Security-Enhanced Linux のサポート

この章では SELinux の機能について説明します。具体的な内容は次のとおりです。

概要

Security-Enhanced Linux（SELinux）は、Linux カーネル セキュリティ モジュールとシステム ユーティリティで構成されるソリューションで、強力で柔軟な Mandatory Access Control（MAC）アーキテクチャを Cisco IOS-XE プラットフォームに組み込みます。

SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

SELinux の前提条件

この機能に関する固有の要件はありません。

SELinux の制限事項

この機能に関する特定の制限はありません。

SELinux に関する情報

SELinux はユーザープログラムやシステムサービスを、割り当てられた機能を実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、（バッファのオーバーフローや設定不備などによって）侵害された場合、害を生じさせるこれらのプログラムやデーモンの機能が削減または排除されます。これは、Cisco IOS-XE プラットフォームで MAC を適用することによる最小権限の原則の実用的な実装です。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して機能します。SELinux は、アプリケーションプロセスからリソースオブジェクトへのアクセスを制御するポリシーを定義する機能を提供します。これにより、プロセス動作の明確な定義と制限を明確にできます。

SELinux は、システムで有効になっている場合、**Permissive モード**または **Enforcing モード**のいずれかで動作します。

- Permissive モードでは、SELinux はポリシーを適用せず、リソースアクセスポリシーの違反によって発生した拒否のシステムログのみを生成します。操作は拒否されず、リソースアクセスポリシー違反についてのみログに記録されます。
- Enforcing モードでは、SELinux ポリシーが有効になり、適用されます。アクセスポリシールールに基づいてリソースアクセスを拒否し、システムログを生成します。

Cisco IOS XE 17.13.1a 以降、サポートされている Cisco IOS XE プラットフォームでは、SELinux はデフォルトで Enforcing モードで有効になっています。Enforcing モードでは、必要な許可ポリシーを持たないシステムリソースアクセスは違反として扱われ、操作は拒否されます。拒否が発生すると、違反操作は失敗し、システムログが生成されます。Enforcing モードでは、ソリューションはアクセス違反防止モードで機能します。

サポートされるプラットフォーム

Cisco IOS XE 17.13.1a 以降、SELinux は次のプラットフォームで有効になっています。

- Cisco 1000 シリーズ アグリゲーション サービス ルータ
- Cisco 1000 シリーズ サービス統合型ルータ
- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco Catalyst 8000v Edge ソフトウェア
- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォーム
- Cisco VG シリーズ ゲートウェイ：VG400、VG410、VG420、および VG450
- Cisco 1100 ターミナル サービス ゲートウェイ

SELinux の設定

Enforcing モードで SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。

SELinux の機能の一部として、次のコマンドが導入されています。

```
set platform software selinux {default | enforcing | permissive}
platform security selinux {enforcing | permissive}
show platform software selinux
```

（注） これらの新しいコマンドは、**service internal** コマンドとして導入されます。

SELinux の設定（EXEC モード）

set platform software selinux コマンドを使用して、EXEC モードで SELinux を設定します。

次に、EXEC モードでの SELinux 設定の例を示します。

```
Device# set platform software selinux ?

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

SELinux の設定（CONFIG モード）

platform security selinux コマンドを使用して、コンフィギュレーション モードで SELinux を設定します。

次の例は、CONFIG モードでの SELinux 設定を示しています。

```
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)#
```

SELinux の例

次に、モードを Enforcing から Permissive に変更した場合の出力例を示します。

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

次に、モードを Permissive から Enforcing に変更した場合の出力例を示します。

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

（注） SELinux モードが変更されると、この変更はシステム セキュリティ イベントと見なされ、システムログメッセージが生成されます。

Syslog メッセージリファレンス

機能重大度ニーモニック	%SELINUX-1-VIOLATION
重大度の意味	アラートレベルログ
メッセージ	該当なし
メッセージの説明	リソースのアクセスポリシーが存在しないプロセスによって、リソースアクセスが実行されました。操作にフラグが設定され、リソースアクセスが拒否されました。プロセスリソースアクセスが拒否されたという情報を含むシステムログが生成されました。
コンポーネント	SELINUX
推奨処置	次の関連情報を添付ファイルで Cisco TAC に送信してください。 • コンソールまたはシステムに出力されるとおりのメッセージ • **show tech-support** コマンドの出力（テキストファイル） • ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）： **request platform software trace archive target <URL>** • **show platform software selinux** コマンドの出力

次に、syslog メッセージの例を示します。

例 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
```

例 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
```

SELinux の有効化の確認

show platform software selinux コマンドを使用して、SELinux 設定モードを表示します。

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

SELinux のトラブルシューティング

デバイスまたはネットワークで SELinux 違反のインスタンスがある場合は、次の詳細を Cisco TAC に連絡してください。

- コンソールまたはシステムログに出力されるとおりのメッセージ。次に例を示します。

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

- **show tech-support** コマンドの出力（テキストファイル）
- ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）：

  request platform software trace archive target <URL>

- **show platform software selinux** コマンドの出力

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。