ACI L3Out 문제 해결 - 직접 연결된 서브넷 PcTag1

목차

소개

이 문서에서는 외부 EPG의 적절한 컨피그레이션 없이 직접 연결된 L3Out 서브넷에서 시작된 트래픽이 계약 삭제로 이어질 수 있는 시나리오를 설명합니다.

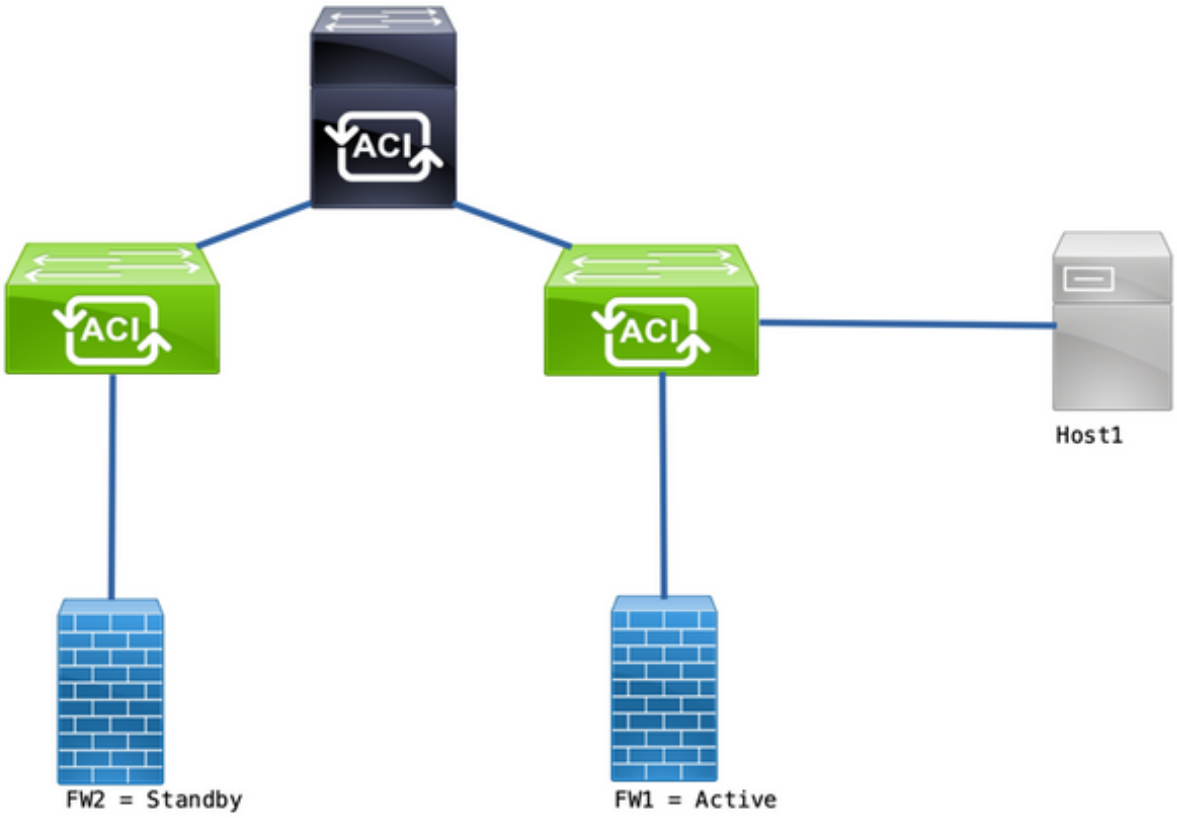
배경 정보

ACI L3out 백서의 "**0.0.0.0/0으로 직접 연결된 서브넷**에 **대한 예외**" 섹션은 pcTag 1과 관련하여 이 동작을 호출합니다.

"...기본적으로 직접 연결된 서브넷에는 계약을 우회하기 위한 특수 pcTag인 pcTag 1이 할당됩니다. 이는 코너 케이스 시나리오에서 경로 프로토콜 통신을 암시적으로 허용하기 위한 것입니다. 그러나... 이로 인해 보안 문제가 발생할 수 있습니다. 따라서 이 동작은 Cisco 버그 ID CSCuz를 통해 자세히 설명됩니다12913 - 해결 방법도 소개합니다."

시나리오

토폴로지 및 컨피그레이션



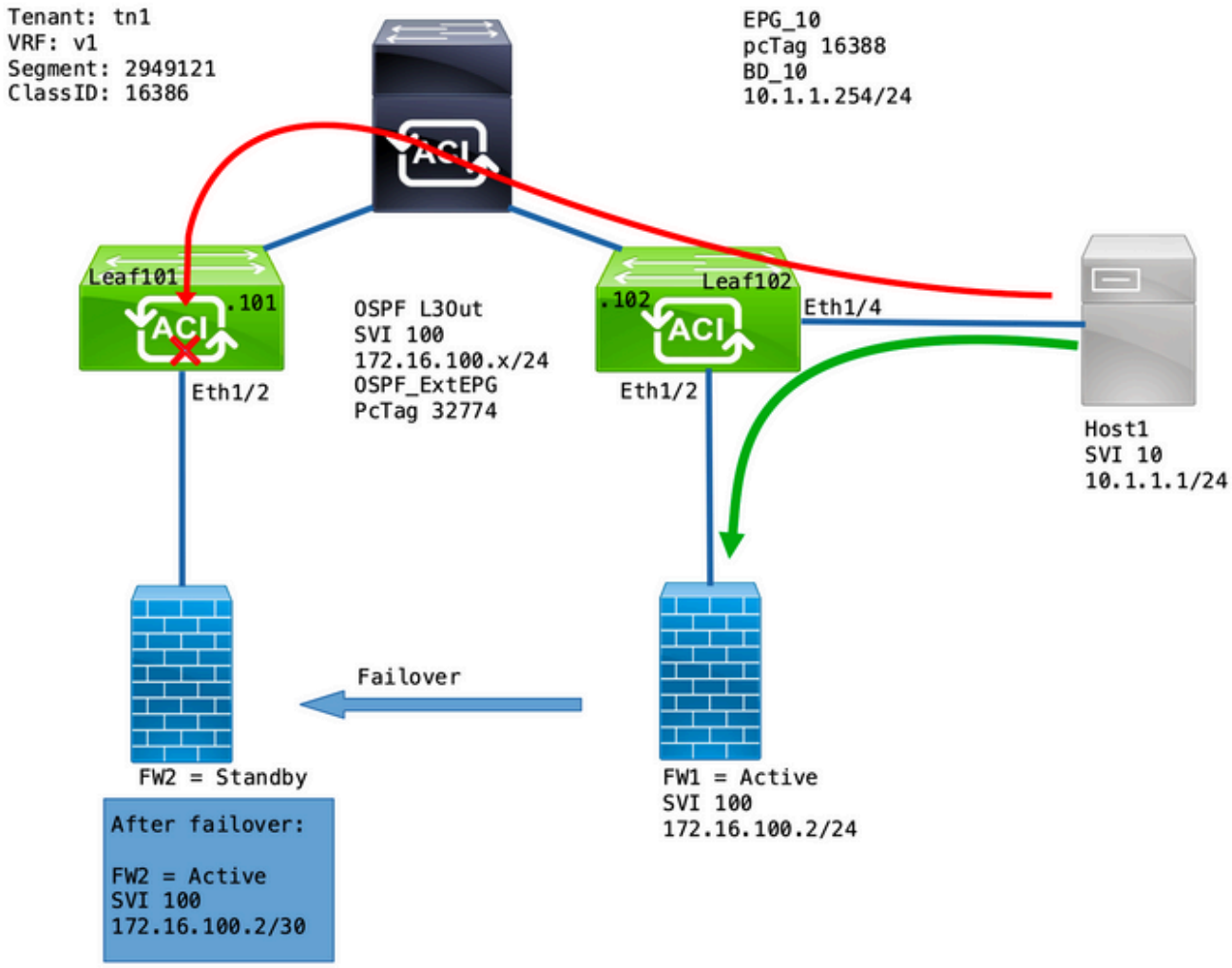
토폴로지

- 방화벽(FW)은 NAT(Network Address Translation)로 구성됩니다.
- ACI 패브릭으로 전송되는 모든 트래픽은 ACI와 OSPF 인접성을 형성하는 FW의 IP에서 비롯됩니다.
- 외부 EPG에는 외부 EPG용 외부 서브넷으로 구성된 0.**0.0.0/0 네트워크가 있습니다**.
- contract는 내부 EPG와 외부 EPG 간의 통신을 위한 것입니다.

관찰된 문제

FW1을 활성 디바이스로 사용하면 트래픽이 예상대로 작동합니다. 관찰된 방울이 없습니다.

방화벽 서비스가 FW2로 장애 조치되면 연결이 끊어집니다. 10.1.1.1과 172.16.100.2는 더 이상 통신할 수 없습니다.



이슈 심층 분석

Leaf101에서 ELAM 캡처를 사용하면 Host1에서 FW2로의 트래픽이 삭제되었는지 확인할 수 있습니다.

다음 ELAM 옵션이 사용되었습니다.

```
leaf101# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 14 out-select 1
module-1(DBG-elam-insel14)# set inner ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel14)# start
module-1(DBG-elam-insel14)# status
```

또한 트리거되면 e-report에서 조회 결과를 볼 수 있습니다.

```
<snip>
================================================================================================================
================================================
Captured Packet
================================================================================================================
================================================
<snip>
```

```
------------------------------------------------------------------------------------------------
------------------------------------------------------
Inner L3 Header
------------------------------------------------------------------------------------------------
------------------------------------------------------
L3 Type : IPv4
DSCP : 0
Don't Fragment Bit : 0x0
TTL : 254
IP Protocol Number : ICMP
Destination IP                 : 172.16.100.2   <<<----
Source IP                      : 10.1.1.1   <<<----
<snip>
================================================================================================
======================================================
Contract Lookup ( FPC )
================================================================================================
======================================================

------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Lookup Key
------------------------------------------------------------------------------------------------
------------------------------------------------------
IP Protocol : ICMP( 0x1 )
L4 Src Port : 2048( 0x800 )
L4 Dst Port : 52579( 0xCD63 )
sclass (src pcTag)                      : 16388( 0x4004 )   <<<----
dclass (dst pcTag)                      : 16386( 0x4002 )   <<<----
<snip>

------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Result
------------------------------------------------------------------------------------------------
------------------------------------------------------
Contract Drop                          : yes   <<<----
Contract Logging : yes
Contract Applied : no
Contract Hit : yes
Contract Aclqos Stats Index : 81824
( show sys int aclqos zoning-rules | grep -B 9 "Idx: 81824" )
```

이 보고서는 플로우가 다음 세부사항과 함께 계약 삭제되었음을 보여줍니다.

- SCLASS16388 EPG_10의 pcTag입니다.
- DCLASS는 16386 v1의 pcTag입니다.

그런 다음 VRF에 대한 영역 지정 규칙을 검증합니다.

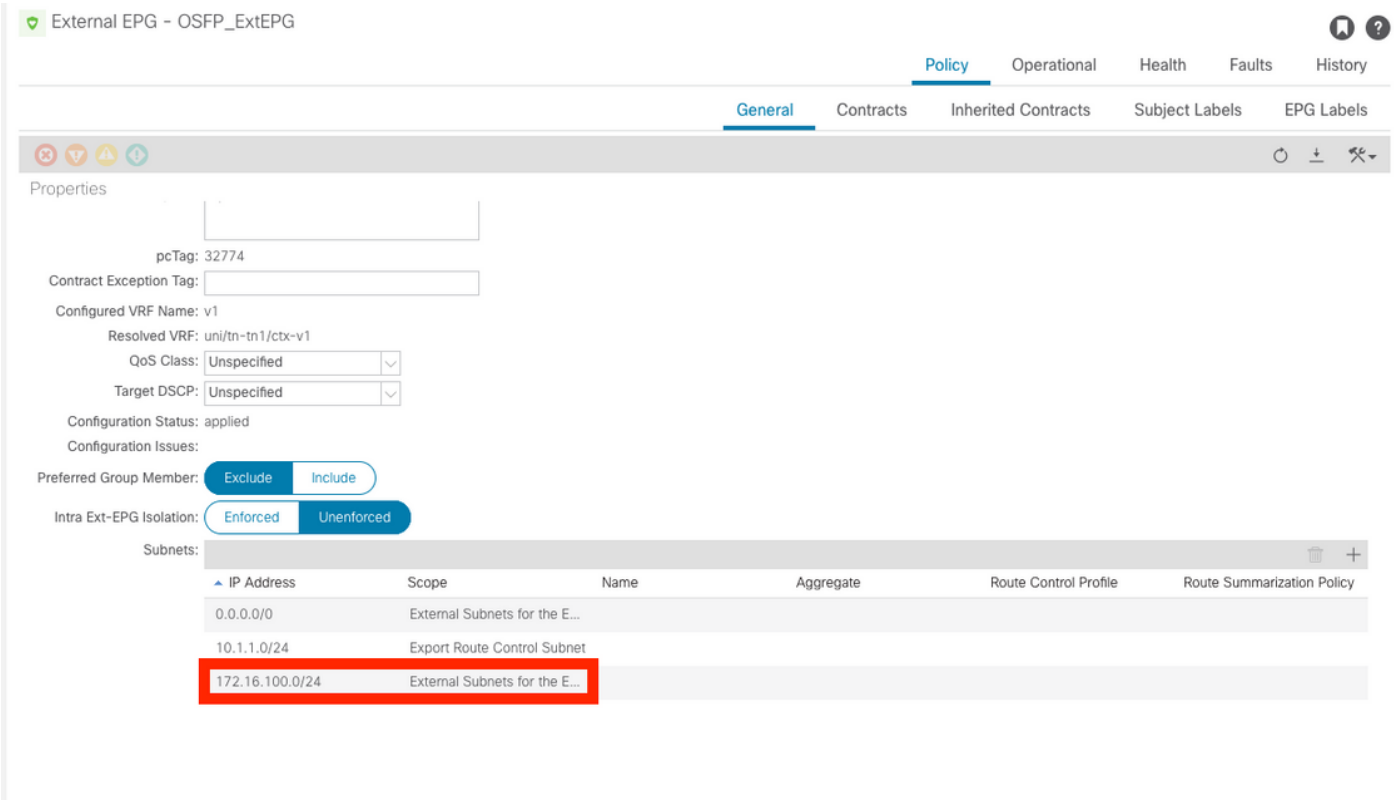
```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  |       Name       |
Action  |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------------------+-------
---+----------------------+
|   4131  |   0    |   15   | implicit | uni-dir | enabled | 2949121 |                  |
deny,log | any_vrf_any_deny(22) |
|   4130  |   0    |   0    | implarp  | uni-dir | enabled | 2949121 |                  |
permit  |  any_any_filter(17)  |
|   4129  |   0    |   0    | implicit | uni-dir | enabled | 2949121 |                  |
deny,log |   any_any_any(21)    |
```

```
|   4132  |   0    | 49155  | implicit | uni-dir | enabled | 2949121 |                 |
permit  |   any_dest_any(16)   |
|   4112  | 16386  | 16388  | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
|   4133  | 16388  |   15   | default  | uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+-----------------+-------
---+----------------------+
```

EPG_10(16388)에서 OSPF L3Out 뒤의 네트워크로 통신을 위한 계약이 있습니다(0.0.0.0/0 = 15). 그러나 172.16.100.2의 트래픽은 VRF v1의 pcTag(16386) 아래에 태그가 지정됩니다.

솔루션

OSPF Ext_EPG 아래에 L3Out의 직접 연결된 서브넷을 추가합니다.



이 덧셈은 2가지 효과를 가집니다.

1. 직접 연결된 서브넷의 트래픽은 OSPF_ExtEPG pcTag(32774) 아래에 태그가 지정됩니다
2. EPG_10 및 OSPF_ExtEPG를 오가는 흐름을 허용하는 규칙이 추가됩니다

```
leaf102# show zoning-rule scope 2949121
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+ | Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt |
Scope | Name | Action | Priority | +---------+--------+--------+----------+----------------+----
-----+---------+------------------+----------+----------------------+ | 4131 | 0 | 15 | implicit
| uni-dir | enabled | 2949121 | | deny,log | any_vrf_any_deny(22) | | 4130 | 0 | 0 | implarp |
uni-dir | enabled | 2949121 | | permit | any_any_filter(17) | | 4129 | 0 | 0 | implicit | uni-
dir | enabled | 2949121 | | deny,log | any_any_any(21) | | 4132 | 0 | 49155 | implicit | uni-dir
| enabled | 2949121 | | permit | any_dest_any(16) | | 4112 | 16386 | 16388 | default | uni-dir |
enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | | 4133 | 16388 | 15 | default |
uni-dir | enabled | 2949121 | tn1:EPG-to-L3Out | permit | src_dst_any(9) | |   4134   | 16388  |
32774  | default  |     bi-dir     | enabled | 2949121 | tn1:EPG-to-L3Out |  permit  |
src_dst_any(9)    |  <<<----
```

```
|   4135  | 32774  | 16388  | default  | uni-dir-ignore | enabled | 2949121 | tn1:EPG-to-L3Out |
permit  |    src_dst_any(9)    |  <<<----
+---------+--------+--------+----------+----------------+---------+---------+-----------------
+----------+----------------------+
```

설명

FW와 호스트가 동일한 leaf에 연결될 때(L3Out 서브넷 추가 없음) 이 문제가 발생하는 이유는 직접 연결된 서브넷에서 모든 계약을 우회하는 특수 pcTag 1을 사용하기 때문입니다. 이는 코너 케이스 시나리오에서 경로 프로토콜 통신을 암시적으로 허용하기 위한 것입니다.

이러한 트리거를 사용하여 Leaf102에서 172.16.100.2에서 10.1.1.1로의 트래픽 흐름을 포착할 수 있습니다.

```
leaf102# vsh_lc
module-1# debug platform internal roc elam asic 0
module-1(DBG-elam)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 172.16.100.2 dst_ip 10.1.1.1
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

이 보고서는 조회 결과를 표시합니다.

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
=========================================================
                                                                  Captured Packet
================================================================================================================
=========================================================

----------------------------------------------------------------------------------------------------------------
---------------------------------------------------
Outer L3 Header
----------------------------------------------------------------------------------------------------------------
---------------------------------------------------
L3 Type                       : IPv4
IP Version                    : 4
DSCP                          : 0
IP Packet Length              : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit            : not set
TTL                           : 255
IP Protocol Number            : ICMP
IP CheckSum                   : 32320( 0x7E40 )
Destination IP                : 10.1.1.1      <<<----
Source IP                     : 172.16.100.2  <<<----

================================================================================================================
=========================================================
                                                                    Contract Lookup ( FPC )
```

```
================================================================================================================
================================================
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 0( 0x0 )
L4 Dst Port                              : 19821( 0x4D6D )
sclass (src pcTag)                       : 1( 0x1 )           <<<----
dclass (dst pcTag)                       : 16388( 0x4004 )    <<<----
src pcTag is from local table            : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet           : no
If yes, Contract is not applied here because it is flooded

--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Result
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Drop                            : no  <<<----
Contract Logging                         : no
Contract Applied                         : no  <<<----
Contract Hit                             : yes
Contract Aclqos Stats Index              : 81903
```

반환 플로우를 검증하려면

```
module-1(DBG-elam-insel6)# trigger reset
module-1(DBG-elam)# trigger init in-select 6 out-select 1
module-1(DBG-elam-insel6)# set outer ipv4 src_ip 10.1.1.1 dst_ip 172.16.100.2
module-1(DBG-elam-insel6)# start
module-1(DBG-elam-insel6)# status
 ELAM STATUS
===========
Asic 0 Slice 0 Status Triggered
```

반환 흐름의 조회 결과:

```
module-1(DBG-elam-insel6)# ereport
Python available. Continue ELAM decode with LC Pkg
 ELAM REPORT
================================================================================================================
================================================
                                                                        Captured Packet
================================================================================================================
================================================
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Outer L3 Header
--------------------------------------------------------------------------------------------------------
-----------------------------------------------------
L3 Type                        : IPv4
IP Version                     : 4
DSCP                           : 0
IP Packet Length               : 84 ( = IP header(28 bytes) + IP payload )
Don't Fragment Bit             : not set
```

```
TTL                          : 255
IP Protocol Number           : ICMP
IP CheckSum                  : 32198( 0x7DC6 )
Destination IP               : 172.16.100.2  <<<----
Source IP                    : 10.1.1.1      <<<----

================================================================================================================
=====================================================
                                                                        Contract Lookup ( FPC )
================================================================================================================
=====================================================

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Lookup Key
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
IP Protocol                              : ICMP( 0x1 )
L4 Src Port                              : 2048( 0x800 )
L4 Dst Port                              : 18134( 0x46D6 )
sclass (src pcTag)                       : 16388( 0x4004 ) <<<----
dclass (dst pcTag)                       : 1( 0x1 )        <<<----
src pcTag is from local table            : yes
derived from a local table on this node by the lookup of src IP or MAC
Unknown Unicast / Flood Packet           : no
If yes, Contract is not applied here because it is flooded

----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Result
----------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
Contract Drop                            : no    <<<----
Contract Logging                         : no
Contract Applied                         : no    <<<----
Contract Hit                             : yes
Contract Aclqos Stats Index              : 81903
```

이 표에는 Gen2 스위치의 예상 동작이 요약되어 있습니다.

시나리오	방향성	계약 폐기	계약 삭제 없음
동일한 리프 전반 VRF 정책 시행: 둘 다	X~L3Out		X
	L3Out - X		X
2개 리프 노드 간 VRF 정책 시행: 인그레스	X~L3Out	X	
	L3Out - X		X
2개 리프 노드 간 VRF 정책 시행: 이그레스	X~L3Out		X
	L3Out - X		X

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.