외부 위협 피드 문제 해결 주요 실패 이유

목차

소개

이 문서에서는 외부 위협 피드 구현, 오류 분석 및 해결을 위한 작업 중에 실패하는 몇 가지 이유에 대해 설명합니다.

사전 요구 사항

특정 요구 사항은 없으므로 다음 항목에 대한 지식을 갖춘 것이 좋습니다.

- Cisco ESA(Secure Email Gateway)
- 외부 위협 피드(ETF)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 12.x 이상 버전을 실행하는 Cisco ESA(Secure Email Gateway)

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.

실패 이유:

ETF 서비스가 비활성화되었거나 서비스에 유효한 기능 키가 없습니다.

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Wed Sep 8 16:15:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: Test_Poll_Path
Machine: ‘esa03.taclab.krk'. A failure was encountered for the source 'Test_Poll_Path'.

Reason for failure: The ETF service is either disabled or there is no valid feature key for the service.
```

솔루션

다음 사항을 확인합니다.

1. ETF 기능 키가 제대로 설치되었습니다.
2. EULA 승인 및 기능 키가 전역적으로 활성화되었습니다.
3. 컴퓨터 레벨에 적용된 라이센스

참고: 클러스터 레벨이 있는 경우 설정을 시스템 레벨로 복사해야 합니다.

새 연결을 설정하지 못했습니다. [Errno 110] 연결 시간 초과

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host= otx.alienvault.comport, port=443): Max retri
Failed to establish a new connection: [Errno 110] Connection timed out',))
```

참고: 일반적으로 연결 시간이 초과되면 ESA에서 응답을 받을 수 없는 네트워크 관련 문제가 발생합니다. 심층적인 분석을 위해 방화벽/프록시 검사 및 패킷 캡처를 권장합니다.

솔루션

1. 방화벽 및 프록시가 트래픽을 차단하지 않는지 확인합니다.
   프록시는 GUI > Security Services(보안 서비스) > Service Updates(서비스 업데이트)에서 확인할 수 있습니다.
2. 패킷 캡처와의 연결을 확인합니다. GUI > Help and Support > Packet Capture로 이동합니다.

팁: 네트워크와 관련된 문제가 있는 경우, 연결이 제대로 설정되었는지 확인하기 위해 패킷 캡

처를 실행하는 것이 좋습니다.

실패 이유: "400"

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 6 13:38" threatfeeds
Mon Sep 6 13:38:16 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Test_Poll_Pat
Mon Sep 6 13:38:55 2021 Info: THREAT_FEEDS: The source 'Test_Poll_Path' is currently in a polling state
```

참고: RFC7231 Error 400 (Bad Request) - 클라이언트 오류로 간주되는 오류로 인해 서버에서 요청을 처리할 수 없거나 요청을 처리하지 않음을 나타냅니다. 잘못된 요청 구문 또는 잘못된 요청 메시지 프레이밍으로 인해 나타나는 경우가 대부분입니다.

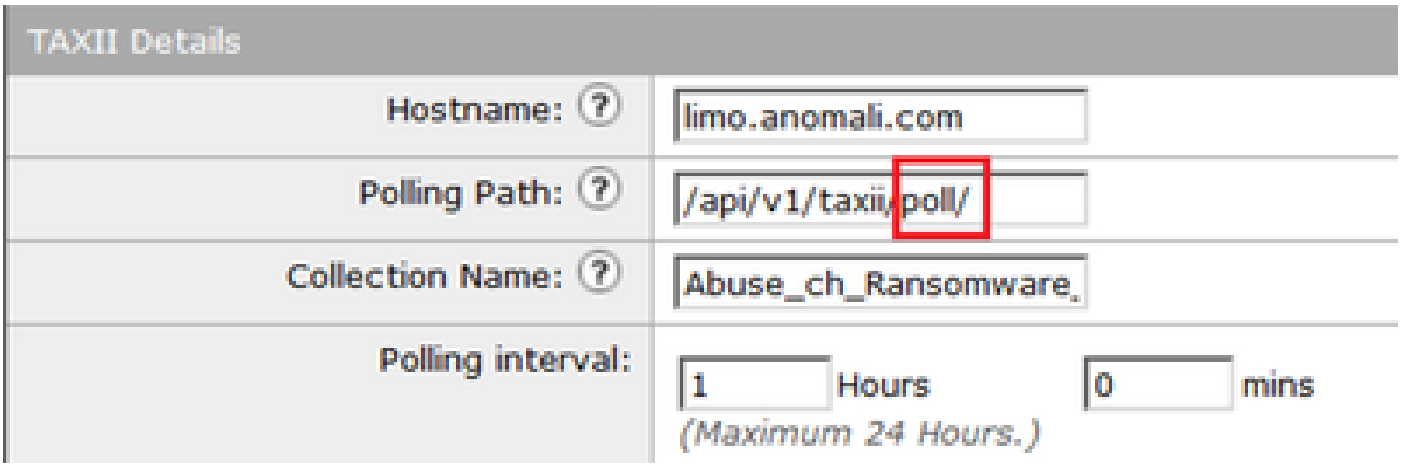
솔루션

오류 "400"은 이 폴링 경로가 존재하지만 TAXII 서버에서 제공하는 다른 서비스를 가리킵니다.

1. 폴링 경로 컨피그레이션이 검색 요청이 아닌 폴링 요청으로 구성되었는지 확인합니다.
2. GUI > Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자) > Use HTTPS(HTTPS 사용)에서 HTTPS가 활성화되었는지 확인합니다.

주의: 일반적으로 이 문제는 Polling Path가 검색 요청으로 잘못 구성된 경우 발생합니다. 예: /api/v1/taxii/taxii-discovery-service/
피드에 대해 폴링 요청을 사용하도록 폴링 경로를 구성할 수 있습니다(예: /api/v1/taxii/poll).

참고: 폴링과 검색 요청의 차이점:
- 폴링 URL은 피드를 소비하는 곳입니다.
- 검색 서비스 URL은 Taxii 서비스가 제공하는 서비스를 찾는 데 사용됩니다.



HTTP 오류: 상태 코드 401 인증 실패

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:39 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-08 16:31:36.071684 for the
Wed Sep 8 16:35:39 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reason
```

솔루션

이 오류 코드는 대상 리소스에 대한 유효한 인증 자격 증명이 없음을 나타냅니다.

자격 증명이 올바르게 구성되었는지 확인합니다.
사용자에 대한 자격 증명을 구성하지 않는 옵션도 있습니다.

Taxii 오류: HTTP 오류: 상태 코드 404 요청된 리소스를 사용할 수 없음

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 27 08:51" threatfeeds
Fri Aug 27 08:51:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test a
Fri Aug 27 08:51:16 2021 Info: THREAT_FEEDS: Job failed with exception : Source: Test. Reason for failu
```

참고: 404(찾을 수 없음) 상태 코드는 원본 서버가 대상 리소스에 대한 현재 표현을 찾지 못했거나 해당 표현이 있음을 공개하지 않을 것임을 나타냅니다. 이는 Invalid URL이 있을 수 있으며 대부분의 경우 리소스 경로로 인해 발생한 를 찾을 수 없음을 나타냅니다.

솔루션

ESA GUI > Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자)에서 소스의 폴링 경로/수집 이름 확인 > 적절한 소스 이름 선택.

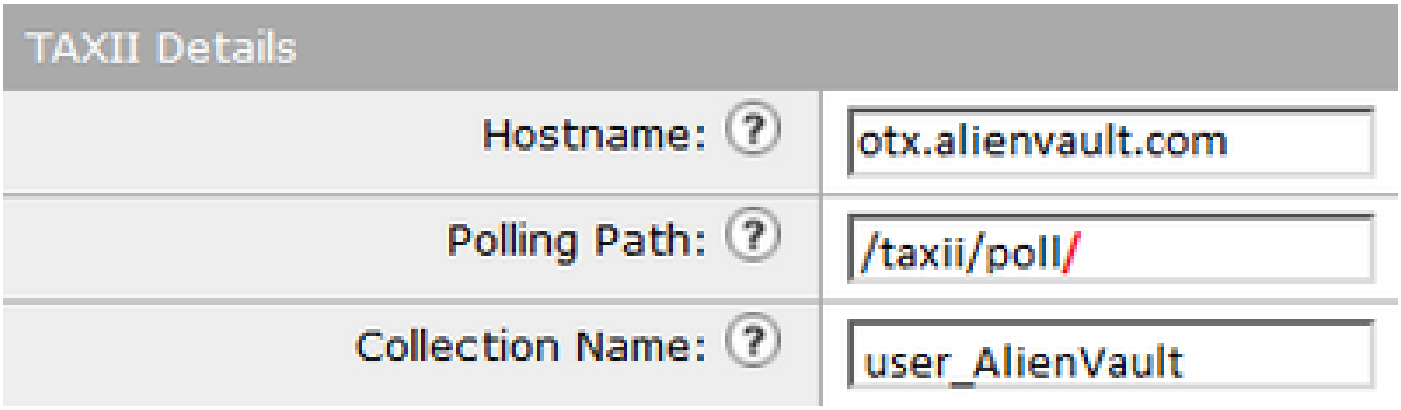
실패 이유: "405"

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 13 00:2" threatfeeds
Mon Sep 13 00:20:21 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Anomali. Rea
```

참고: RFC7231에 따라 Error 405 (Method Not Allowed)(오류 405(메서드가 허용되지 않음)는 요청 라인에서 받은 메서드가 원래 서버에서 인식되지만 대상 리소스에서 지원되지 않음을 나타냅니다.

솔루션

폴링 경로 끝에 "/" 슬래시가 없기 때문에 발생한 구문 오류입니다.
/taxii/poll/ 경로 끝에 트레일 슬래시를 추가합니다.



HTTP 오류: 상태 코드 503 서비스를 사용할 수 없음

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Nov 10 13:45" threatfeeds
Sun Nov 10 13:45:21 2020 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reaso
Sun Nov 10 13:45:22 2020 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
```

참고: RFC7231에 따르면 오류 503 "Service Unavailable"은 HTTP 응답 상태 코드이며 서버가 일시적으로 요청을 처리할 수 없음을 나타냅니다.

솔루션

오류 코드는 대상 TAXII 서버에 문제가 있음을 나타내며 이 문제를 더 자세히 조사해야 합니다.
이는 서버가 오버로드될 때 발생할 수 있습니다. 자세한 내용은 공급업체에 문의하십시오.

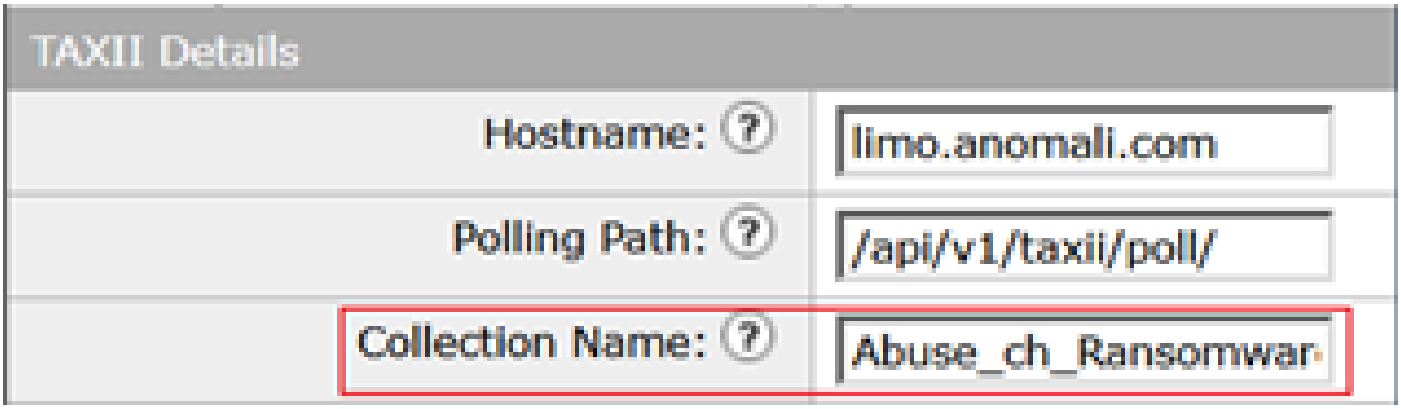
NOT_FOUND: 요청한 컬렉션을 찾을 수 없습니다.

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 7 12:53" threatfeeds
Tue Sep 7 12:53:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test_Po
Tue Sep 7 12:53:16 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-07 12:49:12.648625 for the
```

솔루션

이 오류는 모음 이름의 철자가 올바르다는 것을 나타냅니다. 그러나 모음 아래의 TAXII 서버에 문제가 있어 요청을 거부합니다.

가능한 원인은 컬렉션 이름의 만료 타이머일 수 있습니다.
공급업체에 문의하여 이러한 종류의 불일치를 확인하십시오.



[SSL: CERTIFICATE_VERIFY_FAILED] 인증서 확인 실패(_ssl.c:590)

<#root>

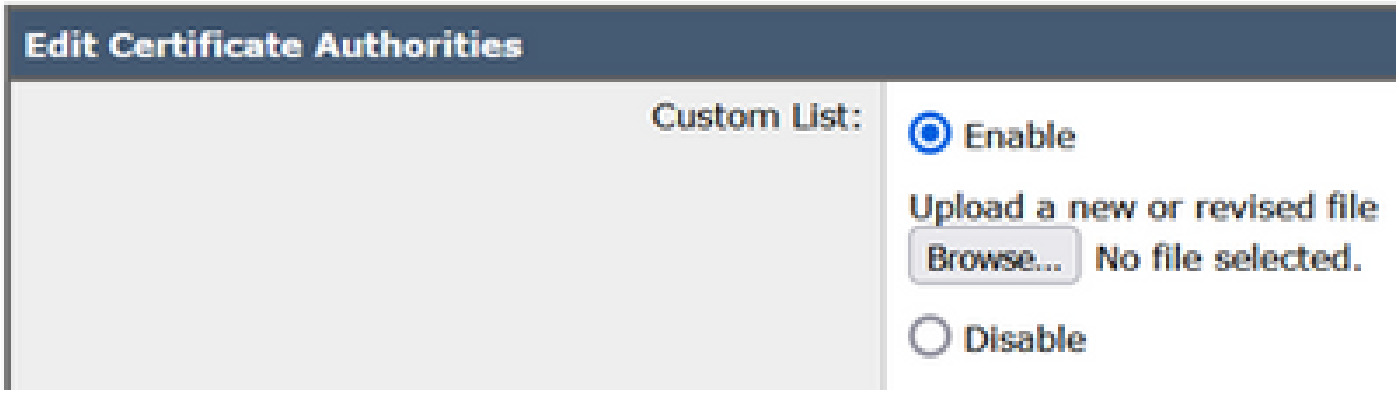
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

Reason for failure: Taxii Error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590)

솔루션

이 오류는 인증서 실패를 나타냅니다.

문제를 해결하려면 CA(Certificate Authority) 목록의 인증서를 가져옵니다.
GUI > Network > Certificates > Edit Settings > Custom List로 이동합니다.
Enable 모드를 선택하고 인증서를 업로드합니다.



XML 파티션 오류: 요소를 찾을 수 없습니다(행 0).

<#root>

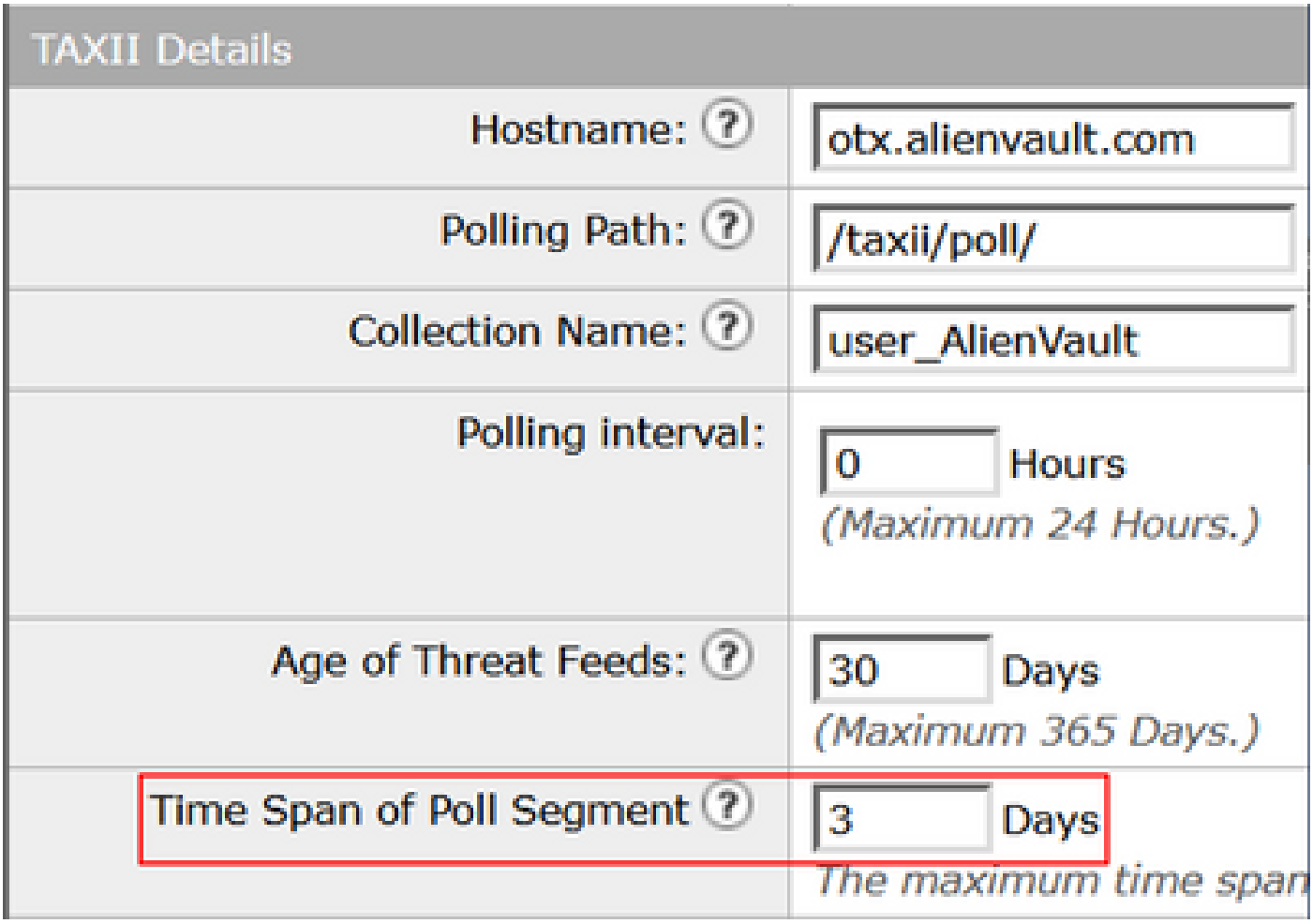
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.

Reason for failure: Taxii Error: XML Parising Error: no element found (line 0)
```

솔루션

ESA 컨피그레이션에서 Poll Segment의 Time Span 값을 3-4일로 줄입니다.

참고: 일부 특정 피드의 경우 Anomali 서버와의 불일치이며, 여기서 피드를 중지하기 위해 데이터 플래그 끝이 전송되지 않습니다.
이 경우 Anomali의 ETF 소스로 구성된 ESA는 5일 이상의 기간 동안 데이터를 폴링할 수 없습니다.
유효한 해결 방법은 ESA 컨피그레이션에서 Poll Segment의 Time Span 값을 줄이는 것입니다.



새 연결을 설정하지 못했습니다. [Errno 111] 연결 거부됨

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host=otx.alienvault.comport=443): Max retries exce
```

Failed to establish a new connection: [Errno 111] Connection refused',))

참고: "연결 거부됨"은 클라이언트가 실행 중인 서버의 포트에 연결할 수 없음을 나타냅니다. 일반적으로 서버가 잘못된 포트에서 수신 대기하거나 포트를 사용할 수 없을 때 발생합니다.

솔루션

1. CLI를 통해 telnet 또는 netstat 명령을 사용하여 적절한 포트가 수신되는지 확인합니다.
2. 방화벽이 포트를 차단하지 않는지 확인합니다.
3. 실행 중인 서비스에 포트 구성 오류/부실 포트가 없는지 확인합니다.

관련 정보

- Cisco Email Security Appliance 최종 사용자 가이드
- STIX와 TAXII는 무엇입니까?
- RFC2741 - 오류 코드
- TAC 워크숍 외부 위협 피드

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.