보안 클라우드 제어에서 도메인 확인 - CUI 업데이트

목차

소개

이 문서에서는 Cisco Unified Identity(CUI) 업데이트 후 SCC(Security Cloud Control)에서 새 도메인 검증을 수행하는 방법에 대해 설명합니다.

배경

Cisco SCC(Security Cloud Control)에서 도메인을 청구 및 확인할 때, 관리자는 도메인의 소유권을 확인하기 위해 DNS TXT 레코드를 게시해야 합니다.

문제

성공적인 확인을 위해 필요한 DNS 레코드 배치가 변경되었습니다. Cisco 설명서에서 참조된 이전 지침은 전용 확인 하위 도메인을 사용합니다.

_cisco-sxso-verification.example.com

그러나 현재 확인 프로세스에서는 전용 확인 하위 도메인이 아닌 루트 도메인 아래에 Cisco에서 제공하는 TXT 확인 토큰을 직접 게시해야 합니다.

무엇이 바뀌었습니까?

이전 컨피그레이션(현재 확인 워크플로에 더 이상 적용되지 않음):

DNS 필드	가치
레코드 유형	TXT
호스트/이름	_cisco-sxso-verification.example.com

가치	Cisco 확인 토큰

새 컨피그레이션(필수):

DNS 필드	가치
레코드 유형	TXT
호스트/이름	@
가치	Cisco 확인 토큰

솔루션

구현 단계

1. 도메인 DNS 공급자(GoDaddy, Cloudflare, Route 53, Azure DNS 등)에 로그인합니다.
2. 도메인에 대한 DNS 관리로 이동합니다.
3. 새 TXT 레코드를 만듭니다.
4. 다음과 같이 레코드를 구성합니다.
   유형: TXT
   호스트/이름: @
   가치: Cisco SCC에서 생성한 확인 토큰을 붙여넣습니다.
   TTL: 기본값.
5. DNS 레코드를 저장하고 DNS 전파 시간을 허용합니다.
6. Cisco SCC로 돌아가 Verify(확인)를 클릭합니다.

확인

다음 명령을 사용하여 TXT 레코드가 올바르게 게시되었는지 확인할 수 있습니다.

```
dig TXT example.com
```

응답에는 Cisco 확인 토큰이 포함되어야 합니다.

DNS에서 레코드가 표시되면 SCC로 돌아가서 도메인 확인을 다시 시도하십시오.

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.