Cisco IOS-XE 17.3.1 の新機能

IOS-XE リリース 17.3.1 の IR1101 で使用可能な新機能は次のとおりです。

IO ポートに対する YANG のサポート

この機能により、コマンド ライン インターフェイスと YANG モデル間の互換性が向上します。Cisco IOS-XE YANG データモデルは次のとおりです。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

各リリースにはディレクトリがあり、17.3.1 リリースは 1731 の下にあります。デジタル IO の 2 つのモジュールは、Cisco-IOS-XE-digital-io-oper と Cisco-IOS-XE-digitalio です。

次に、関連する使用可能な IOS-XE CLI コマンドを示します。

コマンドの表示

- show run
- show alarm
- show led

コンフィギュレーション コマンド

- alarm contact attach-to-iox
- no alarm contact attach-to-iox
- alarm contact 1 enable enable
- no alarm contact <1-4> enable

- alarm contact <1-4> application <wet | dry>
- no alarm contact <1-4> application
- alarm contact <1-4> description <alarm description>
- no alarm contact <1-4> description
- alarm contact <1-4> severity <critical | major | minor | none>
- no alarm contact <1-4> severity
- alarm contact <1-4> threshold <1600-2700>
- no alarm contact <1-4> threshold
- alarm contact <1-4> trigger <closed | open>
- no alarm contact <1-4> trigger
- alarm contact <1-4> output <1 | 0>
- alarm contact <1-4> output relay temperature <critical | major | minor>
- alarm contact <1-4> output relay input-alarm <0-4>
- no alarm contact <1-4> output

Security-Enhanced Linux（SELinux）のサポート

Security-Enhanced Linux は Linux カーネルと一部のユーティリティに対する一連のパッチであり、強力で柔軟性の高い強制アクセス制御（MAC）アーキテクチャをカーネルの主要なサブシステムに導入します。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 はユーザプログラムやシステムサーバを、ジョブ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、侵害された場合（バッファのオーバーフローや設定ミスなどによって）害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。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動作します。

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。ソリューションは、サポートされているプラットフォームの基本 IOS-XE ソフトウェアの一部として、デフォルトで有効または動作可能になります。

次に、SELinux 関連の監査ログを表示するために定義された拡張 show コマンドを示します。

show platform software audit all

show platform software audit summary

show platform software audit switch *<<1-8> | active | standby> <FRU identifier from a drop-down list>*

コマンドの例

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show platform software audit summary
===================================
AUDIT LOG ON switch 1
-----------------------------------
AVC Denial count: 58
===================================
```

次に、**show software platform software audit all** コマンドの出力例を示します。

```
Device# show platform software audit all
===================================
AUDIT LOG ON switch 1
-----------------------------------
========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
 name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc:  denied  { execute } for  pid=8300 comm="sh"
 name="id" dev="loop0" ino=6982
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
========== END ============
```

（簡潔にするために出力は省略）

次に、**show software platform software audit switch** コマンドの出力例を示します。

```
Device# show platform software audit switch active R0
========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
 name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
```

```
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc:  denied  { execute_no_trans } for  pid=8600
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc:  denied  { execute_no_trans } for  pid=9307
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc:  denied  { execute_no_trans } for  pid=10858
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc:  denied  { execute_no_trans } for  pid=11579
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc:  denied  { execute_no_trans } for  pid=12451
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
========== END ============
===================================
```

Syslog メッセージリファレンス

機能重大度ニーモニック

- %SELINUX-3-MISMATCH

重大度の意味

- エラーレベルログ

メッセージの説明

- リソースのアクセスポリシーが定義されていないプロセスによって、リソースアクセスが行われました。操作にフラグが付けられましたが、拒否されませんでした。
- 操作は正常に続行され、中断されませんでした。操作が拒否されたプロセスによるリソースアクセスについてのポリシーが欠落していることに関してシステムログが生成されました。

推奨処置

- 次の関連情報を添付ファイルとして CISCO TAC にご連絡ください。

- 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。
- 「show tech-support」の出力（テキストファイル）
- 次のコマンド（「request platform software trace archive target <URL>」）を使用したボックスからの Btrace ファイルのアーカイブ。例：

Device# **request platform software trace archive target flash:selinux_btrace_logs**

P-LTEAP18-GL モデム PID に対するサポートの追加

P-LTEAP18-GL PID は Telit モデム LM960 モデムを使用します。すべての IR1101 モデムの詳細については、次を参照してください。

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_01.html#con_1161147

初期ブートアップセキュリティの改善点

この項の内容は、次のとおりです。

デフォルトパスワード変更の適用

以前のソフトウェアバージョンでは、ユーザが新しいイネーブルパスワードの設定をバイパスできました。工場出荷時の状態へのリセット後、または工場出荷時の状態からデバイスを最初に起動すると、コンソールに次のプロンプトが表示されます。

Would you like to enter the initial configuration dialog? [yes/no]:

以前のソフトウェアバージョンでは **no** の応答が許可されており、イネーブルパスワードが空白のままのデバイスは **Router>** プロンプトになりました。この時点でルータを設定し、イネーブルパスワードが空白のまま稼働状態にすることができます。

以前のドキュメントでは、**enable password** コマンドの代わりに **enable secret** コマンドを使用することを推奨しています。これは、暗号化アルゴリズムが改善されるためでした。

17.3.1 以降では、初期のダイアログが強制的に新しいイネーブルパスワードを設定し、かつ **enable secret** コマンドを代わりに使用して適用するよう変更されました。次に、例を示します。

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: router-1

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: *******
```

```
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: **********

The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: *********
  Configure SNMP Network Management? [yes]: no

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [yes]: no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

次に、初期設定ダイアログに **no** と応答した場合の動作の例を示します。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: ********
Would you like to terminate autoinstall? [yes]: yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

最初のログイン時にイネーブルシークレットが要求され、管理者がパスワードを入力すると、管理者が入力したパスワードは常にマスクされます。管理者が脆弱なパスワードを入力すると、強力なパスワード（つまり、大文字と小文字、特殊文字、数字などの標準的な組み合わせ）を入力するように求められます。プロンプトは、管理者が強力なパスワードを入力するまで表示されます。管理者は、強力なシークレットパスワードを2回入力して、管理者が設定したシークレットを確認する必要があります。

Telnet と HTTP

Telnet と HTTP のブート設定が変更されました。工場出荷時の状態へのリセット後または工場出荷時の状態からデバイスを初めて起動した場合は、次の処理が行われます。

- Telnet を無効にする。
- HTTPS サーバを無効にする。HTTP クライアントが動作する。
- SSH の有効化
- HTTPS サーバを有効にする。

（注） これは IR1101 にのみ適用され、他の IoT ルータの設定は変わりません。

初期ブートアップセキュリティの改善点

この項の内容は、次のとおりです。

デフォルトパスワード変更の適用

以前のソフトウェアバージョンでは、ユーザが新しいイネーブルパスワードの設定をバイパスできました。工場出荷時の状態へのリセット後、または工場出荷時の状態からデバイスを最初に起動すると、コンソールに次のプロンプトが表示されます。

Would you like to enter the initial configuration dialog? [yes/no]:

以前のソフトウェアバージョンでは **no** の応答が許可されており、イネーブルパスワードが空白のままのデバイスは **Router>** プロンプトになりました。この時点でルータを設定し、イネーブルパスワードが空白のまま稼働状態にすることができます。

以前のドキュメントでは、**enable password** コマンドの代わりに **enable secret** コマンドを使用することを推奨しています。これは、暗号化アルゴリズムが改善されるためでした。

17.3.1 以降では、初期のダイアログが強制的に新しいイネーブルパスワードを設定し、かつ **enable secret** コマンドを代わりに使用して適用するよう変更されました。次に、例を示します。

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: router-1

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: *******
```

```
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: **********

The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: *********
  Configure SNMP Network Management? [yes]: no

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [yes]: no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

次に、初期設定ダイアログに **no** と応答した場合の動作の例を示します。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: ********
Would you like to terminate autoinstall? [yes]: yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

最初のログイン時にイネーブルシークレットが要求され、管理者がパスワードを入力すると、管理者が入力したパスワードは常にマスクされます。管理者が脆弱なパスワードを入力すると、強力なパスワード（つまり、大文字と小文字、特殊文字、数字などの標準的な組み合わせ）を入力するように求められます。プロンプトは、管理者が強力なパスワードを入力するまで表示されます。管理者は、強力なシークレットパスワードを2回入力して、管理者が設定したシークレットを確認する必要があります。

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。