`	Enables the internal commands of the network-based services.
Step 3	**platform security selinux** {**enforcing** | **permissive**} **Example:** `Device(config)# platform security selinux enforcing`	Configures SELinux policy

Examples for SELinux

The following example shows the output for changing the mode from Enforcing to Permissive:

```
"*Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0: SELINUX_MODE_PROG: Platform Selinux
confinement mode downgraded to permissive!"
```

The following example shows the output for changing the mode from Permissive to Enforcing:

```
"*Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0: SELINUX_MODE_PROG: Platform Selinux
confinement mode upgraded to enforcing!"
```

Note If you change the SELinux mode, the change is considered as a system security event, and a system log message is generated.

SELinux Syslog Message Reference

Facility-Severity-Mnemonic	%SELINUX-1-VIOLATION
Severity-Meaning	Alert Level Log
Message	N/A

Facility-Severity-Mnemonic	%SELINUX-1-VIOLATION
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 the Btrace files from the box using the following command: **request platform software trace archive target** *URL* • Output of the **show platform software selinux** command. • Output of the **show platform software audit all | section exclude** command. • Output of the **show platform software audit summary** command.

The following examples display 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
```

Verifying Count of Denials

To verify the count of denials, use the following command:

```
Device# show platform software audit summary
===================================
AUDIT LOG ON chassis 1 route-processor 0
-----------------------------------
AVC Denial count: 6
```

Verifying SELinux Enablement

To verify SELinux enablement, use the following command:

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

Commands

set platform software selinux

To configure security-enhanced Linux (SELinux) in the EXEC mode, use the **set platform software selinux** command.

Note The **service internal** command must be configured before running the **set platform software selinux** command.

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

Syntax Description

default	Sets the SELinux mode to default.
enforcing	Sets the SELinux mode to enforcing. The SELinux mode is enabled and enforced. The Enforcing mode denies resource access based on the access policy rules, and generates system logs.
permissive	Sets the SELinux mode to permissive. SELinux does not enforce the policy, and only generates system logs for any denials caused by violation of the resource access policy.

Command Default None

Command Modes Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to configure SELinux in the EXEC mode:

```
Device# set platform software selinux permissive
```

platform security selinux

To configure the SELinux policy in the platform security settings, use the **platform security selinux** command.

Note The **service internal** command must be configured before running the **platform security selinux** command.

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

Syntax Description

enforcing	Sets the SELinux policy to enforcing mode. The Enforcing mode denies resource access based on the access policy rules, and generates system logs.
permissive	Sets the SELinux policy to permissive mode. SELinux does not enforce the policy, and only generates system logs for any denials caused by violation of the resource access policy.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 17.15.1	This command was introduced.

Examples

The following example shows you how to configure the SELinux policy in the platform security settings:

```
Device# configure terminal
Device(config)# platform security selinux
```