トラブルシューティング

この章は、次の項で構成されています。

トラブルシューティングの概要

ここでは、トラブルシューティングのシナリオについて説明します。

ソフトウェアに関する不具合のトラブルシューティングを行う前に、コンソールポートを使用して PC をルータに接続してください接続した PC を使用してルータのステータス メッセージを表示し、コマンドを入力して問題のトラブルシューティングを実行できます。

また、Telnet を使用してリモートから各インターフェイスにアクセスすることもできます。Telnet オプションを使用する方法では、インターフェイスが稼働していることが前提になります。

診断モードの概要

ルータは、次のような場合に、診断モードを開始するか、または診断モードにアクセスします。

- IOS プロセスの障害が原因の場合があります。あるいは、IOS プロセスで障害が発生したときにシステムがリセットすることがあります。
- **transport-map** コマンドを使ってユーザ設定のアクセス ポリシーが設定されると、ユーザは診断モードに誘導されます。
- ルータにアクセスしている間に送信ブレーク信号（**Ctrl-C** または **Ctrl-Shift-6**）が入力されると、ブレーク信号を受信したルータが診断モードを開始するように設定されている場合があります。

診断モードでは、ユーザ EXEC モードで使用可能なコマンドのサブセットを使用できます。このコマンドは、次のような場合に使用できます。

- IOS ステートなど、ルータ上のさまざまなステートを検査する。
- コンフィギュレーションの置き換えまたはロールバック。
- IOS またはその他のプロセスの再開方法を提供する。
- ルータ全体、モジュール、またはその他のハードウェア コンポーネントなどのハードウェアをリブートします。
- FTP、TFTP、および SCP などのリモート アクセス方式を使用した、ルータに対するファイル転送、またはルータからのファイル転送。

以前のルータでは、障害時に ROMMON などの制限付きアクセス方式を使用して Cisco IOS 問題を診断し、トラブルシューティングを行っていましたが、診断モードを使用すると、より広範なユーザインターフェイスを使用してトラブルシューティングできるようになります。診断モードコマンドは、Cisco IOS プロセスが正常に動作していないときでも動作可能です。また、ルータが正常に動作しているときに、ルータの特権 EXEC モードでもこれらのコマンドを使用できます。

代理店に連絡する前に

問題の原因が見つからない場合は、製品を購入した代理店に連絡し、指示を求めてください。代理店に連絡する前に、次の情報を用意してください。

- シャーシのタイプとシリアル番号
- メンテナンス契約書または保証情報
- ソフトウェアのタイプとバージョン番号

- ハードウェアを受け取った日付
- 問題点の要約
- 問題箇所を特定するために行った手順の概要

show interfaces トラブルシューティング コマンド

ルータ上のすべての物理ポートと論理インターフェイスのステータスを表示するには、**show interface** コマンドを使用します。

IR1101 は次のインターフェイスをサポートしています。

- GigabitEthernet 0/0/0
- Cellular 0/1/0
- FastEthernet 0/0/1 ～ 0/0/4
- Async 0/2/0
- Cellular 0/x/x
- LORAWAN0/x/0

コンフィギュレーション レジスタの変更

コンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ 1 PC をルータのコンソール ポートに接続します。

ステップ 2 特権 EXEC プロンプト（*router_name #*）で **show version** コマンドを入力すると、既存のコンフィギュレーション レジスタ値が表示されます（次の出力例の末尾の太字部分を参照）。

例：

```
Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1,
RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 18:08 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
```

```
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 14 hours, 36 minutes
Uptime for this control processor is 14 hours, 37 minutes
System returned to ROM by reload
System restarted at 08:47:04 GMT Mon Nov 12 2018
System image file is "bootflash:ir1101-universalk9.16.10.01.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
network-essentials     Smart License                    network-essentials


Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711861K/6147K bytes of memory.
Processor board ID FCW222700MY
3 Virtual Ethernet interfaces
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x1821


Router#
```

ステップ 3 コンフィギュレーション レジスタの設定値を記録します。

ステップ 4 ブレークの設定（コンフィギュレーション レジスタのビット 8 の値で示されます）を有効にするには、特権 EXEC モードから **config-register 0x01** コマンドを入力します。

- ブレーク有効：ビット 8 が 0 に設定されています。
- ブレーク無効（デフォルトの設定）：ビット 8 が 1 に設定されています。

自動ブートのコンフィギュレーション レジスタの設定

（注） コンフィギュレーション レジスタの変更は、高度なトラブルシューティングのみを対象としており、シスコのサポートからガイダンスがある場合にのみ行うようにしてください。

コンフィギュレーション レジスタを使用して、ルータの動作を変更できます。これには、ルータの起動方法の制御が含まれます。次のいずれかのコマンドを使用して、ROM で起動するようにコンフィギュレーション レジスタを 0x0 に設定します。

- Cisco IOS コンフィギュレーション モードで **config-reg** 0x0 コマンドを使用します。
- ROMMON プロンプトで **confreg** 0x0 コマンドを使用します。

（注） コンフィギュレーション レジスタを 0x2102 に設定すると、Cisco IOS XE ソフトウェアを自動ブートするようにルータが設定されます。

ルータのリセット

ルータをリセットする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	ブレークが無効になっている場合は、ルータの電源をオフ（O）にしてから 5 秒後に再びオン（|）にします。その後 60 秒以内に、**Break**キーを押します。端末に ROM モニタ プロンプトが表示されます。	（注） 一部の端末では、キーボードに *Break* というラベルの付いたキーがあります。使用するキーボードに Break キーがない場合は、端末に付属のマニュアルを参照して、ブレーク信号の送信方法を確認してください。
ステップ 2	break を押します。端末に次のプロンプトが表示されます。 **例**：	

	コマンドまたはアクション	目的
	`rommon 2>`	
ステップ 3	**confreg 0x142** を入力して、コンフィギュレーション レジスタをリセットします。 **例**： `rommon 2> confreg 0x142`	

ステップ 4	**reset** コマンドを入力して、ルータを初期化します。
	例：
	`rommon 2> reset`
	例：
	`--- System Configuration Dialog ---`
		ルータの電源が一度オフになってからオンになり、コンフィギュレーション レジスタが 0x142 に設定されます。ルータはブート ROM システム イメージを使用します。その状況はシステム コンフィギュレーション ダイアログで示されます。

ステップ 5	次のメッセージが表示されるまで、プロンプトに **no** で応答します。 **例**： `Press RETURN to get started!`	
ステップ 6	**Return** を押します。次のプロンプトが表示されます。 **例**： `Router>`	

ステップ 7	enable コマンドを入力して、イネーブル モードを開始します。コンフィギュレーション変更は、イネーブル モードでだけ行うことができます。
	例：
	`Router> enable`
	例：
	`Router#`
		プロンプトが特権 EXEC プロンプトに変わります。

ステップ 8	**show startup-config** コマンドを入力すると、コンフィギュレーション ファイルに保存されているイネーブル パスワードが表示されます。 **例**： `Router# show startup-config`	

次のタスク

イネーブルパスワードを回復する場合には、「変更を保存」のセクションに示す手順は実行しないでください。代わりに、「コンフィギュレーション レジスタ値」のセクションに記載されている手順を実行して、パスワード回復作業を行ってください。

イネーブル シークレット パスワードを回復する場合、**show startup-config** コマンド出力には表示されません。「パスワードのリセットと変更の保存」セクションに記載されている手順を実行して、パスワード回復作業を完了させてください。

失われたパスワードの復旧

失われたイネーブルパスワードまたはイネーブルシークレットを回復するには、次の作業を行います。

1. コンフィギュレーション レジスタの変更
2. ルータのリセット
3. パスワードをリセットし、変更を保存します（イネーブル シークレット パスワードを忘れた場合のみ）。
4. コンフィギュレーション レジスタ値をリセットします。
5. **write erase** を実行した場合、またはリセット ボタンを使用した場合は、ライセンスを追加する必要があります。

```
IR1101#config term
IR1101#license smart reservation
```

（注） パスワードを回復できるのは、コンソール ポートを使用してルータに接続している場合だけです。Telnet セッション経由では実行できません。

ヒント イネーブル シークレット パスワードの変更方法のさらに詳しい情報については、Cisco.com の「Hot Tips」を参照してください。

パスワードのリセットと変更の保存

パスワードをリセットして、変更を保存するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。 例： `Router# configure terminal`	
ステップ 2	**enable secret** コマンドを入力して、ルータのイネーブル シークレット パスワードをリセットします。 例： `Router(config)# enable secret password`	
ステップ 3	**exit** を入力して、グローバル コンフィギュレーション モードを終了します。 例： `Router(config)# exit`	
ステップ 4	設定変更を保存します。 例： `Router# copy running-config startup-config`	

パスワードリカバリの無効化

No Service Password-Recovery は、Cisco IOS プラットフォームに依存しない機能/CLI で、Cisco IOS-XE デバイスで使用できます。No Service Password-Recovery セキュリティ機能を有効にすると、コンソールアクセス権を持つすべてのユーザが、ブートアップ時にブレークシーケンス（Control+C）を使用して rommon を開始できなくなります。

（注） この機能を有効にする前に、フラッシュ内に有効な Cisco IOS イメージが存在することを確認します。これを行わないと、ルータがブートループに入ります。システムに **no service password recovery** がない場合は、ハード電源リセットボタンが無効になります。

次のイベントにより、ルータは標準の IOS-XE 動作として rommon モードになります。

- config-reg 設定は手動起動
- ユーザが工場出荷時のデフォルトオプションにリセットすることを選択

詳細情報と設定手順については、次を参照してください。https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-sy/sec-usr-cfg-15-sy-book/sec-no-svc-pw-recvry.html

サービス パスワード リカバリ アップデートでのコンフィグレジスタの変更の問題

サービスパスワードリカバリが無効になっている場合、コンフィグレジスタを変更できず、0x01 でスタックされます。この問題は、IR1101 ルータで見つかりました。詳細については、テクニカルノート『Understand Configuration Register Usage on all Routers』を参照してください。

コンフィギュレーション レジスタ値のリセット

パスワードの回復または再設定を行った後にコンフィギュレーション レジスタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。 例： `Router# configure terminal`	
ステップ 2	**configure register** コマンドと、記録しておいた元のコンフィギュレーション レジスタ値を入力します。 例： `Router(config)# config-reg value`	
ステップ 3	**exit** を入力して、コンフィギュレーション モードを終了します。 例： `Router(config)# exit`	（注） 忘れたイネーブル パスワードを回復する前に使用していたコンフィギュレーションに戻るには、コンフィギュレーションの変更を保存せずに、ルータを再起動してください。
ステップ 4	ルータを再起動し、回復したパスワードを入力します。	

コンソール ポートのトランスポート マップの設定

このタスクでは、ルータ上のコンソール ポート インターフェイスにトランスポート マップを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**transport-map type console** *transport-map-name* 例： `Router(config)# transport-map type console consolehandler`	コンソール接続を処理するためのトランスポート マップを作成して名前を付け、トランスポート マップ コンフィギュレーション モードを開始します。
ステップ 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] 例： `Router(config-tmap)# connection wait none`	コンソール接続を処理する方法を、このトランスポート マップで指定します。 • **allow interruptible**：コンソール接続はCisco IOS VTY回線が使用可能になるのを待機します。また、ユーザはCisco IOS VTY 回線が使用可能になるのを待機しているコンソール接続に割り込むことにより、診断モードを開始できます。これがデフォルト設定です。 （注） **Ctrl+C** キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。 • **none**：コンソール接続はただちに診断モードを開始します。

ステップ 5	（任意） **banner** [**diagnostic** | **wait**] *banner-message*
	例：
	`Router(config-tmap)# banner diagnostic X`
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		（オプション）診断モードを開始しているユーザ、またはコンソール トランスポート マップ設定のために Cisco IOS VTY 回線を待機しているユーザに表示されるバナー メッセージを作成します。
		• **diagnostic**：コンソール トランスポート マップ設定のために診断モードに誘導されたユーザに表示されるバナー メッセージを作成します。
		（注） **Ctrl+C** キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。

	コマンドまたはアクション	目的
		• **wait**：Cisco IOS VTY が使用可能になるのを待機しているユーザに表示されるバナー メッセージを作成します。 • *banner-message*：同じデリミタで開始および終了するバナー メッセージ。
ステップ 6	**exit** 例： `Router(config-tmap)# exit`	トランスポートマップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。
ステップ 7	**transport type console** *console-line-number* **input** *transport-map-name* 例： `Router(config)# transport type console 0 input consolehandler`	トランスポートマップで定義された設定をコンソール インターフェイスに適用します。 このコマンドの *transport-map-name* は、**transport-map type console** コマンドで定義された *transport-map-name* と一致する必要があります。

例

次に、コンソール ポートのアクセス ポリシーを設定し、コンソール ポート 0 に接続するためにトランスポート マップを作成する例を示します。

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

コンソール ポート、SSH、および Telnet の処理設定の表示

コンソール ポート、SSH、および Telnet の処理設定を表示するには、次のコマンドを使用します。

- **show transport-map**
- **show platform software configuration access policy**

トランスポート マップ設定を表示するには、**show transport-map** コマンドを使用します。

show transport-map [**all** | **name** *transport-map-name* | **type** [**console**]]

このコマンドは、ユーザ EXEC モードまたは特権 EXEC モードで使用可能です。

例

次に、ルータで設定されたトランスポートマップの例（コンソール ポート（consolehandler）を示します。

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type console
Transport Map:
Name: consolehandler


REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

着信コンソール ポート、SSH、および Telnet 接続の処理に関する現行設定を表示するには、**show platform software configuration access policy** コマンドを使用します。このコマンドの出力には、各接続タイプ（Telnet、SSH、およびコンソール）の現在の待機ポリシーと、現在設定されているバナーの情報が示されます。

show transport-map コマンドとは異なり、**show platform software configuration access policy** コマンドは診断モードで使用可能です。このため、トランスポートマップ設定情報が必要であるにもかかわらず Cisco IOS CLI にアクセスできない場合に、このコマンドを入力できます。

例

次に、**show platform software configuration access policy** コマンドの例を示します。

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

factory reset コマンドの使用

factory reset コマンドは、追加されたルータまたはスイッチ上の特定の顧客データをすべて削除するために使用されます。設定、ログ ファイル、ブート変数、およびコア ファイル形式のデータが対象です。

factory-reset all コマンドは、bootflash、nvram、rommon 変数、ライセンス、およびログを消去します。

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
 *Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory
Reset.

***Return to ROMMON Prompt
```

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**

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。