

# Catalyst Center SWIM 기능 문제 해결

## 목차

---

[소개](#)

[2. 목적](#)

[3. 범위](#)

[4. 대상](#)

[5. 가정 및 참고 사항](#)

[6. 설명서 사용 방법](#)

[7. GUI 워크플로 및 저장소 기능](#)

[7.1 이미지 권장 사항 및 보안 자문 검토](#)

[7.2 이미지 가져오기 워크플로](#)

[7.3 골든 이미지 및 업그레이드 준비](#)

[7.4 원격 배포 서버 인식](#)

[8. 캡처할 최소 데이터](#)

[9. Catalyst Center 검증](#)

[10. 디바이스측 CLI 확인](#)

[10.1 코어 식별 명령](#)

[10.2 설치 및 패키지 상태 명령](#)

[10.3 로깅 및 실패 증거](#)

[10.4 스택 및 HA 명령](#)

[10.5 연결성 및 리소스 확인](#)

[11. 장애 도메인별 문제 해결](#)

[11.1 이미지 배포 실패](#)

[11.2 정품 인증에 실패하고 디바이스에서 기존 이미지를 부팅합니다.](#)

[11.3 설치 모드 불완전 또는 고착](#)

[11.4 디바이스가 부팅 루프를 시작합니다.](#)

[11.5 스택 멤버 버전 불일치](#)

[11.6 업그레이드 후 연결 가능하지만 비준수](#)

[12. 복구 절차](#)

[12.1 안전 스토리지 정리](#)

[12.2 부트 변수 수정](#)

[12.3 준비 제어 후 수동 다시 로드](#)

[12.4 활성 패키지가 올바르면 설치 커밋](#)

[12.5 수동 복구 후 검증](#)

[12.6 GUI 복구 검증](#)

[13.1 장애가 시작된 위치 확인](#)

[13.2 정확한 오류 및 시간 캡처](#)

[13.3 영향 범위 측정](#)

[13.4 SWIM 워크플로 도달 범위 확인](#)

[13.5 이미지가 장치에 도달했는지 확인](#)

---

[13.6 장애 발생 시기 결정](#)

[13.7 재시도 전에 디바이스 상태 확인](#)

[13.8 가장 위험도가 낮은 복구 단계를 먼저 사용하십시오.](#)

[13.9 상태가 클리어 후에만 다시 시도](#)

[14. 에스컬레이션 패키지 체크리스트](#)

[15. 장치 유용한 명령 참조](#)

---

## 소개

이 문서에서는 SWIM 트러블슈팅에 대해 설명하며, 실제적인 확인, 명확한 복구 단계, 에스컬레이션 전에 확인해야 할 정보 등을 제공합니다.

## 2. 목적

- SWIM 워크플로가 실패한 위치를 찾을 수 있도록 지원
- GUI 상태 및 디바이스 상태를 모두 확인할 수 있습니다.
- 안전한 복구 단계 안내
- 에스컬레이션 전에 올바른 정보 수집 지원

## 3. 범위

- 이미지 가져오기 문제
- 황금 이미지 및 규정 준수 문제
- 이미지 배포 실패
- 활성화 및 부팅 문제
- 스택 및 HA 업그레이드 문제
- 업그레이드 후 검증
- 데이터베이스가 잠긴 SWIM 작업을 확인합니다.

## 4. 대상

- TAC 엔지니어
- 에스컬레이션 엔지니어

## 5. 가정 및 참고 사항

이 문서에서 CatC는 Cisco Catalyst Center(CatC)를 의미하며 SWIM은 SWIM(Software Image Management)을 의미합니다.

변경하기 전에 콘솔 또는 관리 액세스를 사용할 수 있는지, 대상 이미지가 올바른지, 백업 경로가 있는지, 디바이스에서 다른 설치 작업을 아직 실행하고 있지 않은지, 변경 사항이 승인되었는지 확인하십시오.

## 6. 설명서 사용 방법

1. GUI 섹션으로 시작하여 작업 흐름 및 영향을 파악합니다.
2. CLI 섹션으로 이동하여 실제 디바이스 상태를 확인합니다.
3. 장애 도메인 섹션을 사용하여 문제를 좁힙니다.
4. 가장 위험도가 낮은 복구 작업을 먼저 적용합니다.
5. 다시 시도하기 전에 TAC 워크플로를 진행합니다.

## 7. GUI 워크플로 및 저장소 기능

GUI는 CLI 또는 데이터베이스 검사로 이동하기 전에 유용한 컨텍스트를 제공합니다.

### 7.1 이미지 권장 사항 및 보안 자문 검토

이 검토는 이미지 배포 또는 활성화 문제 해결 전에 첫 번째 확인 중 하나여야 합니다.

- 디바이스 제품군에 대한 Cisco 권장 이미지 참조(Design > Image Repository)

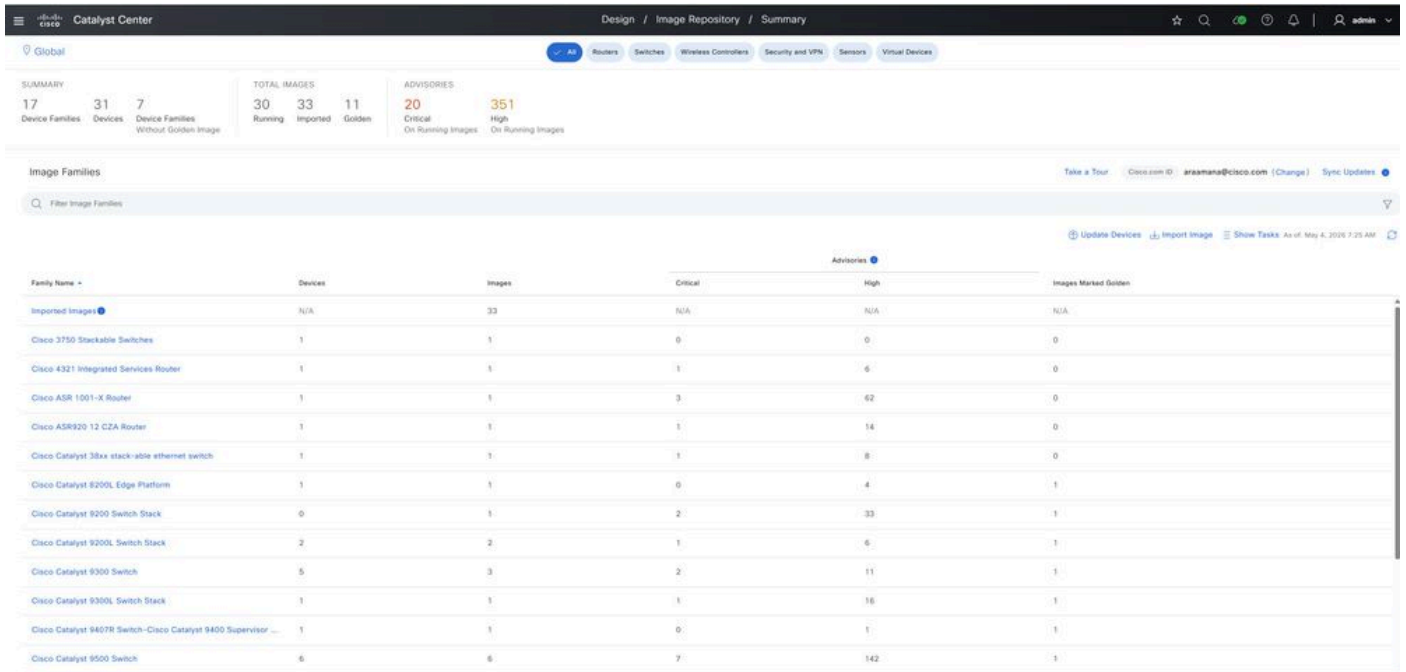
Family Name	Devices	Images	Critical	High	Images Marked Golden
Imported Images	N/A	33	N/A	N/A	N/A
Cisco 3750 Stackable Switches	1	1	0	0	0
Cisco 4321 Integrated Services Router	1	1	1	6	0
Cisco ASR 1001-X Router	1	1	3	62	0
Cisco ASR920 12 CZA Router	1	1	1	14	0
Cisco Catalyst 38xx stack-able ethernet switch	1	1	1	8	0
Cisco Catalyst 8200L Edge Platform	1	1	0	4	1
Cisco Catalyst 9200 Switch Stack	0	1	2	33	1
Cisco Catalyst 9200L Switch Stack	2	2	1	6	1
Cisco Catalyst 9300 Switch	5	3	2	11	1
Cisco Catalyst 9300L Switch Stack	1	1	1	16	1
Cisco Catalyst 9407R Switch-Cisco Catalyst 9400 Supervisor ...	1	1	0	1	1
Cisco Catalyst 9500 Switch	6	6	7	142	1

- 선택한 이미지가 플랫폼 제품군과 일치하는지 확인합니다.
- 선택한 이미지가 플랫폼 제품군과 일치하는지 확인하고 Provision(프로비저닝) > Inventory(인벤토리)에 표시된 디바이스 제품군 및 PID를 Design(설계) > Image Repository(이미지 저장소)에 나열된 이미지 제품군과 비교합니다
- 현재 이미지 및 대상 이미지에 대한 보안 권고 검토
- Design > Image Repository로 이동하여 필요한 디바이스 제품군을 선택합니다. Cisco 권장 소프트웨어 버전을 검토하고 현재 실행 중인 이미지와 비교합니다. Provision(프로비저닝) > Inventory(인벤토리)의 디바이스 제품군과 PID를 Image Repository(이미지 저장소)에 표시된 이미지 제품군과 비교하여 플랫폼 호환성을 검증합니다. 현재 이미지와 대상 이미지 모두에 대한 보안 권고 사항을 검토하여 업그레이드 연관성, 보안 위험 노출 및 소프트웨어 통화를 확인합니다.
- 실행 중인 이미지가 오래되었거나 지원되지 않거나 알려진 보안 문제에 노출되었는지 확인합니다.
- Design(설계) > Image Repository(이미지 저장소)에서 현재 이미지를 검토하고 권장 이미지 및 관련 보안 권고 사항과 비교하여 실행 중인 소프트웨어가 오래되었거나 지원되지 않거나 알려진 보안 문제의 영향을 받았는지 확인합니다.

권장 TAC 검토 흐름:

1. [디자인] > [이미지 저장소]를 엽니다.

- 올바른 디바이스 제품군을 선택합니다.
- 해당 플랫폼에 대해 표시된 권장 이미지를 검토합니다.
- 현재 실행 중인 이미지를 권장 이미지와 비교합니다.
- 심각도, 영향 및 사례와의 관련성에 대해 나열된 자문을 검토합니다.
- 대상 이미지를 이미 가져와서 할당할 수 있는지 확인합니다.
- 대상 이미지가 필요한 범위에 대해 황금으로 표시되었는지 확인합니다.



### TAC에서 검증하는 내용:

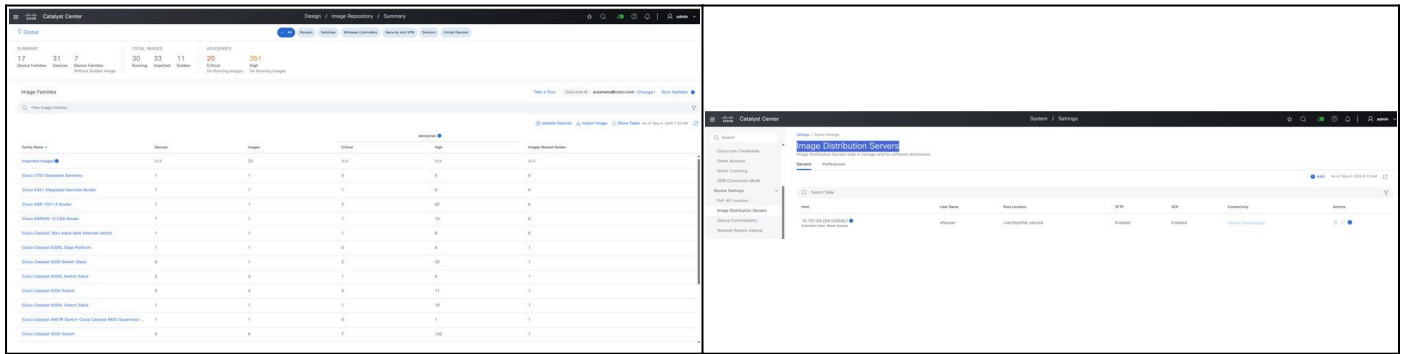
- 이 권장 사항은 정확한 플랫폼 제품군에 적용됩니다
- 선택한 이미지는 다른 하드웨어 제품군을 대상으로 하지 않습니다.
- 사이트 승인 소프트웨어 기준과 일치하는 이미지 선택
- 보안 자문 데이터를 통해 업그레이드 결정 지원

이 단계가 중요한 이유: 이 단계는 이미지 선택 오류를 조기에 포착하는 데 도움이 됩니다. 또한 컴플라이언스, 라이프사이클 조정 또는 보안 권고에 따른 업그레이드 여부도 설명할 수 있습니다.

## 7.2 이미지 가져오기 워크플로

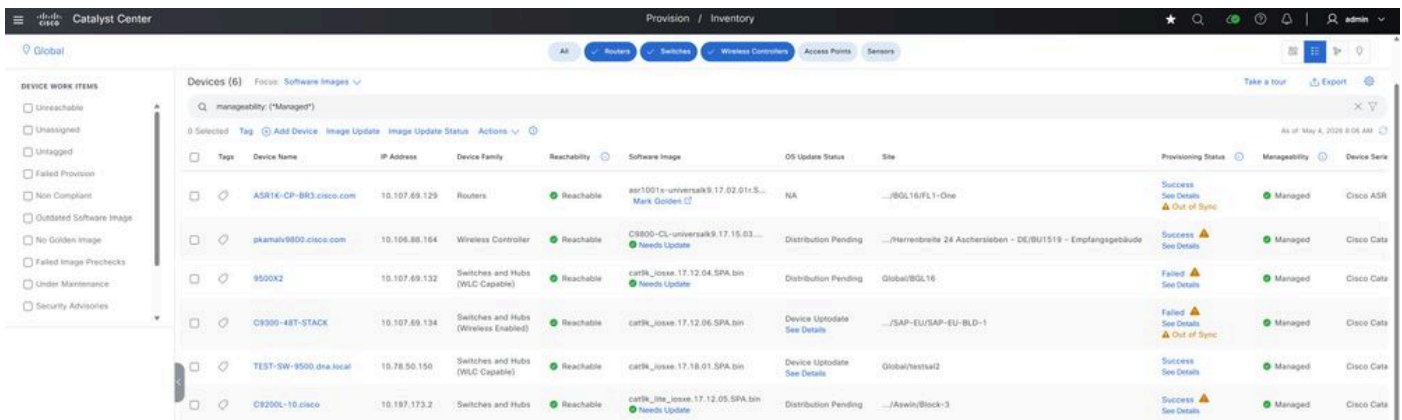
- Design(디자인) > Image Repository(이미지 저장소)로 이동합니다.
- Import Image를 클릭합니다
- Cisco, 로컬 파일 또는 URL과 같은 소스 선택
- 가져오기를 완료하고 메타데이터가 올바르게 표시되는지 확인합니다.

FIPS 모드가 활성화된 경우, URL 기반 이미지 가져오기는 플랫폼 보안 제어에 의해 제한되어야 합니다. 이러한 경우 Cisco.com 또는 로컬 파일 업로드와 같이 지원되는 가져오기 방법을 사용한 다음 가져오기 후에 이미지 메타데이터 및 체크섬이 올바르게 채워졌는지 확인합니다.



### 7.3 골든 이미지 및 업그레이드 준비

- 이미지를 성공적으로 가져왔는지 확인합니다.
- 필요한 경우 이미지가 황금으로 태그가 지정되었는지 확인합니다.
- 사이트 및 장치 제품군 할당이 올바른지 확인합니다.
- 디바이스가 Provision(프로비저닝) > Inventory(인벤토리)에서 관리된 상태인지 확인합니다



### 7.4 원격 배포 서버 인식

원격 배포 서버가 System > Settings > Device Settings > Image Distribution Servers 아래에 구성되어 있는 경우 케이스 처음부터 분석에 포함하십시오. 이는 전송 방법, 전송 타이밍, 스테이징 동작 및 이미지 배포 중 실제 실패 지점에 영향을 줄 수 있습니다.

Family Name	Devices	Images	Critical	High	Images Marked Golden
Imported Images	N/A	33	N/A	N/A	N/A
Cisco 3750 Stackable Switches	1	1	0	0	0
Cisco 4321 Integrated Services Router	1	1	1	6	0
Cisco ASR 1001-X Router	1	1	3	62	0
Cisco ASR920 12 CZA Router	1	1	1	14	0
Cisco Catalyst 38xx stack-able ethernet switch	1	1	1	8	0
Cisco Catalyst 8200L Edge Platform	1	1	0	4	1
Cisco Catalyst 9200 Switch Stack	0	1	2	33	1
Cisco Catalyst 9200L Switch Stack	2	2	1	6	1
Cisco Catalyst 9300 Switch	5	3	2	11	1
Cisco Catalyst 9300L Switch Stack	1	1	1	16	1
Cisco Catalyst 9407R Switch-Cisco Catalyst 9400 Supervisor ...	1	1	0	1	1
Cisco Catalyst 9500 Switch	6	6	7	142	1

### TAC에서 확인하는 내용:

1. 영향을 받는 사이트에 대해 원격 배포 서버가 구성되었는지 여부
2. 사용 중인 전송 프로토콜(예: SCP, HTTPS 또는 SFTP)
3. 대상 장치가 해당 서버에 연결할 수 있는지 여부
4. 원격 서버에서 올바른 이미지가 스테이징되었는지 여부
5. 문제가 하나의 원격 사이트에 영향을 미치는지 또는 동일한 서버를 사용하는 여러 사이트에 영향을 미치는지 여부

### 중요한 이유:

원격 배포 서버를 사용하는 경우 이미지 경로는 더 이상 단순한 컨트롤러 간 전송이 아닙니다. 디바이스 자체보다는 외부 서버, 프로토콜 기본 설정, 연결 가능성, 이미지 스테이징 또는 서버 측 가용성에 의해 장애가 발생합니다.

### 권장 TAC 검증 흐름:

1. 영향을 받는 사이트가 원격 배포 서버를 사용하도록 구성되어 있는지 확인합니다.
2. 선택한 전송 프로토콜을 확인합니다.
3. 대상 이미지를 사용할 수 있고 올바르게 스테이징되었는지 확인합니다.
4. 디바이스, Catalyst Center 및 원격 배포 서버 간의 네트워크 연결성을 확인합니다.
5. 배포를 다시 시도하기 전에 전송 관련 작업 실패 및 로그를 검토하십시오.

### 일반적인 TAC 문제:

1. 이미지가 잘못된 서버에 스테이징되었거나 스테이징되지 않았습니다.
2. 서버 컨피그레이션과 디바이스 기능 간의 프로토콜 불일치
3. 원격 사이트 연결 문제
4. 서버 응답 지연 또는 WAN 불안정으로 인한 전송 시간 초과

## 8. 캡처할 최소 데이터

심층적인 트러블슈팅 전에 다음 정보를 수집합니다.

- Catalyst Center 작업 ID: 표시되는 경우 기본 SWIM 작업 및 모든 하위 작업에 대한 작업 ID를 캡처합니다. GUI 활동, 로그 및 데이터베이스 상태의 상관관계를 나타내는 기본 참조입니다.
- 정확한 오류 메시지: GUI에 표시된 대로 전체 오류 메시지를 정확히 기록합니다. 작은 단어 차이도 진정한 장애 경로를 식별하는 데 도움이 되므로 이 시간을 단축하지 마십시오.
- 호스트 이름 및 관리 IP: 작업 데이터, 인벤토리 상태 및 디바이스 로그가 올바르게 매칭될 수 있도록 디바이스 호스트 이름 및 관리 IP를 기록합니다.
- 플랫폼 모델 및 PID: 정확한 하드웨어 모델 및 PID를 확인합니다. 이는 이미지 호환성, 골든 이미지 매핑 및 업그레이드 경로 검증에 중요합니다.
- 현재 버전 및 대상 버전: 디바이스에서 현재 실행 중인 소프트웨어 버전 및 업그레이드 예정 버전을 확인합니다. 이렇게 하면 이미지가 실제로 변경되기 전이나 후에 작업이 실패했는지 확인할 수 있습니다.
- 알려진 소프트웨어 모드: 해당 정보를 사용할 수 있는 경우 디바이스에서 설치 모드를 사용하는지 번들 모드를 사용하는지 기록합니다. 이는 활성화 동작 및 복구 단계에 직접적인 영향을 미칩니다.
- 디바이스가 독립형, 스택 또는 HA인지 여부: 스택 및 HA 디바이스가 독립형 디바이스와 다르게 실패하는 경우가 많고 추가 확인이 필요하므로 구축 유형을 캡처합니다.
- 비즈니스 영향 및 유지 보수 기간 세부 정보: 문제가 서비스에 영향을 미치는지 여부, 영향을 받는 사용자 또는 사이트 수, 작업이 승인된 유지 관리 기간 내에서 발생하는지 여부를 기록합니다.

권장 TAC 수집 순서:

1. 작업 ID 및 정확한 오류를 캡처합니다.
2. 디바이스 ID 및 플랫폼 세부사항 캡처
3. 현재 버전, 대상 버전 및 소프트웨어 모드를 기록합니다.
4. 디바이스가 독립형, 스택 또는 HA인지 여부를 기록합니다.
5. 비즈니스 영향 및 유지 보수 기간 상태 기록

중요한 이유: 이러한 정보를 조기에 수집하면 에스컬레이션 과정에서 앞뒤가 바뀌는 일이 줄어들며, TAC에서 문제가 이미지 선택, 작업 오케스트레이션, 플랫폼 호환성 또는 디바이스 상태와 관련이 있는지를 파악하는 데 도움이 됩니다.

## 9. Catalyst Center 검증

GUI에서 다음 항목을 확인합니다.

- 작업 세부 정보 및 하위 작업 결과: 상위 작업과 하위 작업 항목을 검토하여 워크플로가 중지된 위치를 정확하게 파악합니다. 따라서 가져오기, 배포, 활성화 및 업그레이드 후 문제가 분리됩니다.
- 실패 메시지 및 실패 시간: 정확한 실패 메시지 및 타임스탬프를 캡처합니다. 이렇게 하면 GUI 이벤트를 디바이스 로그, SWIM 로그 및 데이터베이스 작업 레코드와 일치시킬 수 있습니다.
- 이미지 저장소 항목 및 메타데이터: 저장소에 대상 이미지가 있으며 버전, 제품군 및 메타데이터가 완전한지 확인합니다. 일부 또는 잘못된 저장소 입력으로 인해 할당 및 배포 문제가 발생할 수 있습니다.
- 골든 이미지 할당: 골든 이미지 할당이 원하는 사이트, 역할 및 디바이스 패밀리와 일치하는지 확인합니다. 할당이 잘못되면 준수 불일치가 발생하거나 업데이트 워크플로 중에 잘못된 이미지가 선택될 수 있습니다.
- 인벤토리 연결성: 디바이스가 현재 연결 가능하고 여전히 관리 상태로 표시되는지 확인합니다. 인벤토리 상태가 저하된 경우 작업을 다시 시도하기 전에 먼저 문제를 해결하십시오.
- 작업 전후의 규정 준수 상태: 업그레이드 시도 전과 실패 후의 규정 준수 상태를 비교합니다. 이렇게 하면 이미지가 실제로 변경되었는지, 동기화가 오래되었는지 또는 활성화 전에 오류가 발생했는지 여부를 표시할 수 있습니다.
- 작업이 중단되거나 지연된 경우 플랫폼 상태: 작업이 보류 중이거나 지연되거나 일관성이 없는 경우 Catalyst Center에서 시스템 및 애플리케이션 상태를 확인합니다. 이렇게 하면 문제가 디바이스 측면이 아닌 컨트롤러 측면인지 파악하는 데 도움이 됩니다.
- 소프트웨어 데이터가 오래된 것 같은 경우 인벤토리 재동기화 옵션: 디바이스가 성공적으로 반환되었지만 GUI에 표시된 소프트웨어 버전이 오래된 경우 업그레이드 실패로 간주하기 전에 인벤토리 재동기화를 사용합니다.
- 재시도가 동작을 변경했는지 확인하는 작업 기록: 동일한 디바이스 또는 사이트에 대한 이전 작업 시도를 검토합니다. 이렇게 하면 실패가 일관적인지, 간헐적인지, 재시도 사이의 변경 사항에 영향을 받는지 확인할 수 있습니다.

권장 TAC 검증 순서:

1. 실패한 작업을 열고 상위 작업 및 하위 작업 세부 정보를 검토합니다.
2. 정확한 실패 텍스트 및 실패 시간을 캡처합니다.
3. 저장소의 대상 이미지 항목을 확인합니다.
4. 골든 이미지 할당 및 범위를 확인합니다.
5. 현재 인벤토리 연결 및 관리 상태를 확인합니다.
6. 실패한 시도 전후의 규정 준수 상태를 비교합니다.
7. 다시 시도하기 전에 플랫폼 상태, 인벤토리 동기화 상태 및 작업 기록을 검토하십시오.

중요한 이유: 이러한 검사는 TAC에서 이미지 선택, 할당, 컨트롤러 작업 처리, 인벤토리 동기화 또는 디바이스 자체로 인해 발생한 문제인지 여부를 확인하는 데 도움이 됩니다.

## 10. 디바이스측 CLI 확인

플랫폼 및 소프트웨어 모드에 맞는 명령만 실행합니다.

이러한 설치 관련 명령은 SWIM 업그레이드 분석 시 특히 유용합니다. 이러한 how tech installcommand는 설치 프로세스에 대한 광범위한 기술 스냅샷을 제공하며 일반적으로 검토 또는 에스컬레이션을 위해 전반적인 설치 관련 증거를 수집하는 데 사용됩니다. show platform software install-manager switch X R0 operation history detailcommand는 특정 스택 멤버에 대한 install-manager 작업의 세부 기록을 보여주며 어떤 단계가 완료되었고 어디에서 프로세스가 실패했는지 확인하는 데 도움이 됩니다. show platform software install-manager switch X R0 operation current detailcommand는 해당 스위치의 라이브 설치 상태를 표시하며, 업그레이드가 중지되었거나 아직 실행 중인 경우 유용합니다. 요청 플랫폼 소프트웨어 추적 아카이브 명령은 심층 분석을 위해 플랫폼 소프트웨어 추적 데이터를 수집하는 반면, 요청 플랫폼 소프트웨어 추적 슬롯 스위치 X 아카이브 명령은 특정 스택 멤버에 대해 동일한 추적 데이터를 수집합니다. 이러한 명령을 함께 사용하면 설치 중에 발생한 일, 현재 진행 중인 일, 추가 분석을 위해 수집해야 할 증거 등을 파악할 수 있습니다.

```
show tech install
show platform software install-manager switch X R0 operation history
detail(stack)
show platform software install-manager switch X R0 operation current
detail(stack)
플랫폼 소프트웨어 추적 아카이브 요청
요청 플랫폼 소프트웨어 추적 슬롯 스위치 X 아카이브(스택)
```

### 10.1 코어 식별 명령

```
show version
```

인벤토리 표시

```
show platform
```

```
show boot
```

```
show running-config | 부트 시스템 포함
```

```
startup-config 표시 | 부트 시스템 포함
```

파일 시스템 표시

dir 플래시:

dir bootflash:

이 명령을 사용하여 현재 버전, 부팅 설정 및 사용 가능한 스토리지를 확인합니다.

## 10.2 설치 및 패키지 상태 명령

설치 요약 표시

show install active(활성 설치 표시)

show install committed

설치 로그 세부 정보 표시

설치 요청 표시

이 명령은 이전 설치가 여전히 실행 중인지, 완료되지 않았는지 또는 커밋되지 않았는지 확인하는데 도움이 됩니다.

## 10.3 로깅 및 실패 증거

로깅 표시

로깅 표시 | INSTALL|INSTALL|BOOT|ERROR|FAIL|ROMMON 포함

show archive log config all

다시 로드 표시

show tech-support

## 10.4 스택 및 HA 명령

쇼 스위치

스위치 세부 정보 표시

이중화 표시

show platform software status control-processor 개요

플랫폼 소프트웨어 패키지 상태 표시

## 10.5 연결성 및 리소스 확인

ping <게이트웨이 또는 관리 피어>

show ip interface brief

인터페이스 상태 표시

show processes cpu sorted | 0.00 제외

show processes memory sorted

## 11. 장애 도메인별 문제 해결

### 11.1 이미지 배포 실패

파일 시스템 표시

dir 플래시:

dir bootflash:

로깅 표시 | 포함 SCP|SFTP|HTTP|TFTP|복사|전송|플래시

show processes cpu sorted | 0.00 제외

사용 가능한 공간이 충분한지 확인하고, 관리 경로가 안정적인지 확인하고, 사용 중이 아닌지 확인한 후에만 이전 파일을 제거합니다.

GUI 작업: 실패한 작업을 열고, 디바이스가 여전히 관리되는지 확인하고, 이미지가 저장소에 있는지 확인하고, 원격 배포 서버가 사용 중인지 확인하고, 스토리지, 자격 증명 및 전송 경로가 정상인 경우에만 다시 시도하십시오.

## 11.2 정품 인증에 실패하고 디바이스에서 기존 이미지를 부팅합니다

show version

show boot

show running-config | 부트 시스템 포함

startup-config 표시 | 부트 시스템 포함

설치 요약 표시

부팅 변수가 여전히 이전 이미지를 가리키는지 확인합니다. 필요한 경우 부팅 경로를 수정한 다음 다시 로드하기 전에 컨피그레이션을 저장합니다.

terminalno boot system 구성boot system flash:<target-image.bin>endwrite memoryshow boot

GUI 작업: 작업 일정을 검토하고, 다시 로드한 후 디바이스가 다시 돌아왔는지 확인하고, GUI 버전이 오래된 경우 인벤토리 동기화를 실행하고, 다시 시도하기 전에 활성화 확인 및 정리 설정을 확인합니다.

## 11.3 설치 모드 불완전 또는 고착

설치 요약 표시

show install active(활성 설치 표시)

show install committed

설치 로그 세부 정보 표시

로깅 표시 | 설치 포함 | 설치

패키지가 이미 활성 상태이지만 커밋되지 않았는지 확인합니다. 현재 상태를 이해할 때까지 다른 설치를 시작하지 마십시오.

install commit

## 11.4 디바이스가 부팅 루프를 시작합니다.

먼저 정상 작동이 확인된 이미지를 로컬에서 계속 사용할 수 있는지 확인하고 해당 플랫폼에 대해 승인된 ROMMON 복구 방법을 사용합니다.

dir 플래시:

부트 플래시:<known-good-image.bin>

show version

show boot

configure terminal

no boot system

부트 시스템 플래시:<known-good-image.bin>

끝

write memory

## 11.5 스택 멤버 버전 불일치

쇼 스위치

스위치 세부 정보 표시

show version

dir 플래시:

설치 요약 표시

로깅 표시 | 포함 스위치|버전|설치

모든 멤버가 있는지 확인하고, 모든 멤버의 이미지 가용성을 확인한 후 전체 스택이 정상인 경우에만 다시 시도하십시오.

## 11.6 업그레이드 후 연결 가능하지만 비준수

show version

인벤토리 표시

show running-config | 부트 시스템 포함

디바이스 버전이 올바르면 업그레이드가 실패한 것으로 간주하기 전에 오래된 인벤토리 또는 규정 준수 데이터가 의심됩니다.

GUI 작업: 장치 레코드를 새로 고치고, 규정 준수를 다시 실행하고, 골든 이미지 매핑이 여전히 올바른지 확인하고, 작업 기록을 검토하여 예상 대상 버전을 확인합니다.

## 12. 복구 절차

### 12.1 안전 스토리지 정리

dir 플래시:

dir bootflash:

delete /force flash:<unused-image.bin>

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

## 12.2 부트 변수 수정

show boot

configure terminal

no boot system

부트 시스템 플래시:<target-image.bin>

끝

write memory

show boot

## 12.3 준비 제어 후 수동 다시 로드

reload

## 12.4 활성 패키지가 올바르면 설치 커밋

설치 요약 표시

install commit

show install committed

## 12.5 수동 복구 후 검증

show version

show boot

설치 요약 표시

로깅 표시 | 끄리

show ip interface brief

## 12.6 GUI 복구 검증

1. 디바이스가 관리되고 인벤토리에서 연결 가능한지 확인
2. 버전이 오래된 것 같으면 인벤토리 동기화 실행
3. 규정 준수 다시 실행
4. 이미지 저장소 및 골든 매핑이 여전히 정책과 일치하는지 확인
5. 미완료 업그레이드 작업이 열려 있지 않은지 확인

## 13. TAC 워크플로

기본 GUI 및 CLI 확인 후 이 워크플로를 사용합니다. 이를 실시간 TAC 사례의 작업 시퀀스로 처리합니다.

### 13.1 장애가 시작된 위치 확인

목표: 문제가 Catalyst Center에서 시작되었는지, 전송 경로에서 시작되었는지 아니면 디바이스에서 시작되었는지를 결정합니다.

작업 검사: 작업 세부 정보, 타임스탬프, 인벤토리 상태 및 디바이스 연결성을 검토합니다. 컨트롤러측 장애는 전송 장애와 디바이스측 장애로부터 가능한 한 일찍 분리됩니다.

결정: 이미지가 디바이스에 도달하기 전에 작업이 실패한 경우 인벤토리, 자격 증명, 저장소 상태 및 전송 경로에 계속 집중합니다. 이미지가 복사되었지만 활성화가 실패한 경우 부트 변수, 설치 상태 및 디바이스 로그로 이동합니다.

## 13.2 정확한 오류 및 시간 캡처

목표: 완전한 실패 타임라인을 구축합니다.

캡처: 정확한 GUI 오류 텍스트, 작업 ID, 실패 타임스탬프 및 하위 작업 세부 정보(있는 경우)를 기록합니다.

이 점이 중요한 이유: 데이터는 GUI 이벤트를 디바이스 로그, SWIM 로그 및 데이터베이스 레코드와 일치시켜야 합니다.

## 13.3 영향 범위 측정

목표: 단일 디바이스 문제인지 아니면 더 광범위한 플랫폼 문제인지 결정합니다.

확인: 문제가 환경 전체에서 하나의 디바이스, 하나의 스택, 하나의 사이트, 하나의 플랫폼 제품군 또는 여러 디바이스에 영향을 미치는지 확인합니다.

결정: 여러 디바이스에서 동일한 장애가 나타나는 경우, 한 디바이스를 비난하기 전에 의심스러운 이미지 품질, 플랫폼 호환성, 저장소 상태, 자격 증명 또는 컨트롤러측 작업 처리 등이 있습니다.

## 13.4 SWIM 워크플로 도달 범위 확인

목표: 성공적으로 완료된 마지막 단계를 찾습니다.

트랙: 이미지 가져오기, 할당, 배포, 활성화, 다시 로드 및 업그레이드 후 동기화를 통해 워크플로를 진행합니다.

중요한 이유: 따라서 이미 작동했던 단계를 반복할 필요가 없으며 실제 장애 지점에 집중할 수 있습니다.

## 13.5 이미지가 장치에 도달했는지 확인

목표: 전송 단계가 실제로 완료되었는지 확인합니다.

검사: 이미지가 플래시에 있는지 확인합니다. 또는 bootflash: 사용 가능한 공간이 충분한지, 파일이 완전한지, 이미지가 원하는 플랫폼과 일치하는지 확인합니다.

결정: 이미지가 없는 경우 전송 트러블슈팅을 계속 진행합니다. 이미지가 있는 경우 활성화, 부팅 선택, 패키지 상태 또는 업그레이드 후 검증으로 전환합니다.

## 13.6 장애 발생 시기 결정

목표: 타임라인의 정확한 지점에 오류를 배치합니다.

분류: 이 문제를 다음 시점 중 하나로 분할하십시오. 다시 로드 전, 다시 로드 중 또는 다시 로드 후.

결정: 다시 로드하기 전에 오류가 발생한 경우 설치 로직, 부팅 설정 및 작업 오케스트레이션에 중점을 둡니다. 다시 로드하는 동안 오류가 발생한 경우 콘솔 출력, 다시 로드 이유 및 부팅 동작을 확인합니다. 다시 로드 후 발생한 경우 재검색, 규정 준수 동기화, 스택 상태 및 서비스 복구에 중점을 둡니다.

## 13.7 재시도 전에 디바이스 상태 확인

목표: 다시 실행하기 전에 디바이스가 안정적인지 확인하십시오.

확인: 소프트웨어 모드를 이해하고, 부팅 변수가 올바르고, 스토리지가 정상적이며, 설치 상태가 완전하지 않고, 스택 또는 HA 상태가 정상이고, 이전 설치 작업이 아직 활성 상태가 아닌지 확인합니다.

종료 기준: 이러한 검사가 모두 명확하거나 작업을 계속해야 할 이유가 문서화될 때까지 다시 시도하지 마십시오.

## 13.8 가장 위험도가 낮은 복구 단계를 먼저 사용하십시오.

목표: 케이스를 계속 진행하면서 위험 감소

다음으로 시작: 인벤토리 새로 고침, 컴플라이언스 재실행, 로그 검토, 부팅 변수 수정, 활성화가 이미 성공한 경우 패키지 커밋

지침: 정상 검사에서 작업이 오래된 것으로 표시되어 있고 해당 장치가 워크플로에서 더 이상 활성 상태가 아닌 경우에만 데이터베이스 업데이트나 강제 정리를 진행하십시오.

## 13.9 상태가 클리어 후에만 다시 시도

목표: 다음 시도 전에 명확한 결정 지점을 설정합니다.

다음 경우에만 다시 시도: 현재 문제가 이해되고, 디바이스가 정상이며, 충돌하는 작업이 아직 열려 있지 않으며, 이미지와 할당이 올바르고, 복구 변경 사항이 저장되고 검증되었습니다.

결정: 이러한 조건이 충족되지 않으면 재시도 경로를 중지하고 이미 수집한 증거로 에스컬레이션합니다.

## 14. 에스컬레이션 패키지 체크리스트

- Catalyst Center 작업 세부 정보
- 가져오기, 배포, 활성화 및 다시 로드에 대한 타임스탬프
- show version
- show boot
- 설치 요약 표시
- 설치 로그 세부 정보 표시
- 로깅 표시
- dir 플래시: 또는 dir bootflash: 명령을 함께 사용하여
- 관련성이 있는 경우 show switch 또는 show redundancy
- 디바이스가 ROMMON 또는 부팅 루프에 진입한 경우 콘솔 출력
- 모든 복구 작업이 이미 시도되었습니다.

## 15. 장치 유용한 명령 참조

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.