

# Nexus 상태 및 컨피그레이션 확인 수행

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[상태 및 컨피그레이션 확인 절차](#)

[상태 및 컨피그레이션 확인 모듈](#)

[보고서 및 주의 사항](#)

[FAQ](#)

[피드백](#)

---

## 소개

이 문서에서는 Nexus 3000/9000 및 7000 플랫폼에 대한 자동 상태 및 컨피그레이션 확인을 수행하기 위한 절차 및 요구 사항에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

자동화된 상태 및 컨피그레이션 확인은 독립형 NX-OS 소프트웨어를 실행하는 Nexus 플랫폼에서만 지원되며 ACI 소프트웨어를 실행하는 스위치에서는 지원되지 않습니다.

다음과 같은 하드웨어 플랫폼이 지원됩니다.

- 통합 NX-OS 소프트웨어 이미지를 실행하는 Nexus 3000/9000 Series 스위치: 7.0(3)ix 이상
- NX-OS 소프트웨어 버전 7.x 이상을 실행하는 Nexus 7000/7700 Series 스위치

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

## 상태 및 컨피그레이션 확인 절차

상태 `show tech-support details` 및 컨피그레이션 확인을 수행하려는 Nexus 스위치에서 로그를 수집하거나 `show tech-support` 확인하십시오. 이 `show tech-support details`는 더 많은 검사를 통해 더 높은 값을 제공하므로 권장됩니다. 로그가 `.txt` 또는 `.gz/.tar` 형식으로 캡처되었는지 확인하십시오. 현재 ASCII 및 UTF-8 텍스트 형식으로 캡처된 또는 `show tech-support` `show tech-support details` 파일이 지원됩니다.

Cisco [Support Case Manager](#)에서 다음 키워드 집합(기술/하위 기술/문제 코드)으로 정기 TAC 서비스 요청을 엽니다.

기술: 데이터 센터 및 스토리지 네트워킹

하위 기술: (적절한 플랫폼 선택)

Nexus 3000(N3000 시리즈에만 해당) - 상태 및 컨피그레이션 확인(자동)

Nexus 3000(N3100-N3600 시리즈) - 상태 및 컨피그레이션 확인(자동)

Nexus 7000 Series 스위치 - 상태 및 컨피그레이션 확인(자동)

Nexus 9200 - 상태 및 컨피그레이션 확인(자동)

Nexus 9300(Non EX/FX/R Series) - 상태 및 컨피그레이션 확인(자동)

Nexus 9300(EX/FX/R Series) - 상태 및 컨피그레이션 확인(자동)

Nexus 9400 series 스위치 - 상태 및 컨피그레이션 확인(자동)

Nexus 9500(Non EX/FX/R Series) - 상태 및 컨피그레이션 확인(자동)

Nexus 9500(EX/FX/R Series) - 상태 및 컨피그레이션 확인(자동)

Nexus 9800 series 스위치 - 상태 및 컨피그레이션 확인(자동)

문제 코드: 상태 및 컨피그레이션 확인

SR이 열리면 Cisco Guided [Workflow](#)에서는 또는 로그를 업로드하는 단계를 `show tech-support details` `show tech-support` 안내합니다.

필수 출력이 업로드되면 Cisco는 로그를 분석하고 사용자에게 전송된 이메일에 첨부된 상태 확인 보고서(PDF 형식)를 제공합니다. 이 보고서에는 탐지된 문제 목록, 문제 해결을 위한 관련 단계, 권장 조치 계획이 포함되어 있습니다.

보고된 상태 검사 실패와 관련하여 질문이 있는 경우, 사용자는 적절한 키워드와 함께 별도의 서비스 요청을 열어 전문가의 도움을 받는 것이 좋습니다. 신속한 조사를 위해 생성된 보고서와 함께 Automated Health and Config Check를 위해 개설된 SR(Service Request) 번호를 참조하는 것이 좋습니다.

## 상태 및 컨피그레이션 확인 모듈

Automated Nexus Health and Configuration Check 버전 1, 2022년 8월 릴리스는 표 1에 나열된 검사를 수행합니다.

표 1: 모듈에서 사용하는 상태 확인 모듈 및 관련 CLI

색인	상태 확인 모듈	모듈에 대한 간략한 설명	상태 확인을 수행하는 데 사용되는 CLI
1.	NX-OS 릴리스 확인	디바이스에서 Cisco 권장 NX-OS 소프트웨어 릴리스를 실행하는지 확인합니다.	show version
2.	Nexus EoS/EoL 제품 검사	구성 요소(하드웨어/소프트웨어) 중 어느 하나가 EOL(단종) 또는 EOS(판매 종료)에 도달했는지 확인	show version show module show inventory
3.	필드 알림 확인	디바이스가 알려진 PSIRT/CVE 또는 Field Notice의 영향을 받을 가능성이 있는지 확인합니다.	show version show module show inventory show running-config 그리고 지정된 FN/PSIRT를 기준으로 파일을 검사하는 데 필요한 모든 명령을 입력할 수 있습니다.
4.	NX-OS CPU 상태 확인	CPU 사용률이 향상되었는지 증상을 확인합니다. 현재/기록 CPU 사용량이 60%를 초과할 때 보고됩니다.	show processes cpu show processes cpu sort show processes cpu history show system resources
5.	NX-OS 메모리 상태 확인	디바이스의 메모리 사용량이 시스템 메모리 임계값(기본값 또는 사용자 구성 값)을 초과하는지 확인합니다.	show version show processes memory show system resources
6.	NX-OS 인터페이스 확인	보고된 인터페이스 중 하나가 RX 또는 TX 방향으로 삭제되는지 확인합니다. 이 모듈은 각 방향으로 가장 높은 오류율을 보이는 인터페이스 5개를 인쇄합니다.	show interface show interface brief show queuing
7.	CoPP 상태 확인	CoPP가 비활성화되었거나 잘못 구성되었는지(예: 기본 클래스에 도달하는 모든 CPU 바운드 트래픽), 오래된 CoPP 정책이 있는지(예: 이전 릴리스에서 전달됨) 또는 기본이 아닌 클래스에서 보고된 1000개 이상의 삭제를 확인합니다.	show copp status show policy-map interface control-plane show running-config
8.	MTS(프로세스 간	프로세스 간 통신(MTS라고 함) 메시지가	show system internal mts buffer summary show system internal mts

	통신) 상태 확인	1일 이상 지속되는지 여부를 탐지합니다.	buffer details
9.	Nexus 모듈 상태 확인	모듈(라인 카드, 패브릭 등)에서 진단 장애를 보고했는지 또는 전원이 꺼졌거나 장애가 발생한 상태인지 확인합니다.	show moduleshow inventory show diagnostic result module all detail
10.	PSU 및 팬 상태 확인	전원 공급 장치가 작동 상태에 있지 않은지 여부를 탐지합니다.	show inventoryshow environment  show logging log show logging nvrnram
11.	vPC 모범 사례 확인	디바이스 컨피그레이션이 피어 라우터, 피어 스위치, 피어 게이트웨이 컨피그레이션과 같은 vPC 모범 사례를 충족하는지 확인합니다.	<u>레이어 3 피어 라우터:</u> show running-config (OSPF, EIGRP 및 BGP 인접성의 형성 여부 확인) <u>피어 게이트웨이/피어 스위치:</u> show running-config show spanning-tree show vpc brief show interface brief
12.	MTU 확인	Layer2 인터페이스와 Layer3 SVI의 MTU 컨피그레이션이 일치하지 않거나, OTV 조인 인터페이스의 MTU가 잘못되었거나, 필요한 인터페이스에서 점보 MTU가 활성화되지 않은 경우 등 일관성 없는 MTU 컨피그레이션을 탐지합니다.	show running-configshow interface show ip arp  show mac address-table show ip route detail  show ip eigrp neighbors  show ip ospf neighbors  show bgp
13.	레이어 2 기능 컨피그레이션 상태 확인	L2 기능이 활성화되었지만 사용되지 않았는지 확인합니다.	show running-config

14.	NX-OS vPC 호환성 검사	vPC(Virtual Port-Channel)에 대해 유형 1/유형 2 비호환성 오류가 보고되었는지 확인합니다.	show running-config show vpc
15.	스패닝 트리 프로토콜 상태 확인	연결된 출력에서 스페닝 트리 프로토콜 불안정성을 나타내거나 예기치 않은 상태에 있는지 확인합니다. 모듈은 몇 가지 추가 정보와 함께 가장 최근의 토폴로지 변경이 발생한 VLAN을 보고합니다.  타임스탬프, 인터페이스 및 루트 브리지 ID입니다.  현재 이 상태 확인 모듈은 RSTP만 지원합니다. MST는 향후 버전에서 지원할 계획입니다.	show spanning-tree detail show spanning-tree internal errors show spanning-tree internal event-history  show spanning-tree active show logging log  show mac address-table notification mac-move show system internal
16.	PortChannel 상태 확인	구성된 포트 채널 멤버 중 (I), (S) (D) 또는 (H)가 비정상 상태인지 탐지합니다.	show port-channel summary
17.	SFP 검증 확인	"SFP 검증 실패" 오류를 보고한 트랜시버를 탐지합니다	<b>show interface brief</b>
18.	Layer3 기능 컨피그레이션 상태 확인	L3 기능이 활성화되었지만 사용되지 않았는지 확인합니다.	show running-config
19.	관리 VRF 확인을 통한 기본 경로	디바이스에 Management vrf를 가리키는 Default vrf에 구성된 기본 경로가 있는지 확인합니다.	show running-config show accounting log
20.	지원되지 않는 vPC를 통한 멀티캐스트 라우팅 확인	vPC에서 지원되지 않는 PIM 인접성을 확인합니다.	<b>show running-config show ip pim interface vrf all internal show ip pim neighbor vrf all detail</b>
21.	OSPF 상태 확인	디바이스에서 관찰된 가능한 인접성 문제를 확인합니다.예:  <ul style="list-style-type: none"> <li>• P2P로 구성된 인터페이스에서 여러 인접 디바이스 탐지</li> <li>• 수동으로 구성되지 않았거나 루프백 IP를 사용한 라우터 ID</li> <li>• FULL 상태가 아닌 인접성</li> </ul>	show running-config show ip interface brief vrf all show ip ospf neighbors detail vrf all private show ip ospf interface vrf all private show logging log

		<ul style="list-style-type: none"> <li>• 최근 FULL 상태에 도달했으며 잠재적인 불안정을 나타내는 인접성</li> </ul>	
22 .	EIGRP 상태 확인	<p>디바이스에서 관찰되는 가능한 인접성 문제를 확인합니다. 예를 들면 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• AS 번호가 구성되지 않음</li> <li>• 활성 인접 디바이스가 검색되지 않음</li> <li>• 높은 SRTT, RTO 또는 Q Cnt 값 감지</li> <li>• 많은 수의 삭제된 EIGRP 패킷이 감지되었습니다.</li> <li>• 인접성의 가동 시간이 15분 미만이며, 잠재적인 불안정성이 나타남</li> <li>• 인접성이 지난 7일 동안 저하되었습니다.</li> </ul>	<pre>show running-config show logging log show ip eigrp neighbors detail vrf all show ip eigrp detail vrf all</pre>
23 .	BGP 피어 상태 확인	<p>IDLE 상태의 BGP 인접성을 확인합니다.</p>	<pre>show running-config show bgp vrf all all summary</pre>
24.	FHRP(First-Hop Redundancy Protocol)	<p>이러한 컨피그레이션으로 인해 성능이 저하될 수 있으므로 기본 타이머 컨피그레이션이 아닌 타이머 컨피그레이션을 확인합니다.</p> <p>이 상태 확인 모듈에서는 HSRP(Hot-Standby Routing Protocol)만 다룹니다</p>	<pre>show running-config</pre>
25 .	VXLAN EVPN 구성 일관성 검사기	<p>NX-OS VXLAN 컨피그레이션 가이드에 따라 연결된 출력의 컨피그레이션을 확인합니다. 예를 들어 다음을 확인합니다.</p> <ul style="list-style-type: none"> <li>• NVE의 소스로 사용되는 루프백 인터페이스와 소스 BGP 업데이트로 사용되는 루프백 인터페이스는 동일하지 않습니다</li> <li>• NVE 소스로 사용되는 루프백 인터페이스는 기본 VRF에 있습니다</li> <li>• VXLAN으로 캡슐화된 트래픽 L3 업링크는 기본 VRF에 있으며 SVI 또는 하위 인터페이스로 구성되지 않습니다.</li> </ul>	<pre>show running-config show version show module show inventory show vpc show port-channel summary show vlan all-ports</pre>

- L3 업링크에는 단일 ARP 항목이 있습니다(즉, 다중 액세스 없음).
- vPC 기능이 활성화되었으며 vPC 도메인이 있음
- 백업 SVI는 기본 VRF에 있으며 vPC 피어 링크를 통해 허용되고 infra-vlan으로 정의됩니다.
- NVE 상태의 관리자 상태가 두 vPC 피어에 대해 모두 UP입니다(vPC 일관성 매개변수).
- "ingress-Replication" 또는 "mcast-group"이 각 L2 VNI에 대해 구성되거나 "global mcast-group"이 NVE에 정의되어 있습니다.
- PIM Sparse-mode가 L3 업링크에서 활성화됨 멀티캐스트가 BUM 트래픽의 복제 모드로 사용되는 경우
- PIM Sparse-mode는 L3 업링크에서 활성화되며, "evpn multisite dci-tracking" 없음
- "suppress-arp"는 확장 VLAN의 SVI가 "패브릭 포워딩 모드 anycast-gateway"로 구성된 L2VNI에서만 구성됩니다.
- "advertise l2vpn evpn"은 9.2 이전 버전의 NX-OS에서 구성됩니다.
- 'multisite'는 클라우드 규모 ASIC가 포함된 Nexus 9000에서만 구성됩니다
- "evpn multisite dci-tracking"은 DCI 링크에 구성되고 "fabric-tracking"은 L3 업링크에 구성되며 인터페이스는 SVI가 아닙니다.
- "peer-type fabric-external"은 BGW 간의 L2VPN 세션에 구성됩니다
- 멀티사이트의 소스로 사용되는 루프백 인터페이스는 NVE에서 정의됩니다.
- "peer-gateway", "peer-switch", "ip arp synchronize", "ipv6 nd synchronize"가 vPC 도메인에 구성되어 있습니다.
- 'associate-vrf'는 L3VNI에 대해 구성되며 L3VNI의 SVI에는 VN 세그먼트가 있습니다.
- 원격 BGW에 대한 L2VPN EVPN 인

		접성에 "peer-type fabric-external" 및 "rewrite-evpn-rt-asn"이 있음	
--	--	--	--

## 보고서 및 주의 사항

- 상태 및 컨피그레이션 확인 SR은 가상 TAC 엔지니어가 자동으로 처리합니다.
- 보고서(PDF 형식)는 일반적으로 모든 필요한 로그가 SR에 첨부된 후 24시간(업무 시간 기준) 내에 생성됩니다.
- 이 보고서는 서비스 요청과 관련된 모든 연락처(기본 및 보조)와 이메일 (jhwatson@cisco.com에서 제공)을 통해 자동으로 공유됩니다.
- 이 보고서는 서비스 요청에도 첨부되어 나중에 사용할 수 있도록 합니다.
- 보고서에 나열된 문제는 제공된 로그를 기반으로 하며 앞서 표 1에 나열된 상태 확인 모듈의 범위에 속합니다.
- 수행되는 상태 및 컨피그레이션 확인 목록은 완전한 것이 아니며, 사용자는 필요에 따라 추가 상태 확인을 수행하는 것이 좋습니다.
- 여러 VDC(Virtual Device Context)가 있는 Nexus 7000의 경우 최상의 결과를 얻으려면 각 VDC에서 show tech-support details 파일이 필요합니다.
- VxLAN EVPN의 경우 다음 검사가 수행되지 않습니다.
  - L2, L3 VNI, 테넌트 VRF, 오버레이 Mac 주소 또는 멀티캐스트 그룹 수에 맞게 확장됩니다.
  - TRM(Tenant Routed Multicast), vPC Fabric Peering, DSVNI(Downstream VNI), 새 L3VNI, Q-in-VNI 또는 Q-in-Q-in-VNI, vPC Peer reserved-vlan miss-match 또는 경로 기본 설정의 컨피그레이션입니다. 여기서 다른 사이트로의 경로는 DCI 인터커넥트가 아닌 백업 SVI를 통해 이루어집니다.
- VxLAN EVPN 컨피그레이션의 경우 vPC 리프 스위치 간 백업 SVI에 대해 다음을 수행합니다.
  - DCNM 또는 NDFC를 사용하여 구성: 기본값인 "3600"을 VLAN으로 선택했다고 가정하여 인터페이스 VLAN 3600을 백업 SVI로 간주합니다.
  - SVI에 구성된 IGP는 OSPF 또는 ISIS입니다. Underlay의 vPC 피어 간에 iBGP IPv4 유니캐스트 세션이 설정되고 SVI에 구성된 IGP가 없는 컨피그레이션에는 백업 SVI가 없는 것으로 보고됩니다.

## FAQ

Q1: 동일한 SR에 있는 둘 이상의 스위치에 show tech-support details 대해 업로드하여 모든 스위치의 상태 점검 보고서를 받을 수 있습니까?

A1: 자동화된 케이스 처리이며 상태 검사는 가상 TAC 엔지니어가 수행합니다. 상태 확인은 처음 show tech-support details 업로드된 항목에 대해서만 수행됩니다.

Q2: 몇 시간 간격으로 캡처한 동일한 디바이스에 대해 둘 이상 show tech-support details의 디바이스를 업로드하여 둘 다에 대한 상태 확인을 수행할 수 있습니까?

A2: 이는 가상 TAC 엔지니어가 수행하는 자동화된 상태 비저장 케이스 처리이며, 업로드된 파일이 동일한 스위치에서 show tech-support details 온 것인지 아니면 다른 스위치에서 온 것인지에 상관없이 SR에



업로드된 파일에 대해 상태 및 컨피그레이션 확인이 수행됩니다.

Q3: 단일 rar/gz 파일로 압축되어 SR에 업로드된 `show tech-support details` 파일의 스위치에 대한 상태 확인을 받을 수 있습니까?

A3: 아니요. 여러 개 `show tech-support details`가 단일 rar/zip/gz 파일로 업로드되면 아카이브의 첫 번째 파일만 상태 확인을 위해 처리됩니다.

Q4: Nexus 5000/6000 플랫폼에 적용되는 상태 및 컨피그레이션 확인이 표시되지 않습니다. 나중에 다룰 수 있습니까?

A4: 아니요. 현재로서는 Nexus5000/6000 플랫폼을 지원할 계획이 가까운 장래에 없습니다.

Q5: 보고된 상태 검사 실패 중 하나에 대한 질문이 있는 경우 어떻게 해야 합니까?

A5: 특정 상태 확인 결과에 대한 추가 지원을 받으려면 별도의 TAC 서비스 요청을 여십시오. 상태 확인 보고서를 첨부하고 자동 상태 및 컨피그레이션 확인을 위해 개설된 SR(Service Request) 케이스 번호를 참조하는 것이 좋습니다.

Q6: 발견된 문제를 트러블슈팅하기 위해 Automated Health and Config Check에 대해 열려 있는 동일한 SR을 사용할 수 있습니까?

A6: 아니요. 사전 예방 상태 검사가 자동화되었으므로, 새 서비스 요청을 열어 문제를 해결하고 보고된 문제를 해결하십시오. 상태 확인을 위해 개설된 SR은 상태 보고서가 게재된 후 24시간 이내에 종료됨을 알려드립니다.

Q7: 이전에 언급한 버전보다 이전 버전을 실행하는 스위치의 `show tech-support details` 파일에 대해 자동화된 상태 및 컨피그레이션 검사가 실행됩니까?

A7: 자동화된 상태 및 컨피그레이션 확인은 아래에 언급된 플랫폼 및 소프트웨어 릴리스에 대해 구축됩니다. 이전 버전을 실행하는 장치의 경우, 이는 최선의 노력이며 보고서의 정확성에 대한 보장은 없습니다.

- 통합 NX-OS 소프트웨어 이미지를 실행하는 Nexus 3x00 시리즈 스위치: 7.0(3)ix 이상
- NX-OS 소프트웨어 버전 7.x 이상을 실행하는 Nexus 7000/7700 Series 스위치
- 통합 NX-OS 소프트웨어 이미지를 실행하는 Nexus 9x00 시리즈 스위치: 7.0(3)ix 이상

Q8: 상태 확인을 위해 연 SR을 닫으려면 어떻게 해야 합니까?

A8: 첫 번째 상태 확인 보고서가 전송된 후 24시간 내에 SR이 종료됩니다. SR 마감을 위한 사용자의 조치가 필요하지 않습니다.

Q9: 사전 대응적 상태 및 컨피그레이션 확인에 대한 의견이나 피드백을 공유하려면 어떻게 해야 합니까?

A9: Nexus-HealthCheck-Feedback@cisco.com으로 이메일을 통해 공유하십시오.

Q10. 스위치에서 캡처하거나 캡처하는 데 `show tech-support` 권장되는 `show tech-support details` 방법은 무엇입니까?

A10: 터미널 응용 프로그램의 로그 파일(예: SecureCRT, PuTTY)로 캡처하는 것보다 `show tech-support show tech-support details bootflash:` 또는 명령의 출력을 직접(다음 예시에 표시된 것처럼) 캡처하는 것이 좋습니다. 터미널 애플리케이션에서 캡처한 로그 파일은 자동 상태 검사에서 지원되지 않는 UTF-8-BOM 형식(또는 유사)일 수 있습니다. Automated Health & Config 확인은 ASCII 또는 UTF-8 형식의 파일만 지원합니다.

출력을 파일로 리디렉션하고 `bootflash:` 압축하는 CLI 예:

```
Nexus1# show tech-support details >> bootflash:showtechdetails_Nexus1.txt  
Nexus1# gzip bootflash:showtechdetails_Nexus1.txt
```

## 피드백

이러한 툴의 운영에 대한 피드백은 매우 소중합니다. 관찰 또는 제안 사항이 있는 경우(예: 생성된 보고서의 사용 편의성, 범위, 품질 등) [Nexus-HealthCheck-Feedback@cisco.com](mailto:Nexus-HealthCheck-Feedback@cisco.com)에서 공유해 주시기 바랍니다.

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.