Cisco Catalyst Center의 WLC 9800에서 보증 없는 데이터 문제 해결

목차

소개

이 문서에서는 Cisco Catalyst Center에서 Catalyst 9800 Series WLC(Wireless LAN Controller)의 보증 데이터를 표시하지 않는 경우의 트러블슈팅 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst Center CLI maglev 사용
- 기본 Linux 기반
- Catalyst Center 및 Catalyst 9800 플랫폼의 인증서 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 1.x 또는 2.x 보장 패키지가 포함된 Catalyst Center 어플라이언스 1세대 또는 2세대
- Catalyst 9800 Series WLC

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.

참고: 이 문서는 처음에 Catalyst Center 1.x용으로 작성되었지만 대부분은 Catalyst Center 2.x용으로 유효합니다.

참고: Catalyst 9800 WLC는 Catalyst Center에서 이미 검색하여 사이트에 할당해야 하며, 호환되는 Cisco IOS® XE 버전을 실행해야 합니다. 상호 운용성에 대한 자세한 내용은 Catalyst Center 호환성 매트릭스를 참조하십시오.

배경 정보

검색 프로세스가 진행되는 순간 Catalyst Center는 다음 컨피그레이션을 WLC에 푸시합니다.

참고: 이 예는 Catalyst 9800-CL Cloud Wireless Controller에서 가져온 것입니다. 물리적 Catalyst 9800 Series 어플라이언스를 사용하는 경우 일부 세부사항이 다를 수 있습니다. X.X.X.X는 Catalyst Center 엔터프라이즈 인터페이스의 VIP(가상 IP) 주소이고 Y.Y.Y.Y는 WLC의 관리 IP 주소입니다.

<#root>

```
crypto pki trustpoint sdn-network-infra-iwan
 enrollment pkcs12
 revocation-check crl
 rsakeypair sdn-network-infra-iwan

crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
 source interface GigabitEthernet1

crypto pki certificate chain sdn-network-infra-iwan
 certificate 14CFB79EFB61506E
  3082037D 30820265 A0030201 02020814 CFB79EFB 61506E30 0D06092A 864886F7
  <snip>
        quit

 certificate ca 7C773F9320DC6166
  30820323 3082020B A0030201 0202087C 773F9320 DC616630 0D06092A 864886F7
  <snip>
        quit

crypto pki certificate chain DNAC-CA
 certificate ca 113070AFD2D12EA443A8858FF1272F2A
  30820396 3082027E A0030201 02021011 3070AFD2 D12EA443 A8858FF1 272F2A30
  <snip>
        quit

telemetry ietf subscription 1011
 encoding encode-tdl
 filter tdl-uri /services;serviceName=ewlc/wlan_config
 source-address
```

Y.Y.Y.Y

```
 stream native
 update-policy on-change
 receiver ip address
```

x.x.x.x

```
 25103 protocol tls-native profile sdn-network-infra-iwan

telemetry ietf subscription 1012
<snip - many different "telemetry ietf subscription" sections - which ones depends on
Cisco IOS version and Catalyst Center version>

network-assurance enable
network-assurance icap server port 32626
network-assurance url https://
```

x.x.x.x

```
network-assurance na-certificate PROTOCOL_HTTP
```

x.x.x.x

```
 /ca/ pem
```

Catalyst Center에서 WLC의 No Assurance 데이터 트러블슈팅

1단계. WLC가 Catalyst Center 인벤토리에서 연결 및 관리되는지 확인합니다.

WLC가 Managed(관리됨) 상태가 아닌 경우 계속하기 전에 연결성 또는 프로비저닝 문제를 해결해야 합니다.

팁: 오류를 식별하려면 inventory-manager, spf-device-manager 및 spf-service-manager 로그를 확인하십시오.

2단계. Catalyst Center에서 필요한 모든 컨피그레이션을 WLC에 푸시하는지 확인합니다.

Background Information(백그라운드 정보) 섹션에서 설명한 컨피그레이션이 다음 명령을 사용하여 WLC에 푸시되었는지 확인합니다.

```
show run | section crypto pki trustpoint DNAC-CA
show run | section crypto pki trustpoint sdn-network-infra-iwan
show run | section network-assurance
show run | section telemetry
```

알려진 문제:

- Cisco 버그 ID CSCvs62939 - Cisco DNA Center는 검색 후 텔레메트리 구성을 9xxx 스위치에 푸시하지 않습니다.

- Cisco 버그 ID CSCvt83104 - 디바이스에 Netconf 후보 데이터 저장소가 있는 경우 eWLC Assurance config push failure.
- Cisco 버그 ID CSCvt97081 - DNS 이름으로 검색된 디바이스에 대한 eWLC DNAC-CA 인증서 프로비저닝이 실패합니다.

확인할 로그:

- dna-wireless-service - DNAC-CA 인증서 및 텔레메트리 컨피그레이션용
- network-design-service - sdn-network-infra-iwan 인증서

3단계. 필요한 인증서가 WLC에서 생성되는지 확인합니다.

다음 명령을 사용하여 WLC에서 인증서가 올바르게 생성되었는지 확인합니다.

```
show crypto pki certificates DNAC-CA
show crypto pki certificates sdn-network-infra-iwan
```

알려진 문제 및 제한 사항:

- Cisco 버그 ID CSCvu03730 - sdn-network-infra-iwan 인증서가 설치되지 않았기 때문에 eWLC가 Cisco DNA Center에서 모니터링되지 않습니다(근본 원인은 pki-broker 클라이언트 인증서가 만료되었기 때문).
- Cisco 버그 ID CSCvr44560 - 참고: IOS-XE에 대해 2099년 이후에 만료되는 CA 인증서에 대한 지원 추가
- Cisco 버그 ID CSCwc99759 - ENH: 8192비트 RSA 인증서 서명 지원 추가

4단계. 텔레메트리 연결 상태를 확인합니다.

다음 명령을 사용하여 텔레메트리 연결이 WLC의 "Active" 상태인지 확인합니다.

```
<#root>

wlc-01#

show telemetry internal connection


Telemetry connection

Address          Port   Transport   State          Profile
-------------------------------------------------------------------
X.X.X.X       25103  tls-native

Active

     sdn-network-infra-iwan
```

또는 Cisco IOS XE Release 17.7 이상에서:

<#root>

```
wlc-01#

show telemetry connection all


Telemetry connections

Index Peer Address               Port  VRF Source Address             State      State Description
----- ------------------------- ----- --- ------------------------- ---------- --------------------
 9825 X.X.X.X                   25103 0   Y.Y.Y.Y

Active

     Connection up
```

X.X.X.X IP 주소는 Catalyst Center Enterprise 인터페이스여야 합니다. Catalyst Center가 VIP로 구성된 경우 엔터프라이즈 인터페이스의 VIP여야 합니다. IP 주소가 올바르고 상태가 "Active"올바른 경우 다음 단계로 진행합니다.

상태가 "Connecting" 인 경우 WLC에서 Catalyst Center로의 HTTPS(Hypertext Transfer Protocol Secure) 연결이 성공적으로 설정되지 않았습니다. 여기에는 여러 가지 이유가 있을 수 있습니다. 가장 일반적인 이유는 다음에 나열되어 있습니다.

4.1. WLC에서 Catalyst Center VIP에 연결할 수 없거나 현재 상태에 "DOWN" 있습니다.

- VIP가 있는 단일 노드에서 클러스터 인터페이스가 다운되면 VIP가 다운됩니다. 클러스터 인터페이스가 연결되었는지 확인합니다.
- WLC가 Enterprise VIP(ICMP/ping)에 연결되어 있는지 확인합니다.
- 다음 명령을 사용하여 Catalyst Center Enterprise VIP가 "UP" 상태인지 확인합니다. **ip a | grep en.**
- 다음 명령을 사용하여 Catalyst Center Enterprise VIP가 올바르게 구성되었는지 확인합니다. **etcdctl get /maglev/config/cluster/cluster_network.**

4.2. WLC가 HA(고가용성)에 있으며 장애 조치 후에는 보증이 작동하지 않습니다.

이는 Catalyst Center에서 HA를 구성하지 않은 경우 발생할 수 있습니다. 이 경우: 인벤토리에서 WLC를 제거하고, HA를 중단하고, 두 WLC를 모두 검색하고, Catalyst Center가 HA를 구성하도록 합니다.

참고: 이 요구 사항은 이후 Catalyst Center 버전에서 변경될 수 있습니다.

4.3. Catalyst Center에서 DNAC-CA 신뢰 지점 및 인증서를 생성하지 않았습니다.

- 이 문제를 해결하려면 2단계와 3단계를 선택합니다.

4.4. Catalyst Center에서 신뢰 지점과 인증서를 sdn-network-infra-iwan 생성하지 않았습니다.

- 2단계와 3단계를 선택하여 이 문제를 해결합니다.

4.5. Catalyst Center에서 보증 구성을 푸시하지 않았습니다.

- 이 명령은 **show network-assurance summary** Network-Assurance를 다음과 같이 **Disabled**표시합니다.

```
<#root>

DC9800-WLC#

show network-assurance summary

-------------------------------------------------
Network-Assurance                       :

Disabled

Server Url                              :
ICap Server Port Number            :
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

- Catalyst Center에서 컨피그레이션을 푸시하는 데 필요하므로 WLC에 Device Controllability(디바이스 제어 기능)가 활성화되어 있는지 확인합니다. 디바이스 제어성은 검색 프로세스에서 활성화하거나, WLC가 인벤토리에 포함되고 Catalyst Center에서 관리되면 활성화할 수 있습니다. 해당 페이지로 **Inventory** 이동합니다. 를 **Device** > **Actions** > **Inventory** > **Edit Device** > **Device Controllability** > **Enable**선택합니다.

4.6. Catalyst Center는 텔레메트리 서브스크립션 컨피그레이션을 푸시하지 않습니다.

- WLC에 명령과 함께 서브스크립션이 있는지 **show telemetry ietf subscription all** 확인합니다.
- 그렇지 않은 경우 2단계와 3단계를 확인하여 이 문제를 해결합니다.

4.7. WLC에서 Catalyst Center 인증서를 확인할 수 없으므로 WLC와 Catalyst Center 간의 TLS 핸드셰이크가 실패합니다.

여러 가지 이유로 인해 발생할 수 있으며, 가장 일반적인 이유는 다음과 같습니다.

4.7.1. Catalyst Center 인증서가 만료 또는 취소되었거나 주체 대체 이름(SAN)에 Catalyst Center IP 주소가 없습니다.

- 인증서가 Catalyst Center Security Best Practices Guide에 지정된 모범 사례와 일치하는지 확인합니다.

4.7.2. CRL(Certificate Revocation List)을 검색할 수 없기 때문에 폐기 검사에 실패합니다.

- DNS 실패, 방화벽 문제, WLC와 CDP(CRL Distribution Point) 간 연결 문제, 알려진 문제 등 CRL 검색이 실패하는 이유는 다양할 수 있습니다.
  - Cisco 버그 ID CSCvr41793 - PKI: CRL 검색은 HTTP Content-Length를 사용하지 않습니다.
  - Cisco 버그 ID CSCvo03458 - CRL에 연결할 수 없는 경우 PKI "revocation check crl none"이 폴백되지 않습니다.
  - Cisco 버그 ID CSCue73820 - PKI 디버그가 CRL 구문 분석 실패에 대해 명확하지 않습니다.

- 이를 해결하려면 DNAC-CA 신뢰 지점**revocation-check none**에서 구성합니다.

4.7.3. 인증서 오류 "피어 인증서 체인이 너무 길어 확인할 수 없음"

- 명령의 출력을 **show platform software trace message mdt-pubd chassis active R** 확인합니다.
- 표시되는 경우 다음**"Peer certificate chain is too long to be verified"**을 확인하십시오.

  Cisco 버그 ID CSCvw09580 - 9800 WLC는 Cisco DNA Center 인증서 체인 깊이(4개 이상)를 취하지 않습니다.

- 이 문제를 해결하려면 Catalyst Center 인증서를 발급한 중간 CA의 인증서를 다음 명령을 사용하여 WLC의 신뢰 지점으로 가져옵니다. **echo | openssl s_client -connect**

  :443 -showcerts

  .

참고: 이렇게 하면 신뢰 체인의 인증서 목록(PEM 인코딩)이 생성되므로 각 인증서는 -----BEGIN CERTIFICATE-----으로 시작합니다. 해결 방법 섹션에서 언급한 URL을 참조하고, DNAC-CA 인증서를 구성하는 단계를 실행하되 루트 CA 인증서는 가져오지 않습니다. 대신 문제가 있는 CA의 인증서를 가져옵니다.

4.7.4. WLC 인증서가 만료되었습니다.

- Catalyst Center 버전이 1.3.3.7 이전 버전이면 WLC 인증서가 만료되었을 수 있습니다. Catalyst Center 버전이 1.3.3.8 이상(2.1.2.6 이상은 아님)인 경우 버전 1.3.3.7 이하에서 업그레이드하기 전에 인증서가 만료된 경우에도 문제가 될 수 있습니다.
- 명령의 출력에서 유효성 종료 날짜를 **show crypto pki certificates sdn-network-infra-iwan** 확인합니다.

4.8. Catalyst Center의 collector-iosxe 서비스가 WLC의 연결을 수락하지 않습니다. 인벤토리 관리자 서비스에서 새 디바이스에 대해 알리지 않았기 때문입니다.

- iosxe-collector에서 알려진 디바이스 목록을 확인하려면 Catalyst Center CLI에서 다음 명령을 입력합니다.

  curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data'

- 호스트 이름 및 IP 주소의 목록만 가져오려면 이 명령을 사용하여 jq로 출력을 구문 분석합니다.

  Catalyst Center 1.3 이상:

  curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data' | jq '.devices[] | .hostName, .mgmtIp'

  Catalyst Center 1.3.1 이하 버전:

  curl -s 'http://collector-iosxe-db.assurance-backend.svc.cluster.local:8077/api/internal/device/data' | jq '.device[] | .hostName, .mgmtIp'

- 이 목록에 WLC가 포함되어 있지 않으면 collector-iosxe 서비스를 다시 시작하고 이 문제가 해결되는지 확인합니다.
- collector-iosxe만 다시 시작해도 문제가 해결되지 않을 경우, collector-manager 서비스를 다시 시작하면 이 문제를 해결하는 데 도움이 됩니다.

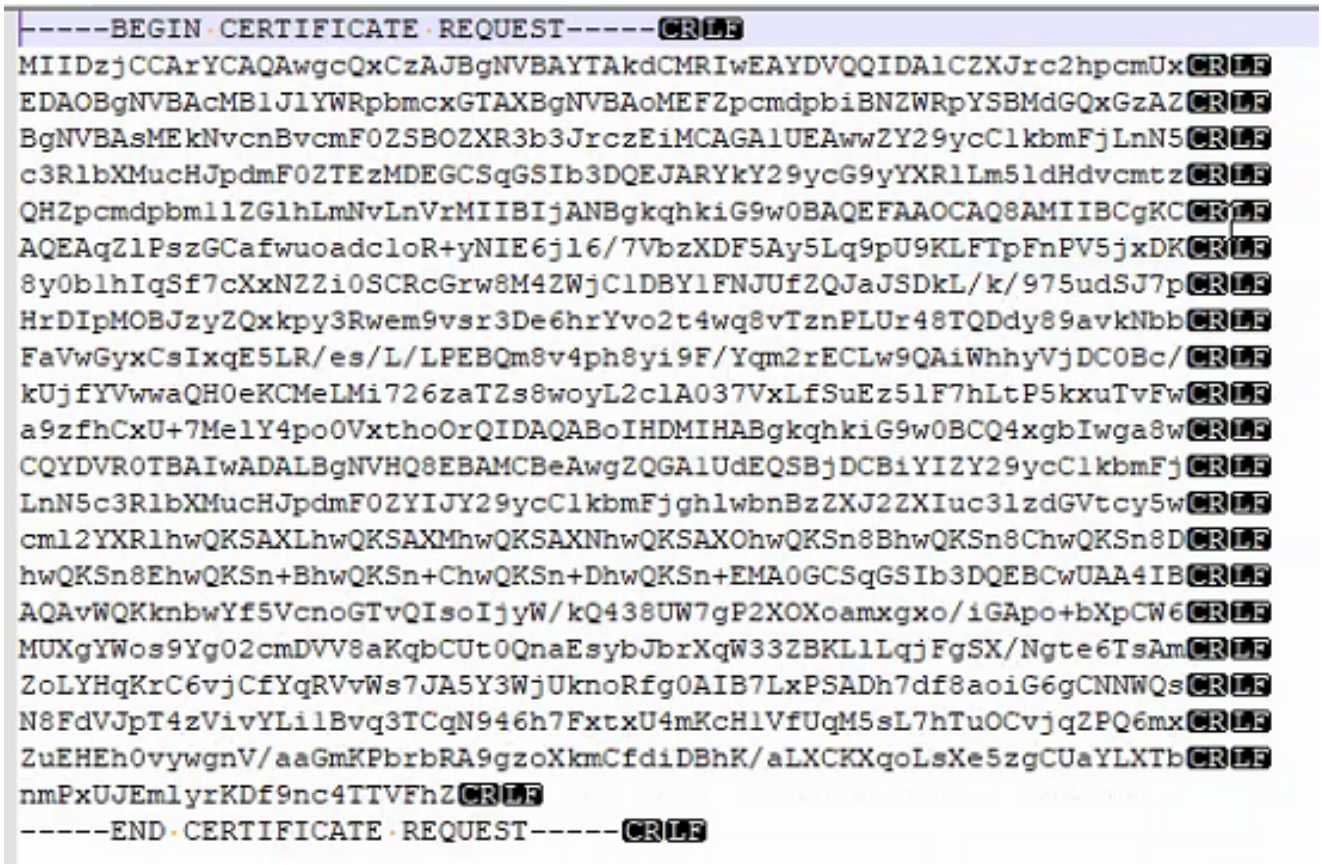
팁: 서비스를 다시 시작하려면 을 **magctl service restart -d** 입력합니다.

- 명령의 출력이 여전히 **show telemetry internal connection** 지속되면 "Connecting"로그에 **collector-iosxe** 오류를 기록합니다.

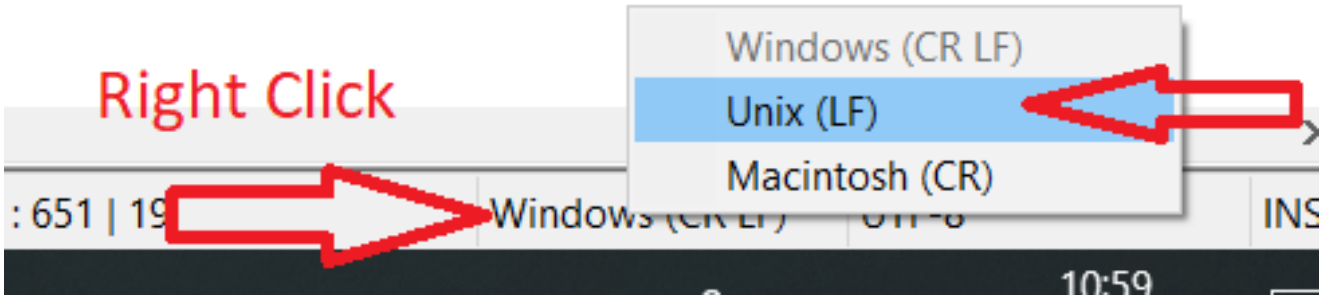
팁: 로그 파일을 추적하려면 명령을 **magctl service logs -rf** 입력합니다. 이 경우, **magctl service logs -rf collector-iosxe | lql**.

```
40 | 2021-04-29 08:09:15 | ERROR | pool-15-thread-1 | 121 | com.cisco.collector.ndp.common.KeyStor
      at java.util.Base64$Decoder.decode0(Base64.java:714)
```

- 이 오류가 표시되면 Notepad++에서 .key 및 .pem(certificate chain) 파일인 Catalyst Center에 추가된 인증서를 엽니다. Notepad(메모장++에서 로 **View** > **Show Symbol** > **Show All Characters**이동합니다.
- 다음과 같은 경우:



다음으로 이동:



인증서를 저장합니다.

- Catalyst Center에 다시 추가하고 명령이 **show telemetry internal connection** 표시되는지 확인합니다 "Active".

4.9. 관련 결함

- Cisco 버그 ID CSCvs78950 - 'Connecting' 상태의 eWLC와 Wolverine 클러스터 원격 분석 연결
- Cisco 버그 ID CSCvr98535 - Cisco DNA Center는 PKI에 대한 HTTP 소스 인터페이스를 구성하지 않습니다. eWLC 원격 분석은 '연결' 상태를 유지합니다.

5단계. 텔레메트리 상태가 활성 상태이지만 보증에 데이터가 표시되지 않습니다.

다음 명령을 사용하여 텔레메트리 내부 연결의 현재 상태를 확인합니다.

```
<#root>

dna-9800#

show telemetry internal connection


Telemetry connection

Address          Port   Transport   State          Profile
------------------------------------------------------------------------
X.X.X.X       25103  tls-native

Active

        sdn-network-infra-iwan
```

가능한 결함:

- Cisco 버그 ID CSCvu27838 - eWLC를 사용하는 9300에서 무선 보증 데이터를 제공하지 않습니다.

- Cisco 버그 ID CSCvu00173 - 1.3.3.4로 업그레이드한 후 보증 API 경로가 등록되지 않았습니다(eWLC에만 국한되지 않음).

해결 방법

필요한 컨피그레이션의 일부 또는 전체가 WLC에 없는 경우, 컨피그레이션이 없는 이유를 확인해 보십시오. 일치하는 결함이 있는 경우 관련 로그 파일을 확인합니다. 그런 다음 이러한 옵션을 해결 방법으로 고려하십시오.

Catalyst Center 버전 2.x

Catalyst Center GUI에서 해당 페이지로 **Inventory** 이동합니다. 를 **WLC** > **Actions** > **Telemetry** > **Update Telemetry Settings** > **Force Configuration Push** > **Next** > **Apply**선택합니다. 그런 다음 WLC에서 재동기화 프로세스를 완료할 때까지 잠시 기다립니다. Catalyst Center에서 이 문서의 Background Information 섹션에 언급된 컨피그레이션을 푸시하는지 확인하고 이 명령을 사용하여 WLC에 보증 컨피그레이션이 있는지 **show network-assurance summary** 확인합니다.

Catalyst Center 버전 1.x

이전 GUI 방법이 여전히 원하는 효과를 얻지 못하는 경우 Catalyst Center 2.x에도 이 방법을 사용할 수 있습니다.

- 신뢰 sdn-network-infra-iwan 지점 및/또는 인증서가 누락되었습니다.

  Catalyst Center Assurance 인증서 및 서브스크립션을 수동으로 설치하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

- 네트워크 보증 구성이 없습니다.

  WLC에서 Catalyst Center 엔터프라이즈 VIP 주소에 연결할 수 있는지 확인합니다. 그런 다음 다음 다음 예제와 같이 섹션을 수동으로 구성합니다.

```
conf t
network-assurance url https://X.X.X.X
network-assurance icap server port 32626
network-assurance enable
network-assurance na-certificate PROTCOL_HTTP X.X.X.X /ca/ pem
```

> 참고: 다섯 번째 행에서 X.X.X.X와 /ca/ 사이의 공백 및 /ca/와 pem 사이의 공백을 확인합니다.

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.