

# DNS 장애로 인한 리소스 커넥터를 통한 ZTNA CLAP/BAP의 개인 액세스 문제 해결

## 목차

---

[문제](#)

[환경](#)

[해결](#)

[1단계: 환경 간 DNS 컨피그레이션 비교](#)

[2단계: 대체 DNS 서버 구성 테스트](#)

[3단계: DNS 확인 및 연결 확인](#)

[원인](#)

[관련 콘텐츠](#)

---

- [문제](#)
  - [환경](#)
  - [해결](#)
    - [1단계: 환경 간 DNS 컨피그레이션 비교](#)
    - [2단계: 대체 DNS 서버 구성 테스트](#)
    - [3단계: DNS 확인 및 연결 확인](#)
  - [원인](#)
  - [관련 콘텐츠](#)
- 

## 문제

ZTNA(Zero Trust Network Access)용으로 구성된 전용 리소스는 개발 환경에서 리소스 커넥터를 사용할 때 올바르게 작동합니다. 그러나 프라이빗 리소스 컨피그레이션이 프로덕션 환경에서 리소스 커넥터를 사용하도록 변경되면 프라이빗 리소스 또는 연결에 대한 액세스가 DNS 관련 오류와 함께 실패합니다. 연결이 기본 차단 규칙에 도달하여 생산 전용 리소스를 라우팅하기 전에 새 생산 리소스 커넥터의 유효성을 검사할 수 없습니다.

구체적인 증상은 다음과 같습니다.

- 프로덕션 리소스 커넥터에 대해 기록된 DNS 오류
- 활동 검색 보고서의 기본 차단 규칙에 도달하여 연결 실패
- 생산 자원 커넥터 기능의 유효성을 검사할 수 없음

- 리소스 커넥터를 사용하여 ZTNA CLAP를 통해 프라이빗 리소스에 액세스하는 데 잠재적인 영향

리소스 커넥터에서 직접 생성하는 프라이빗 웹 서버 호스트 이름의 성공적인 DNS 확인 및 Ubuntu 서버의 포트 8443에 대한 TCP 연결을 포함하여 네트워크 연결이 확인되었습니다. 모든 것이 정상이지만 프로덕션 리소스 커넥터에서 DNS 오류 알림을 수신합니다.

## 환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스 - 제로 트러스트 액세스(ZTNA, Posture, 클라이언트 기반, 등록, 개인 리소스)
- 제품군: 보안 액세스, 제로 트러스트/ZTNA, 리소스 커넥터
- 대상 개인 응용 프로그램/서버: TCP 포트 8443에서 액세스할 수 있는 Ubuntu 서버
- 네트워크 구성 요소: DEV 및 PROD 환경의 리소스 커넥터

## 해결

트러블슈팅 접근 방식은 개발 및 프로덕션 리소스 커넥터 간의 DNS 컨피그레이션 차이에 중점을 둡니다. 개발 리소스 커넥터가 작동 중입니다. 개인 리소스에 성공적으로 액세스할 수 있습니다. 프로덕션 리소스 커넥터가 작동하지 않습니다. PR에 액세스할 수 없으며 RC > 네트워크 연결 > 리소스 커넥터 > DNS 오류에서 DNS 오류가 발생합니다.

DNS 확인 문제를 파악하고 해결하려면 다음 체계적인 단계를 따르십시오.

### 1단계: 환경 간 DNS 컨피그레이션 비교

DEV 및 PROD 리소스 커넥터 간의 DNS 설정을 종합적으로 비교합니다.

1.- 개발 및 프로덕션 리소스 커넥터 모두에서 DNS 서버 구성을 문서화합니다.

- 2.- 개발 커넥터에서 기본 DNS 설정을 사용하는지 또는 대체 DNS 서버를 사용하는지 확인합니다.
- 3.- 프로덕션 커넥터 DNS 컨피그레이션을 진행 중인 개발 설정과 비교합니다.
- 4.- DNS 확인 방법, 시간 제한 또는 폴백 컨피그레이션의 차이점을 확인합니다.

## 2단계: 대체 DNS 서버 구성 테스트

프로덕션 리소스 커넥터가 기본 DNS 설정을 사용하고 있고 개발 커넥터가 대체 DNS 서버를 사용하거나 그 반대의 경우:

- 작동 중인 개발 커넥터와 동일한 DNS 서버 설정을 사용하도록 프로덕션 리소스 커넥터를 구성합니다
- 또는 프로덕션 리소스 커넥터 컨피그레이션에서 대체 DNS 서버를 지정합니다
- 각 DNS 컨피그레이션 변경 후 프라이빗 리소스 연결 테스트
- PR 대상 IP에 대한 진단, tcpdump를 사용할 때 커넥터 로그에서 DNS 확인 성공 또는 지속적 인 오류를 모니터링합니다



참고: 두 리소스 커넥터 모두 RC에 구성된 기본 DNS를 사용할 경우 PR의 FQDN(정규화된 도메인 이름)을 확인할 수 있지만, 비작동 또는 프로덕션 RC에 대한 전용 리소스 구성에 구성된 내부 DNS와 일치하지 않습니다.

## 3단계: DNS 확인 및 연결 확인

내부 DNS 서버를 사용하여 PR 컨피그레이션과 일치시켜 문제를 해결하려면 Production Resource Connector를 업데이트해야 합니다. Use Alternate DNS(대체 DNS 사용)를 선택하려면 리소스 커넥터 ID를 클릭하고 Edit(수정)를 클릭합니다. 커넥터 컨피그레이션 내의 도메인 설정을 기반으로 프라이빗 리소스를 확인하기 위해 Use alternate DNS servers(대체 DNS 서버 사용)를 탐색할 수 있습니다. 이렇게 하면 연결이 개선되는지 테스트하기 위해 도메인 및 DNS 서버를 수동으로 지정할 수 있습니다. 이 변경 후 개인 리소스 또는 Ubuntu 서버에 성공적으로 액세스할 수 있습니다.

DNS 컨피그레이션 변경 사항 구현 후:

- 1.- 프로덕션 리소스 커넥터에서 DNS 확인이 올바르게 작동하는지 확인합니다.
- 2.- 프라이빗 리소스가 더 이상 기본 차단 규칙에 맞지 않음을 확인합니다.
- 3.- 프로덕션 커넥터를 통한 엔드 투 엔드 연결 테스트

## 원인

개발 및 프로덕션 리소스 커넥터 간의 DNS 컨피그레이션 차이와 관련된 문제의 근본 원인입니다. 프로덕션 환경에서는 기본적으로 서로 다른 DNS 서버를 사용하고 있었습니다. 이 DNS 확인 실패로 인해 연결이 기본 보안 정책으로 되돌아가 트래픽이 ZTNA 프레임워크를 통해 제대로 라우팅되지 않고 기본 차단 규칙에 의해 차단됩니다. Development Resource Connector는 프라이빗 리소스 컨피그레이션에 구성된 내부 DNS와 일치하는 내부 DNS 서버를 사용하도록 구성되어 있습니다.

그러나 Production Resource Connector는 기본 DNS를 사용하도록 구성되어 있습니다. 기본 DNS는 PR 컨피그레이션에 언급된 내부 DNS 서버와 다릅니다.

내부 DNS 서버를 사용하여 문제를 해결하기 위해 PR 컨피그레이션과 일치하도록 Production Resource Connector가 업데이트되었습니다.

## 관련 콘텐츠

- [Cisco 기술 지원 및 다운로드](#)

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.