Catalyst Center SWIM機能のトラブルシューティング

内容

はじめに

このドキュメントでは、SWIMのトラブルシューティングについて説明し、実際のチェック、クリアな回復手順、およびエスカレーション前の確認に必要な情報を示します。

2. 目的

- SWIMワークフローが失敗した場所を見つけるのに役立ちます
- GUIの状態とデバイスの状態の両方の確認に役立つ
- 安全な回復手順の案内
- エスカレーションの前に適切な情報を収集

3. 対象範囲

- イメージのインポートの問題
- ゴールデンイメージとコンプライアンスの問題
- イメージ配布エラー
- アクティベーションとブートの問題
- スタックおよびHAアップグレードの問題
- アップグレード後の検証
- SWIMタスクのスタックに関するデータベースチェック

4. 対象者

- TACエンジニア
- エスカレーションエンジニア

5. 前提・注意事項

この文書では、「CatC」はCisco Catalyst Center(CatC)、「SWIM」はSoftware Image Management(SWIM)を意味します。

変更を行う前に、コンソールまたは管理アクセスが使用可能であること、ターゲット・イメージが正しいこと、バックアウト・パスが存在すること、デバイスで別のインストール操作がまだ実行されていないこと、および変更が承認されていることを確認します。

6. このガイドの使用方法

1. GUIのセクションから始めて、タスクフローと影響を理解します。
2. CLIのセクションに移動し、実際のデバイスの状態を確認します。
3. failure-domainセクションを使用して、問題を絞り込みます。
4. 最もリスクの低いリカバリアクションを最初に適用します。
5. 再試行する前にTACワークフローに進んでください。

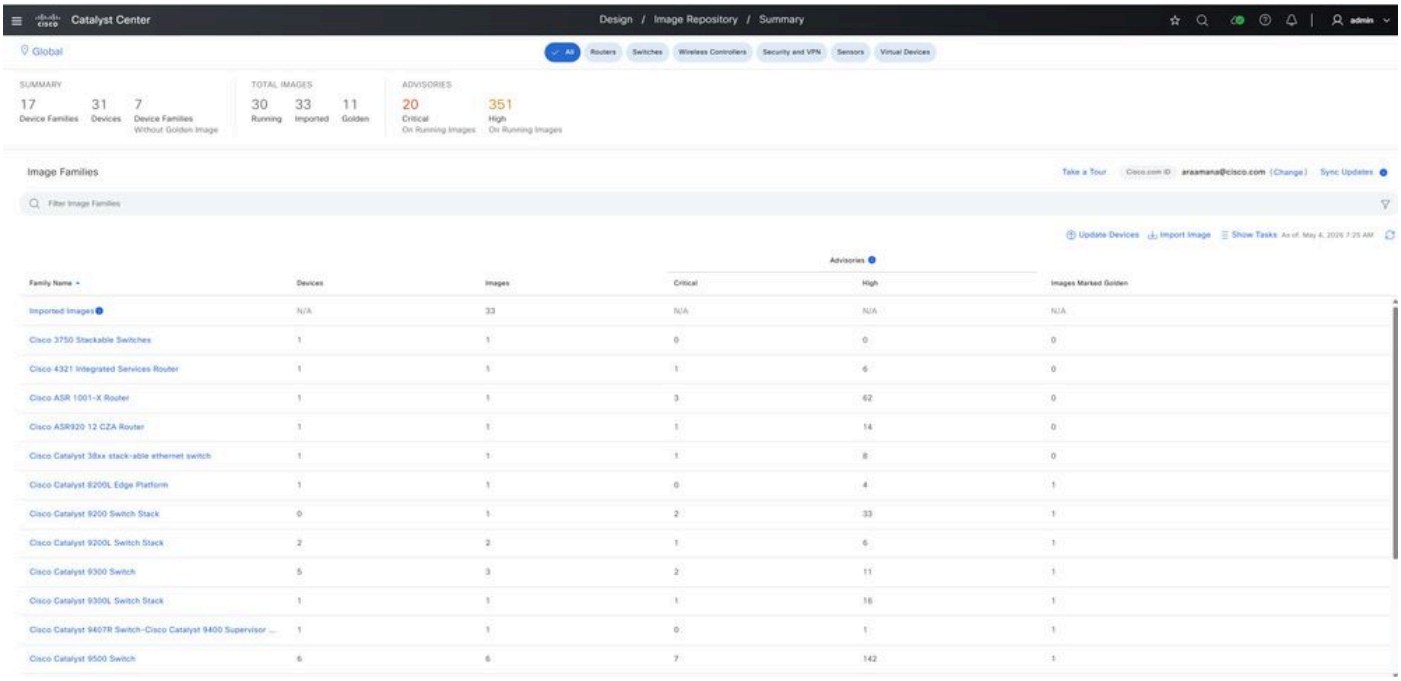
7. GUIワークフローおよびリポジトリ機能

CLIまたはデータベースチェックに移行する前に、GUIに役立つコンテキストが表示されます。

7.1イメージの推奨事項とセキュリティアドバイザリレビュー

この確認は、イメージ配布またはアクティベーションのトラブルシューティングを行う前に最初に行うチェックの1つでなければなりません。

- Cisco-recommended images for the device familyを参照してください(Design > Image Repository)



- 選択したイメージがプラットフォームファミリに一致するかどうかを確認します。

- 選択したイメージがプラットフォームファミリと一致することを確認し、[プロビジョニング] > [インベントリ]に表示されたデバイスファミリとPIDを、[設計] > [イメージリポジトリ]に表示されたイメージファミリと比較します

- 現在のイメージとターゲットイメージのセキュリティアドバイザリを確認する

- Design > Image Repositoryに移動し、必要なデバイスファミリを選択します。シスコが推奨するソフトウェアバージョンを確認し、現在稼働中のイメージと比較します。Provision > InventoryのデバイスファミリとPIDを、Image Repositoryに表示されているイメージファミリと比較して、プラットフォームの互換性を検証します。アップグレードの関連性、セキュリティの危険性、およびソフトウェアの通貨を判断するには、現在のイメージとターゲットイメージの両方のセキュリティアドバイザリを確認します。

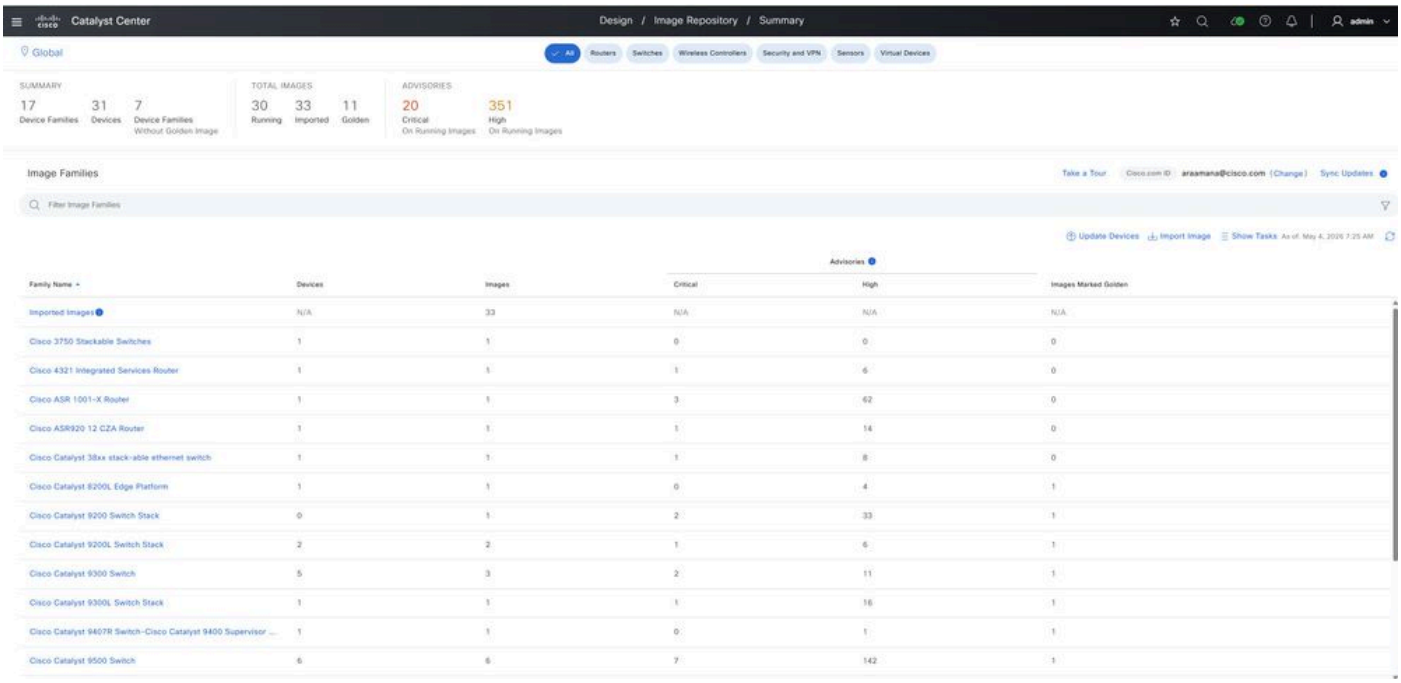
- 実行イメージが古いか、サポートされていないか、または既知のセキュリティ問題に該当するかを確認します。

- Design > Image Repositoryで現在のイメージを確認し、推奨イメージおよび関連するセキュリティアドバイザリと比較して、実行されているソフトウェアが古いか、サポートされていないか、または既知のセキュリティ問題の影響を受けているかどうかを判断します。

推奨されるTACレビューフロー：

1. Design > Image Repositoryを開きます。

2. 正しいデバイスファミリを選択します。
3. そのプラットフォーム用に表示された推奨イメージを確認します。
4. 現在実行中のイメージを推奨イメージと比較します。
5. リストされているアドバイザリで、重大度、影響、ケースとの関連性を確認します。
6. ターゲットイメージがすでにインポートされ、割り当てに使用できるかどうかを確認します。
7. ターゲットイメージが必要なスコープに対してゴールデンとしてマークされているかどうかを確認します。



TACによる確認内容：

- この推奨事項は、正確なプラットフォームファミリに適用されます
- 選択されたイメージは別のハードウェアファミリ用ではありません
- イメージの選択は、サイトで承認されているソフトウェアのベースラインと一致している
- アップグレードの決定は、セキュリティアドバイザリデータによってサポートされます

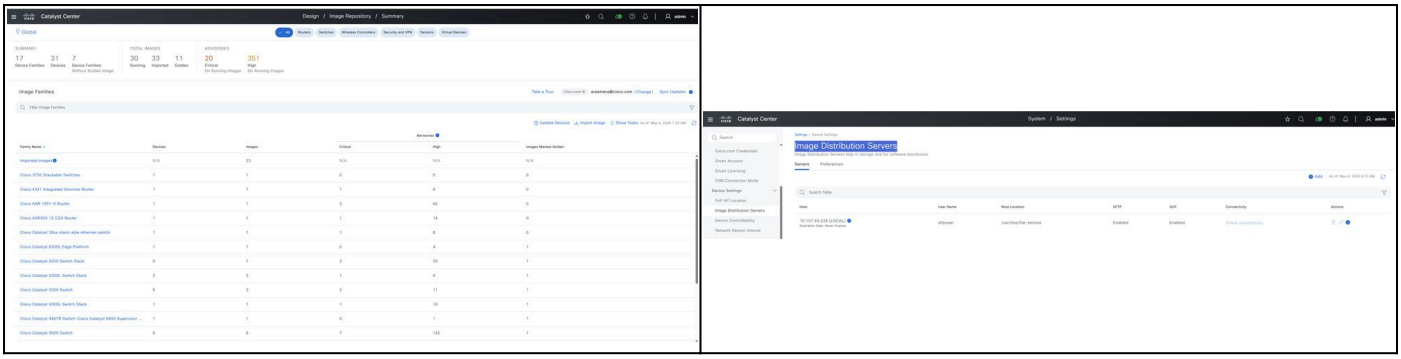
この手順が重要な理由：この手順を実行すると、イメージ選択の誤りを早く検出できます。また、アップグレードがコンプライアンス、ライフサイクルの調整、セキュリティアドバイザリのいずれによって行われたかを説明できます。

7.2イメージのインポートワークフロー

- Design > Image Repositoryの順に選択します。
- [イメージを読み込み]をクリックします

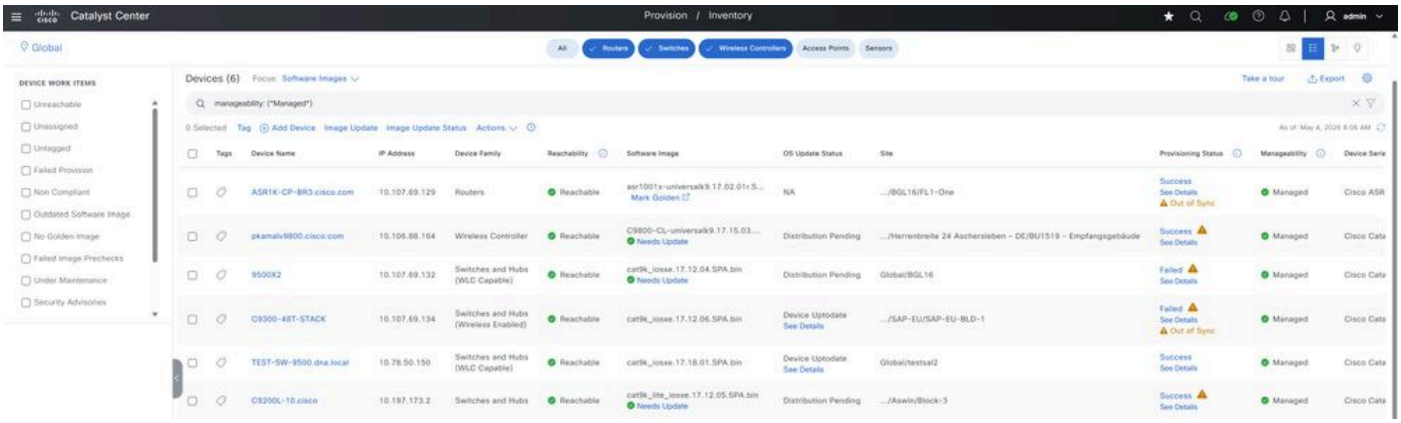
- Cisco、ローカルファイル、URLなどのソースを選択します
- インポートを完了し、メタデータが正しいことを確認します

FIPSモードが有効になっている場合は、プラットフォームのセキュリティ制御によってURLベースのイメージインポートを制限する必要があります。このような場合は、Cisco.comやローカルファイルのアップロードなどのサポートされているインポート方法を使用し、インポート後にイメージメタデータとチェックサムが正しく入力されていることを確認します。



7.3ゴールデンイメージとアップグレードの準備

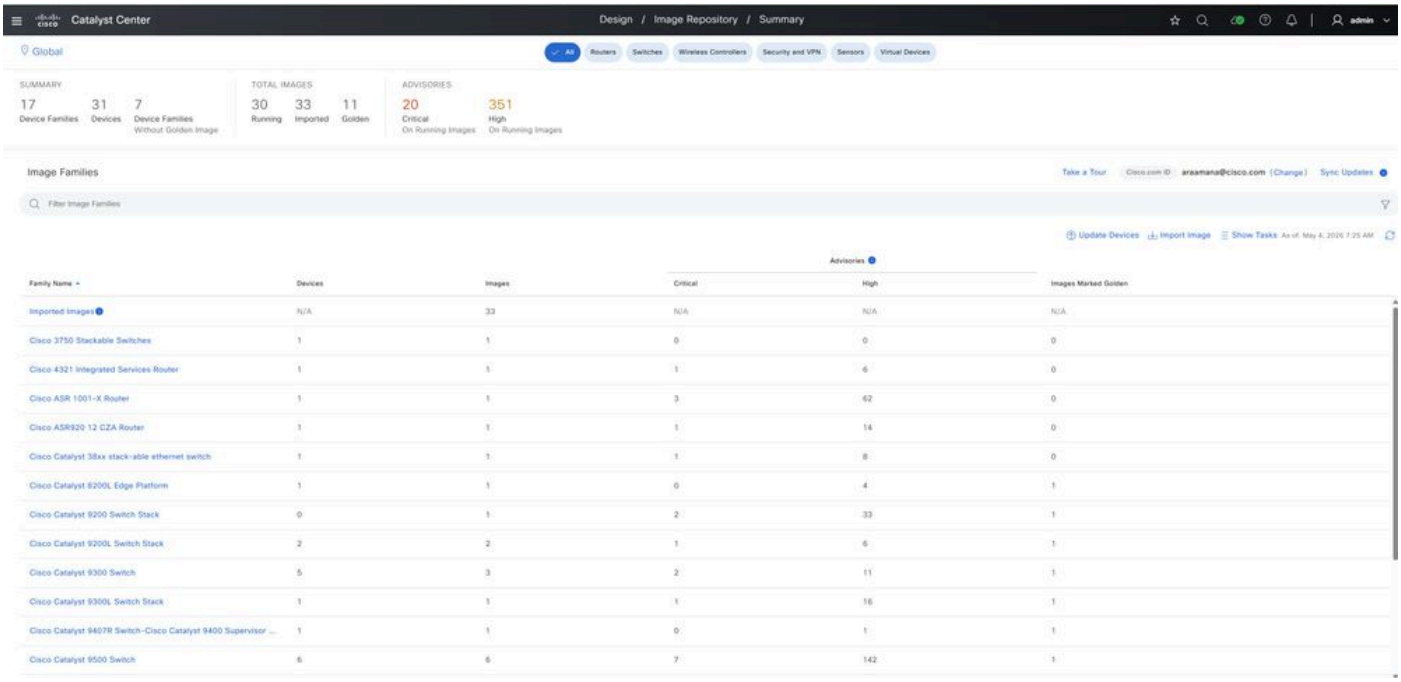
- イメージが正常にインポートされたことを確認します。
- 必要に応じて、イメージがゴールデンとしてタグ付けされていることを確認します
- サイトとデバイスファミリの割り当てが正しいことを確認します。
- Provision > Inventoryでデバイスが管理状態になっていることを確認します。



7.4リモート配布サーバの認識

リモート配布サーバがSystem > Settings > Device Settings > Image Distribution Serversの順に選択して設定されている場合は、サービスリクエストの最初から分析に含めてください。これは、転送方式、転送タイミング、ステージング動作、およびイメージ配信中の実際の障害ポイントに

影響を与える可能性があります。



TACによるチェック内容：

1. 影響を受けるサイトに対してリモート配布サーバーが構成されているかどうか
2. 使用されている転送プロトコル（SCP、HTTPS、SFTPなど）
3. ターゲットデバイスがそのサーバに到達できるかどうか
4. 正しいイメージがリモートサーバにステージングされているかどうか
5. 問題が1つのリモートサイトに影響を与えるか、同じサーバを使用する複数のサイトに影響を与えるか

なぜこれが重要なのか。

リモート配布サーバを使用している場合、イメージパスは単純なコントローラ間転送ではなくなります。障害の原因は、デバイス自体ではなく、外部サーバ、プロトコルのプリファレンス、到達可能性、イメージステージング、またはサーバ側のアベイラビリティにあります。

推奨されるTAC検証フロー：

1. 影響を受けるサイトがリモート配布サーバを使用するように設定されているかどうかを確認します。
2. 選択した転送プロトコルを確認します。
3. ターゲットイメージが使用可能で、正しくステージングされていることを確認します。
4. デバイス、Catalyst Center、およびリモート配布サーバ間のネットワーク到達可能性を確認します。

5. 配布を再試行する前に、転送に関連するタスクの失敗と口グを確認してください。

注意が必要なTACの一般的な問題：

1. イメージが誤ったサーバでステージングされているか、まったくステージングされていない
2. サーバ設定とデバイス機能の間のプロトコルの不一致
3. リモートサイトの到達可能性の問題
4. サーバ応答遅延またはWANの不安定性による転送タイムアウト

8. キャプチャする最小データ

詳細なトラブルシューティングを行う前に、次の情報を収集します。

- Catalyst CenterタスクID:表示されている場合は、メインのSWIMジョブとすべての子タスクのタスクIDをキャプチャします。これは、GUIのアクティビティ、ログ、およびデータベースの状態を関連付けるための主要なリファレンスです。
- 正確なエラーメッセージ：完全なエラーメッセージを、GUIで表示されているとおりに記録します。短くしないでください。少しの文言の違いでも、実際の障害パスを特定するのに役立ちます。
- ホスト名と管理IP:デバイスのホスト名と管理IPを記録して、タスクデータ、インベントリの状態、およびデバイスログが正しく一致するようにします。
- プラットフォームモデルとPID:正確なハードウェアモデルとPIDを確認します。これは、イメージの互換性、ゴールデンイメージマッピング、およびアップグレードパスの検証にとって重要です。
- 現在のバージョンとターゲットバージョン：デバイスで現在実行されているソフトウェアバージョンと、アップグレードが計画されているバージョンをメモします。これは、イメージが実際に変更される前または後にタスクが失敗したかどうかを確認するのに役立ちます。
- ソフトウェアモード（既知の場合）:デバイスがインストールモードを使用しているか、またはバンドルモードを使用しているかを記録します（情報がある場合）。これは、アクティブ化の動作と回復手順に直接影響します。
- デバイスがスタンドアロン、スタック、またはHAのいずれであるか：スタックデバイスとHAデバイスはスタンドアロンデバイスとは異なる方法で失敗することが多く、追加のチェックが必要であるため、導入タイプをキャプチャします。
- ビジネスへの影響とメンテナンス時間帯の詳細：問題がサービスに影響するかどうか、影響を受けるユーザまたはサイトの数、および作業が承認されたメンテナンス時間帯に行われているかどうかを記録します。

推奨されるTAC収集順序：

1. タスクIDと正確なエラーをキャプチャします。

2. デバイスIDとプラットフォームの詳細をキャプチャします。
3. 現在のバージョン、ターゲットバージョン、およびソフトウェアモードを記録します。
4. デバイスがスタンドアロン、スタック、またはHAのいずれであるかを記録します。
5. ビジネスへの影響とメンテナンス時間帯のステータスを記録します。

これが重要な理由：この情報を早期に収集することにより、エスカレーション中の前後関係が減少し、TACが問題がイメージの選択、タスクオーケストレーション、プラットフォームの互換性、またはデバイスの状態に関連しているかどうかを判断するのに役立ちます。

9. Catalyst Centerの検証

GUIで次の項目を確認します。

- タスクの詳細と子タスクの結果：親タスクと子タスクのエントリを確認して、ワークフローが停止した場所を正確に把握します。これにより、インポート、配布、アクティブ化、およびアップグレード後の問題を分離できます。
- Failure message and failure time:正確なエラーメッセージとタイムスタンプをキャプチャします。これにより、GUIイベントをデバイスログ、SWIMログ、およびデータベースタスクレコードと照合できます。
- イメージ・リポジトリ・エントリおよびメタデータ：ターゲット・イメージがリポジトリに存在し、バージョン、ファミリおよびメタデータが完了していることを確認します。リポジトリエントリの一部または誤りにより、割り当てと配布の問題が発生する可能性があります。
- ゴールデンイメージの割り当て：ゴールデンイメージの割り当てが、目的のサイト、ロール、およびデバイスファミリに一致していることを確認します。割り当てが正しくないと、コンプライアンスの不一致が発生したり、更新ワークフロー中に間違ったイメージが選択される可能性があります。
- インベントリの到達可能性：デバイスが現在到達可能であり、管理対象の状態として引き続き表示されていることを確認します。インベントリの状態が低下している場合は、タスクを再試行する前に、まずそれを修正してください。
- タスクの前後のコンプライアンスステータス：アップグレードを試行する前と失敗した後で、コンプライアンスの状態を比較します。これは、イメージが実際に変更されたかどうか、同期が古くなっているかどうか、またはアクティブ化の前に障害が発生したかどうかを示します。
- タスクがスタックまたは遅延した場合のプラットフォームの状態：Catalyst Centerで、タスクが保留状態、遅延状態、または不整合のままになっている場合のシステムとアプリケーションの状態を確認します。これにより、問題がデバイス側ではなくコントローラ側にあるかどうかを特定できます。
- ソフトウェアデータが古くなったように見える場合のInventory再同期オプション：デバイスは正常に戻ったが、GUIに表示されるソフトウェアバージョンが古い場合は、ケースをアップグレードの失敗として扱う前にInventory再同期を使用します。
- 再試行によって動作が変更されたかどうかを確認するタスク履歴：同じデバイスまたはサイ

トに対する以前のタスク試行を確認します。これにより、失敗が一貫しているか、断続的であるか、または再試行間に行われた変更の影響を受けているかどうかを確認できます。

推奨されるTAC検証順序：

1. 失敗したタスクを開き、親タスクと子タスクの詳細を確認します。
2. 正確な障害テキストと障害発生時刻をキャプチャします。
3. リポジトリ内のターゲットイメージエントリを検証します。
4. ゴールデンイメージの割り当てとスコープを確認します。
5. 現在のインベントリの到達可能性と管理容易性の状態を確認します。
6. 失敗した試行の前後のコンプライアンスステータスを比較します。
7. 再試行する前に、プラットフォームの状態、インベントリの同期状態、タスクの履歴を確認してください。

これが重要な理由：これらのチェックにより、TACは、問題の原因がイメージの選択、割り当て、コントローラタスク処理、インベントリの同期、またはデバイス自体のいずれにあるのかを判断できます。

10. デバイス側のCLIチェック

プラットフォームモードとソフトウェアモードに適合するコマンドのみを実行します。

これらのインストール関連のコマンドは、SWIMのアップグレード分析の際に特に役立ちます。show tech installcommandは、インストールプロセスの幅広い技術的スナップショットを提供し、通常、レビューまたはエスカレーションの対象となるインストール関連の全体的な証拠をキャプチャするために使用されます。show platform software install-manager switch X R0 operation history detailsコマンドは、特定のスタックメンバーに関するインストールマネージャ操作の詳細な履歴を表示し、完了した手順とそのプロセスが失敗した場所を確認するのに役立ちます。show platform software install-manager switch X R0 operation current detailsコマンドは、そのスイッチのライブインストールステータスを表示し、アップグレードが停止しているように見えるか、まだ実行している場合に役立ちます。request platform software trace archivecommandは、より深い分析のためにプラットフォームソフトウェアトレースデータを収集し、request platform software trace slot switch X archivecommandは、特定のスタックメンバーのために同じトレースデータを収集する。これらのコマンドを組み合わせることで、チームはインストール中に何が起こったのか、今何が起こっているのか、さらなる分析のためにどのような証拠を収集する必要があるかを理解できます。

show tech install（登録ユーザ専用）
show platform software install-manager switch X R0操作履歴の詳細（スタック）
show platform software install-manager switch X R0動作の現在の詳細（スタック）
要求プラットフォームソフトウェアトレースアーカイブ

要求プラットフォームソフトウェアトレーススロットスイッチXアーカイブ（スタック）

10.1コア識別コマンド

show version

show inventory

show platform

show boot

show running-config | include boot system（ブートシステムを含める）

show startup-config | include boot system（ブートシステムを含める）

ファイルシステムの表示

dir flash:

dir bootflash:

これらのコマンドを使用して、現在のバージョン、ブート設定、および使用可能なストレージを確認します。

10.2インストールおよびパッケージ状態コマンド

インストールの概要を表示

show install active

コミットされたインストールの表示

インストールログの詳細の表示

インストール要求の表示

これらのコマンドを使用すると、以前のインストールがまだ実行中か、不完全か、またはコミットされていないかを確認できます。

10.3ロギングおよび障害の証拠

show logging

show logging | include INSTALL|install|BOOT|boot|ERROR|FAIL|ROMMON

show archive log config all（アーカイブログの設定をすべて表示）

show reload（隠しコマンド）

show tech-support

10.4スタックおよびHAコマンド

showスイッチ

show switch detail（隠しコマンド）

show redundancy

show platform software status control-processor brief

show platform software packageのステータス

10.5到達可能性とリソースのチェック

ping <ゲートウェイまたは管理ピア>

show ip interface brief

show interfaces status

show processes cpu sorted | exclude 0.00

show processes memory sorted

11. 障害ドメイン別トラブルシューティング

11.1イメージ配布の失敗

ファイルシステムの表示

dir flash:

dir bootflash:

show logging | include SCP|SFTP|HTTP|TFTP|copy|transfer|flash

show processes cpu sorted | exclude 0.00

十分な空き領域があることを確認し、管理パスが安定しているかどうかを確認し、古いファイルが使用されていないことを確認した後にのみ、古いファイルを削除します。

GUI操作：失敗したタスクを開き、デバイスが引き続き管理されていることを確認し、イメージがリポジトリにまだ存在することを確認し、リモート配布サーバーが使用中かどうかを確認し、ストレージ、資格情報、および転送パスが良好に見えた後にのみ再試行します。

11.2アクティベーションが失敗し、デバイスが古いイメージをブートする

show version

show boot

show running-config | include boot system（ブートシステムを含める）

show startup-config | include boot system（ブートシステムを含める）

インストールの概要を表示

ブート変数が引き続き古いイメージを指しているかどうかを確認します。必要に応じてブートパスを修正し、リロードの前に設定を保存します。

terminalno boot systemboot system flash:<target-image.bin>endwrite memoryshow bootを設定する

GUIアクション：タスクタイムラインを確認し、リロード後にデバイスが復帰したかどうかを確認し、GUIバージョンが古い場合はインベントリ同期を実行し、再試行する前にアクティブ化チェックとクリーンアップ設定を確認します。

11.3インストールモードが不完全またはスタックしている

インストールの概要を表示

show install active

コミットされたインストールの表示

インストールログの詳細の表示

show logging | include install|INSTALL

パッケージがすでにアクティブで、コミットされていないかどうかを確認します。現在の状態を理解するまで、別のインストールを開始しないでください。

install commit

11.4デバイスがブートループに入る

最初に、正常なイメージがローカルで使用できるかどうかを確認し、そのプラットフォームに対して承認されているROMMON回復方法を使用します。

dir flash:

boot flash:<known-good-image.bin>（正常なイメージが見つからない場合）

show version

show boot

configure terminal

no boot system

boot system flash:<known-good-image.bin>

end

write memory

11.5スタックメンバーのバージョンの不一致

showスイッチ

show switch detail（隠しコマンド）

show version

dir flash:

インストールの概要を表示

show logging | include switch|version|インストール

すべてのメンバが存在することを確認し、すべてのメンバ上でイメージの可用性を確認して、完全なスタックが正常な場合にのみ再試行してください。

11.6アップグレード後に到達可能だが準拠していない

show version

show inventory

show running-config | include boot system（ブートシステムを含める）

デバイスのバージョンが正しい場合は、アップグレードの失敗として処理する前に、古いインベントリデータまたはコンプライアンスデータが疑われます。

GUIアクション：デバイスレコードを更新し、コンプライアンスを再実行し、ゴールデンイメージマッピングがまだ正しいことを確認し、タスク履歴を確認して予想されるターゲットバージョンを確認します。

12. 回復手順

12.1安全なストレージクリーンアップ

dir flash:

dir bootflash:

/force flash:<unused-image.bin>を削除します

delete /force /recursive flash:<unused-package-directory>

12.2ブート変数の修正

show boot

configure terminal

no boot system

boot system flash:<target-image.bin>

end

write memory

show boot

12.3制御された準備後の手動リロード

reload

12.4アクティブなパッケージが正しいときのコミットのインストール

インストールの概要を表示

install commit

コミットされたインストールの表示

12.5手動リカバリ後の検証

show version

show boot

インストールの概要を表示

show logging | tail（ログの表示）

show ip interface brief

12.6 GUIによるリカバリの検証

1. デバイスが管理対象であり、インベントリで到達可能であることを確認します。
2. バージョンが古い場合にインベントリ同期を実行する
3. コンプライアンスの再実行

4. イメージリポジトリとゴールデンマッピングがまだポリシーに一致していることを確認する
5. 未完了のアップグレードタスクが開いたままになっていないことを確認します

13. TACワークフロー

このワークフローは、メインGUIおよびCLIによるチェックの後に使用します。ライブTACケースの作業シーケンスとして扱います。

13.1障害が発生した場所の特定

目的：問題の起点がCatalyst Center、転送パス、またはデバイスのいずれにあるかを決定する

作業チェック：タスクの詳細、タイムスタンプ、インベントリ状態、およびデバイスの到達可能性を確認します。コントローラ側の障害を、可能な限り早期に転送障害やデバイス側の障害から切り離します。

判断：イメージがデバイスに到達する前にタスクが失敗した場合は、インベントリ、クレデンシャル、リポジトリの状態、転送パスに注目します。イメージは正常にコピーされたがアクティブ化が失敗した場合は、ブート変数、インストール状態、およびデバイスログに移動します。

13.2正確なエラーと時間のキャプチャ

目的：問題のないスケジュールを作成する

キャプチャ：正確なGUIエラーテキスト、タスクID、失敗のタイムスタンプ、および子タスクの詳細（可能な場合）を記録します。

これが重要な理由：データはGUIイベントとデバイスログ、SWIMログ、およびデータベースレコードを一致させる必要があります。

13.3影響範囲の測定

目的：これが単一デバイスの問題か、より広範なプラットフォームの問題かを判断する

チェック：問題が1つのデバイス、1つのスタック、1つのサイト、1つのプラットフォームファミリ、または環境全体にわたる多数のデバイスに影響するかどうかを判断します。

判断：同じ障害が複数のデバイスで発生している場合は、1つのデバイスを責める前に、イメージ品質、プラットフォームの互換性、リポジトリの状態、クレデンシャル、またはコントローラ側のタスク処理に問題があると考えられます。

13.4 SWIMワークフローが到達した距離の確認

目的：正常に完了した最後の段階を見つけます。

トラック：イメージのインポート、割り当て、配布、アクティベーション、リロード、アップグレード後の同期を通じてワークフローを実行します。

これが重要な理由：これにより、すでに動作している手順の繰り返しを行わずに、実際の障害ポイントに集中できます。

13.5イメージがデバイスに到達したかどうかを確認する

目的：転送ステージが本当に完了したかどうかを確認する

確認：イメージがflash：またはbootflash：にあるかどうかを確認し、十分な空き容量があることを確認し、ファイルが完全であることを確認し、イメージが目的のプラットフォームに一致することを確認します。

判断：イメージがない場合は、転送のトラブルシューティングを続行します。イメージが存在する場合は、アクティベーション、ブート選択、パッケージの状態、またはアップグレード後の検証に移行します。

13.6障害の発生時期の判断

目的：タイムラインの正しいポイントに障害を配置する

分類：問題をリロード前、リロード中、またはリロード後のいずれかのタイミングに切り分けます。

判断：リロード前に障害が発生した場合は、インストールロジック、ブート設定、およびタスクオーケストレーションに焦点を当てます。リロード中にこの問題が発生した場合は、コンソール出力、リロードの原因、およびブート動作を確認します。リロード後に発生した場合は、再検出、コンプライアンスの同期、スタックの健全性、およびサービスの回復に重点を置きます。

13.7再試行の前のデバイス状態の確認

目的：何かを再度実行する前に、デバイスが安定していることを確認する

確認：ソフトウェアモードが理解されていること、ブート変数が正しいこと、ストレージが正常であること、インストール状態が不完全でないこと、スタックまたはHA状態が正常であること、以前のインストール操作がまだアクティブでないことを確認します。

終了基準：これらのチェックがすべてクリアされるか、処理を続行する理由が文書化されるまで、再試行しないでください。

13.8最もリスクの低いリカバリステップを最初に使用する

目的：ケースを前に進めながらリスクを軽減する

最初に、インベントリの更新、コンプライアンスの再実行、ログの確認、ブート変数の修正、またはアクティブ化がすでに成功した場合のパッケージのコミットを行います。

ガイダンス：通常のチェックでタスクが古くなっており、デバイスがワークフローでアクティブでなくなっている場合を除き、データベースの更新や強制クリーンアップにジャンプしないでください。

13.9状態がクリアになった後にのみ再試行

目的：次の試行の前に明確な判断ポイントを設定する

次の場合のみ再試行する：現在の問題が認識され、デバイスが正常で、競合するタスクがまだ開いていないこと、イメージと割り当てが正しいこと、および回復の変更が保存および検証されていること。

判断：これらの条件が満たされない場合は、再試行パスを停止し、収集した証拠を使用して

エスカレーションに進みます。

14. エスカレーションパッケージのチェックリスト

- Catalyst Centerタスクの詳細
- インポート、配布、アクティブ化、リロードのタイムスタンプ
- show version
- show boot
- インストールの概要を表示
- インストールログの詳細の表示
- show logging
- dir flash：またはdir bootflash:
- show switchまたはshow redundancy when relevant
- デバイスがROMMONに入ったか、またはブートループになった場合のコンソール出力
- すべての回復操作は既に試行されています

15. デバイスに役立つコマンドリファレンス

```
show version
show boot
show install summary
show install log detail
show logging
show switch
show redundancy
dir flash:
dir bootflash:
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。