ASAvでのレイヤ2サービスグラフ設定の設定と確認

内容

はじめに

このドキュメントでは、シスコアプリケーションセントリックインフラストラクチャ(ACI)でレイヤ2サービスグラフ(L2SP)設定を設定および確認する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ACIでのレイヤ3サービスグラフの動作の仕組みについて
- ACIでのエンドポイントポリシーグループ、ブリッジドメイン、およびコントラクトの設定方法に関する理解
- トランスペアレントファイアウォールとして(Adaptive Security Applicance Virtual)ASAvを設定する方法についての理解

使用するコンポーネント

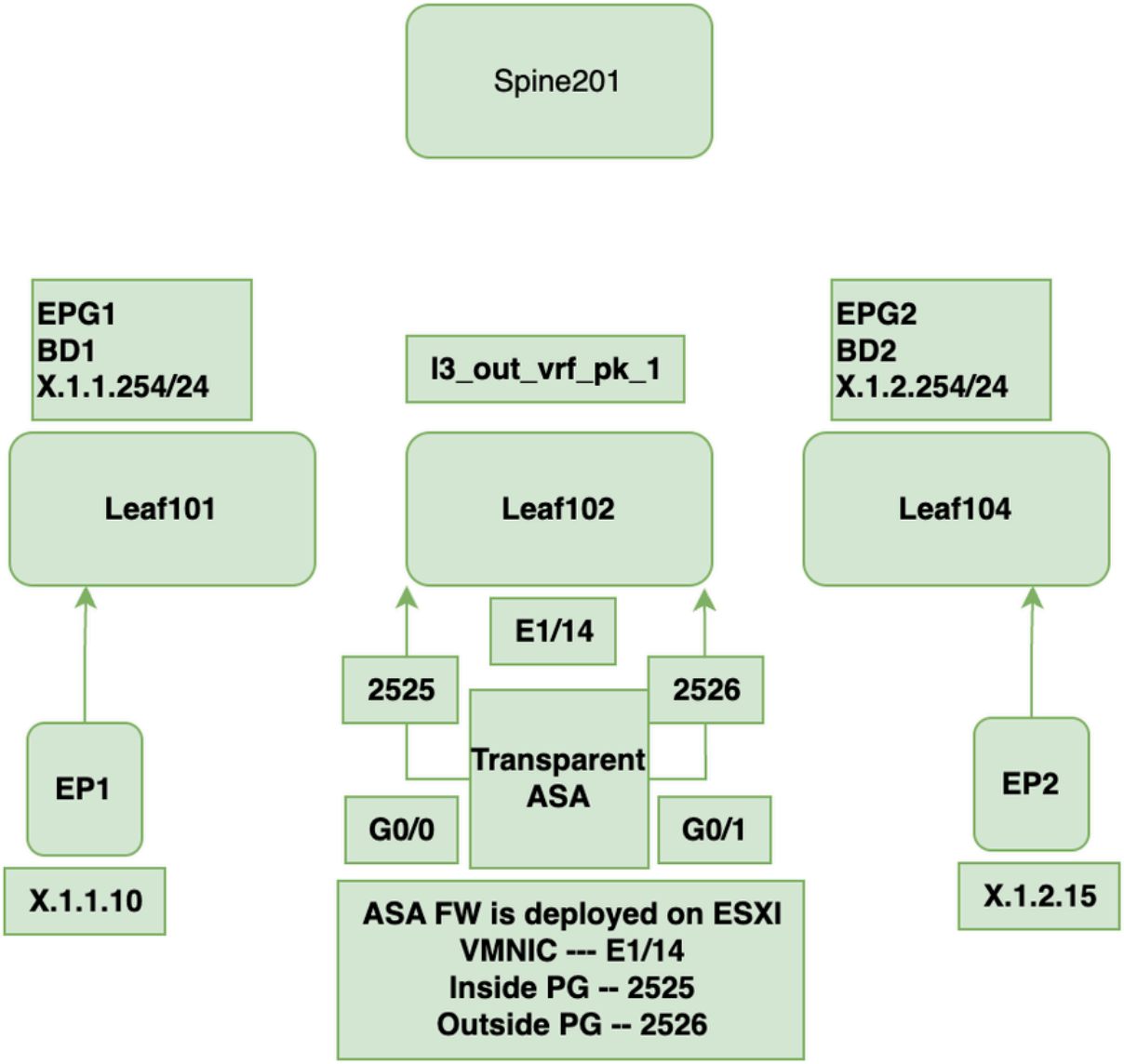
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- APICバージョン：6.0(3g)
- リーフH/W:N9K-C93180YC-FX

- リーフS/W:n9000-16.0(3g)
- リーフノード101、102、103
- ESXiサーバに導入されたASAv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

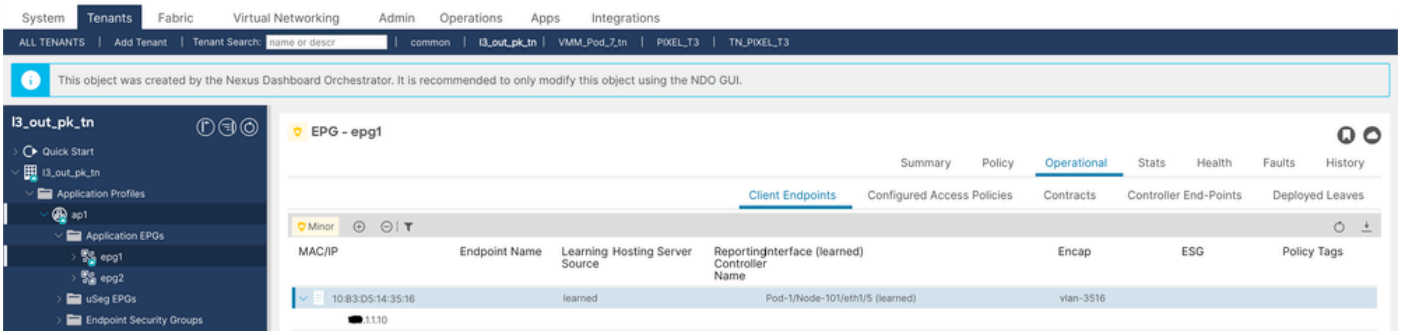
トポロジ



トポロジ

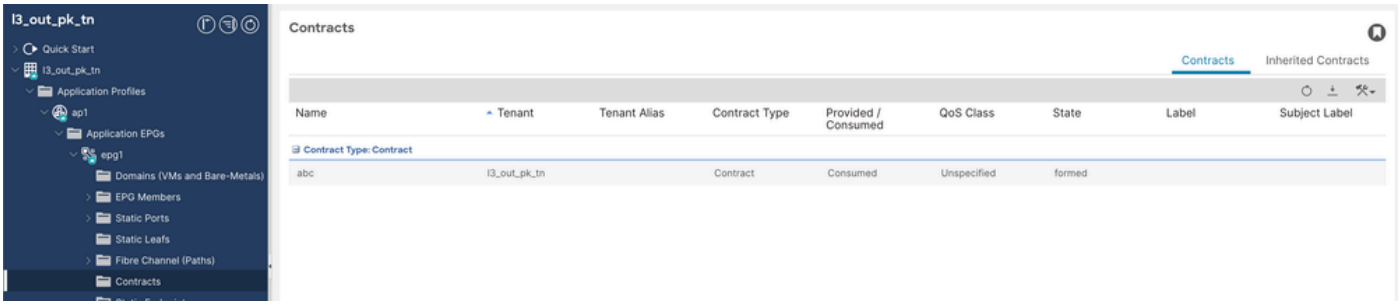
EPG1とEPG2の設定はこのドキュメントに示されていません。手およびエンドポイントを学習する前に設定する必要があります。

1. EPG1 haṣエンドポイントX.1.1.10 learned（ノード101）を検証します。



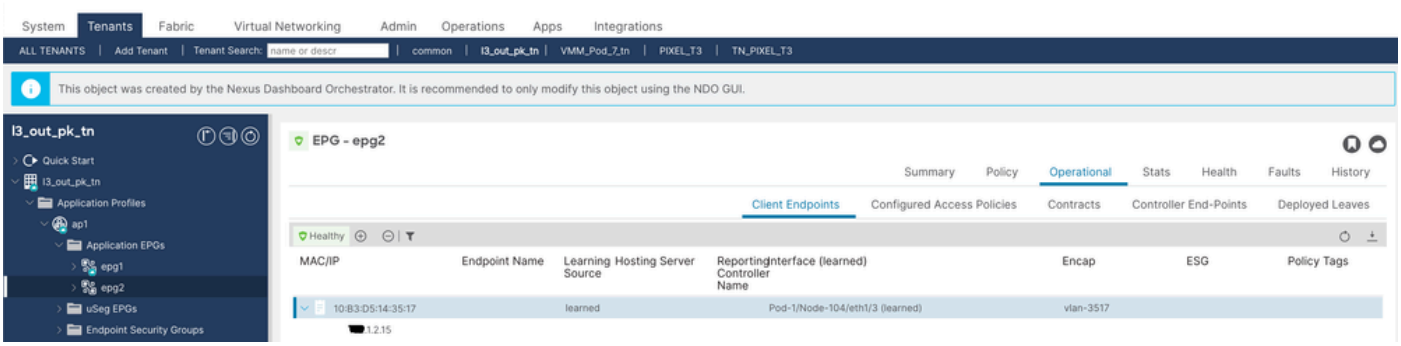
クライアントエンドポイント

2. 契約abcはEPG1で消し込まれます。



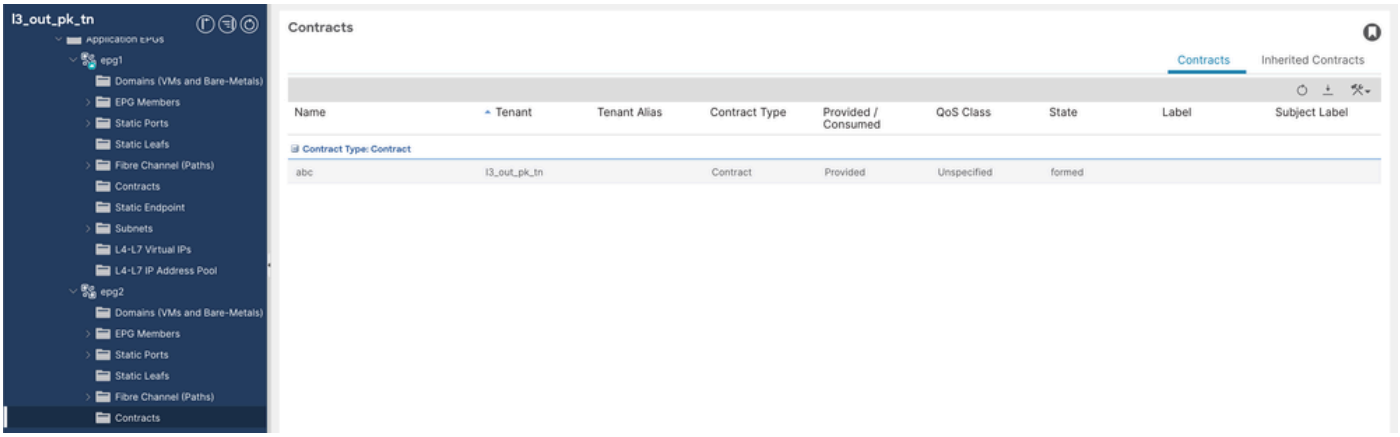
使用済み契約

3. EPG2のエンドポイントがX.1.2.15であることを確認する学習（ノード104）



クライアントエンドポイント

4. abc契約はEPG2によって提供される。



ACIでL2サービスグラフが必要な理由

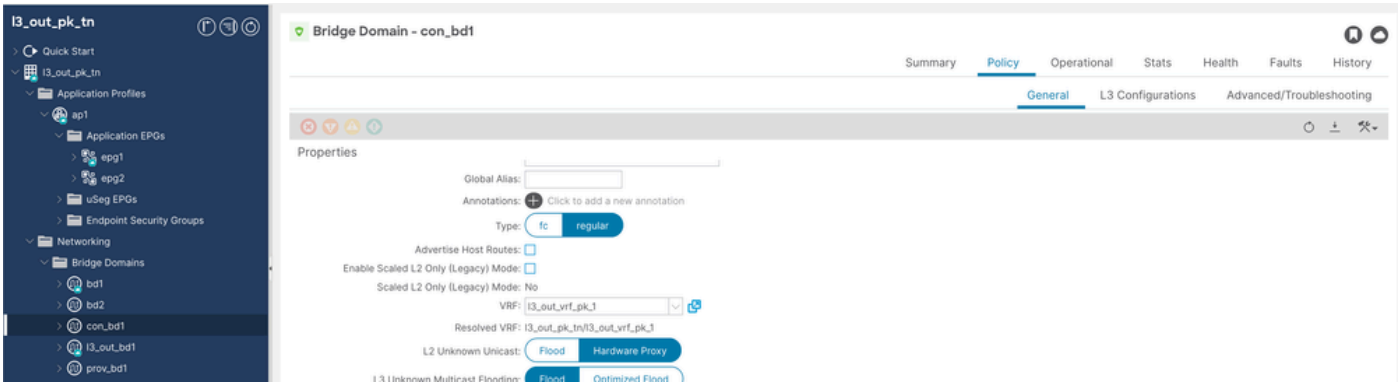
- Cisco ACIでは、L4-L7サービスデバイスをレイヤ3(L3)、レイヤ2(L2)、またはレイヤ1(L1)に挿入できます。
- レイヤ3サービスの挿入：外部デバイス(ファイアウォール、侵入防御システム(IPS)など)がルーティングの決定を行い、IPアドレスに基づいてトラフィックを転送します。
- レイヤ2サービスの挿入：トラフィックはMACアドレスに基づいて転送され、ルーティングは関与しません。これは、透過型ファイアウォールまたはIPSデバイスに便利です。
- L2ポリシーベースルーティング(PBR)は、ACIにIPSやトランスペアレントファイアウォールなどのL2サービスデバイスを挿入するときに使用されます。
- トラフィック転送メカニズムは、L3とL2の両方のPBRで同じままです。
- 主な違いは次のとおりです。
    - L3 PBR：トラフィックがIPアドレスにリダイレクトされる（デバイスはルーティングに参加）。
    - L2 PBR：トラフィックがMACアドレスにリダイレクトされる（デバイスはレイヤ2で動作）。
- L2 PBRでは、適切なトラフィック転送を確保するために、MACアドレスがリーフインターフェイスに静的にバインドされます。

アクティブ/スタンバイまたはアクティブ/アクティブL1/L2 PBRの使用例の詳細については、『PBRホワイトペーパー』を参照してください。

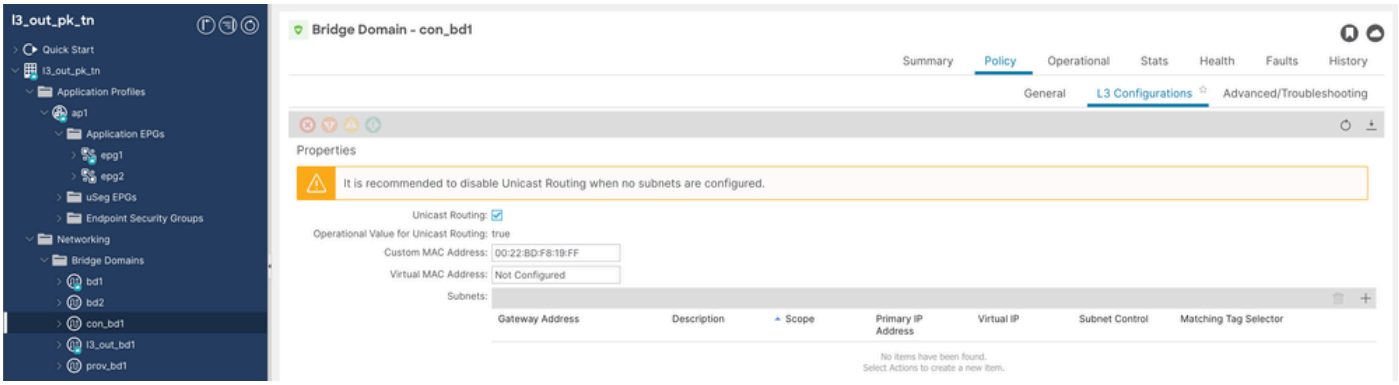
L2サービスグラフの設定

ステップ 1：consumer bdをcon-bd1という名前で設定します。

ユニキャストルーティングを有効にし、L2不明なユニキャストをハードウェアプロキシに設定する必要があります。また、conおよびprovブリッジドメイン(BD)にサブネットは必要ありません。

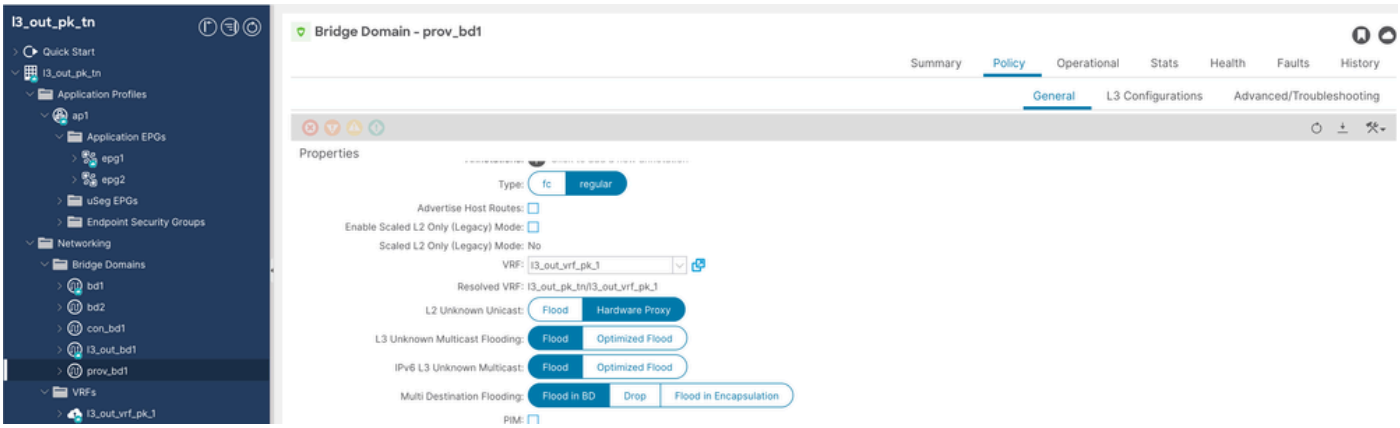


短所BD設定

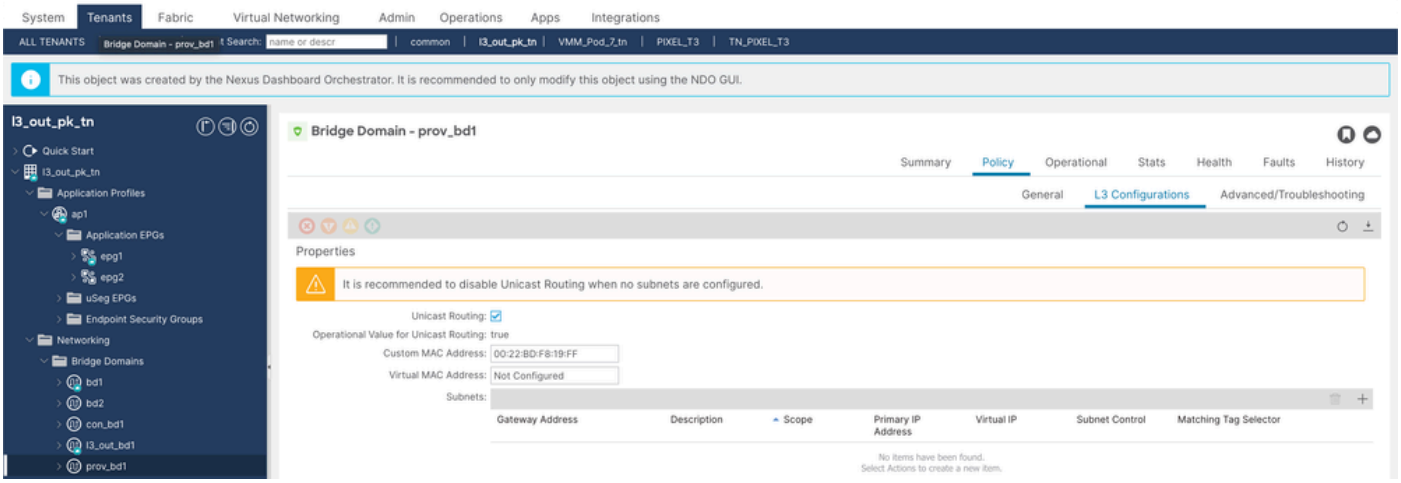


短所BD構成2

ステップ 2：prov-bd1という名前のプロバイダーbdを設定します。



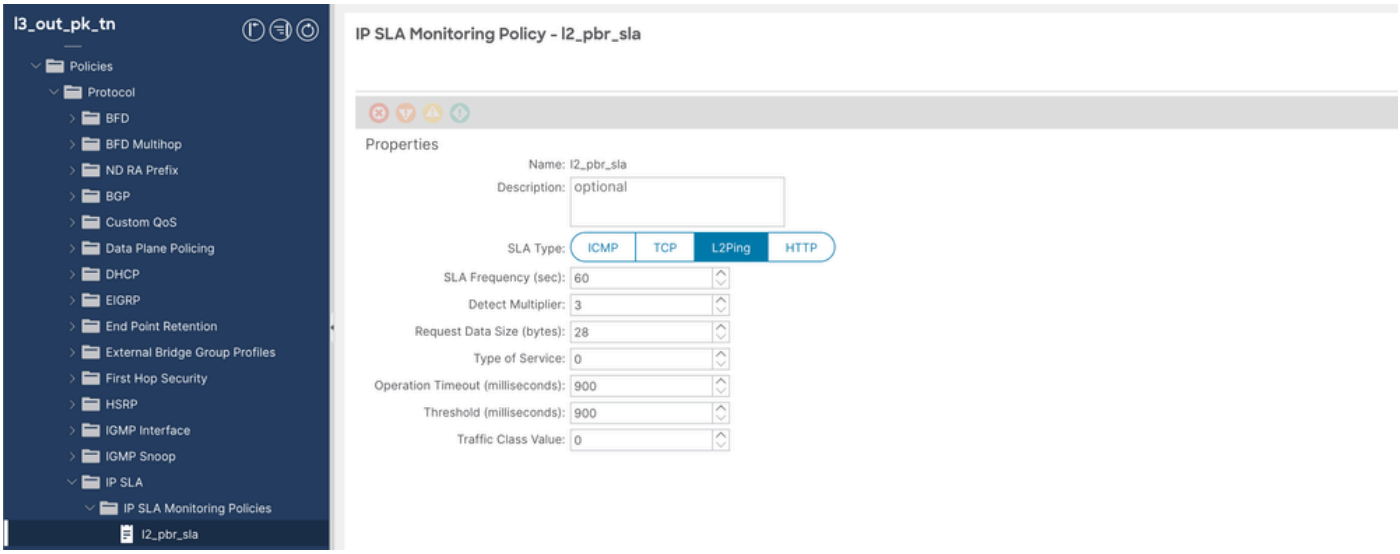
プロビジョニングBD設定



プロビジョニングBD構成2

ステップ 3：SLAタイプL2PingでIPサービスレベル契約(SLA)ポリシーを設定します。

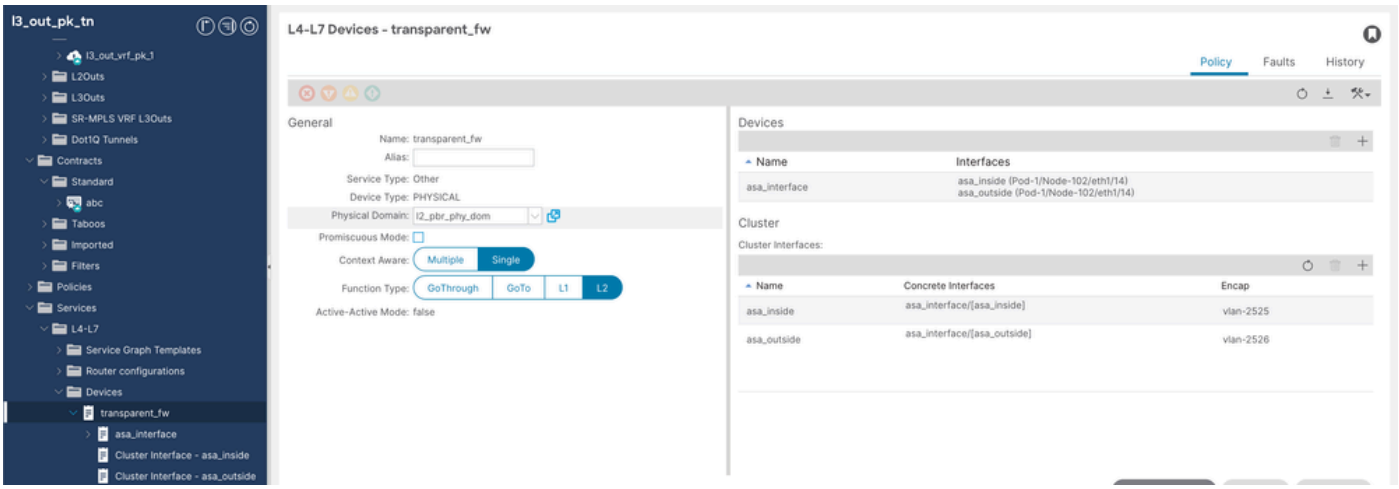
Tenant > Policies > Protocol > IP SLA > IP SLA Monitoring Policiesの順に移動し、右クリックしてポリシーを作成します。



IP SLAポリシー

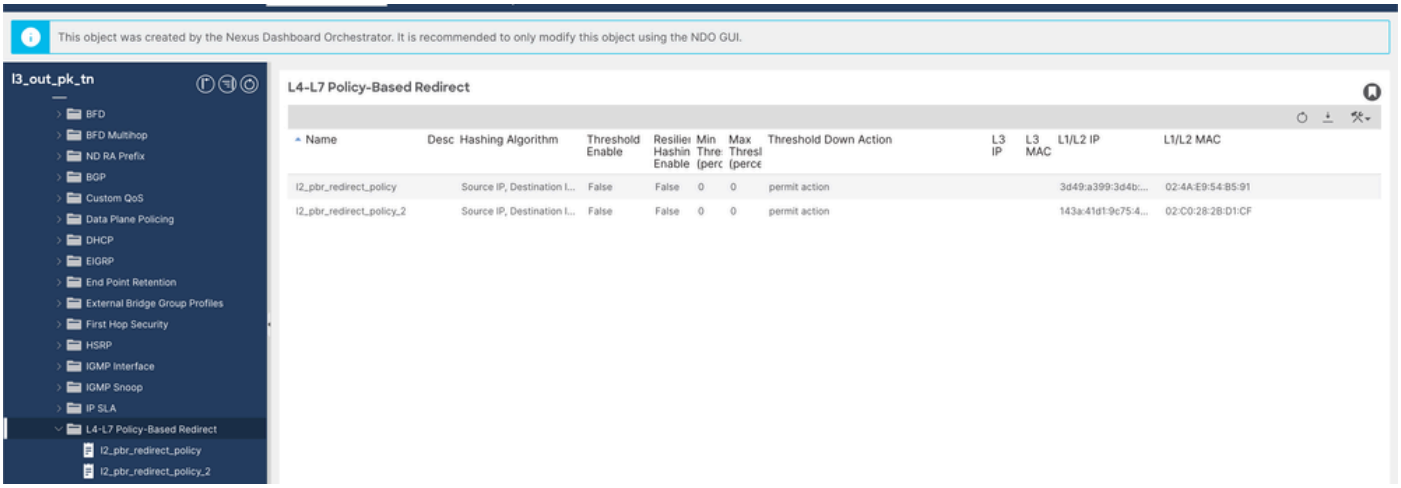
ステップ 4：L4/L7デバイスを設定します。

テナント>サービス>デバイスに移動し、右クリックしてL4-L7デバイスを作成します。



L4-L7デバイス

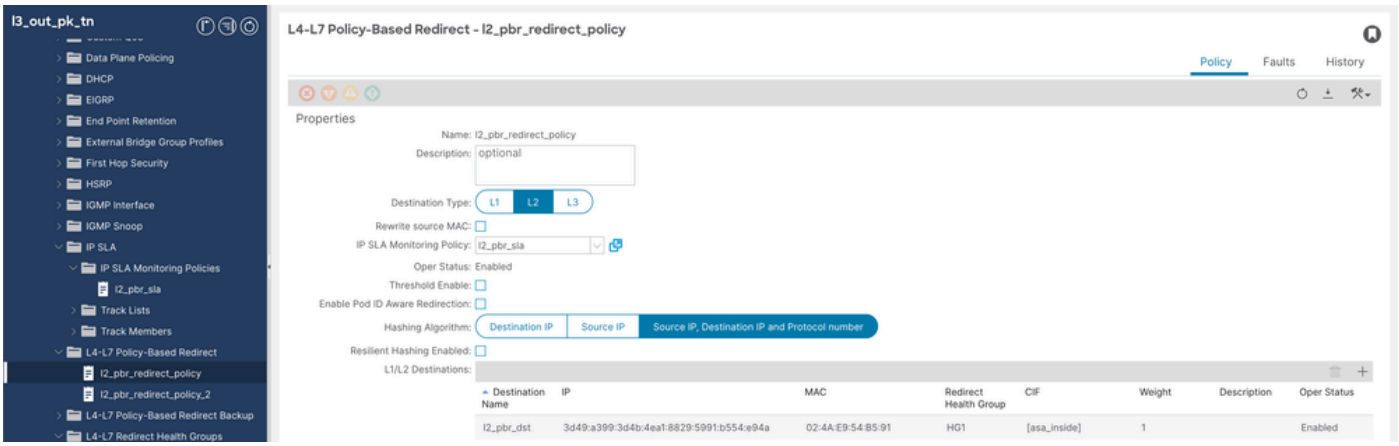
ステップ 5：ポリシーベースのリダイレクトの検証の概要（5aおよび5bの設定後に確認できます）



L4-L7リダイレクトポリシー

ステップ 5.1：適応型セキュリティアプライアンス(ASA)の内部インターフェイスに対して、L4-L7ポリシーベースのリダイレクトポリシーを設定します（MACまたはIPを指定する必要はなく、APIC自体によって入力されます）。

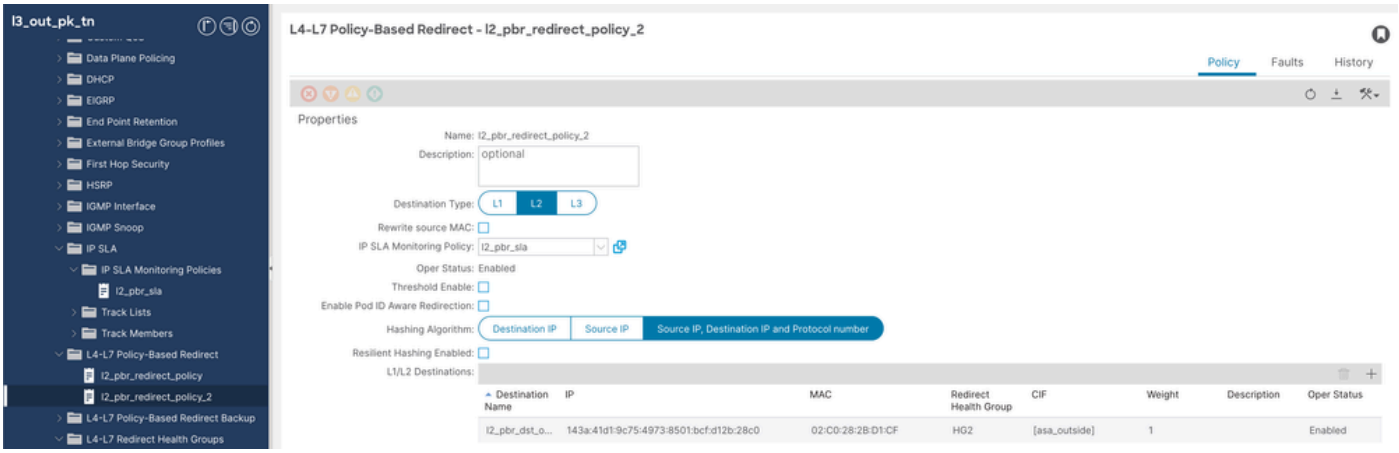
Tenant > Policies > Protocol > L4-L7 Policy based redirectの順に移動し、右クリックしてポリシーを作成します。



L4-L7リダイレクトポリシー設定

ステップ 5.2：ASA外部インターフェイスに対してL4-L7ポリシーベースのリダイレクトポリシーを設定します（MACまたはIPを指定する必要はなく、APIC自体によって入力されます）。

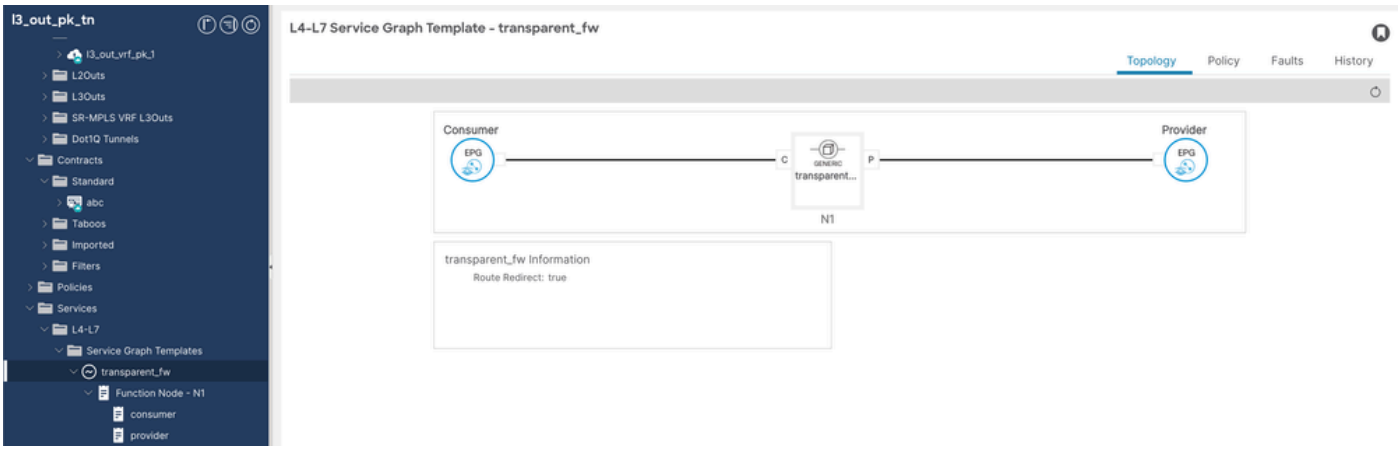
Tenant > Policies > Protocol > L4-L7 Policy based redirectの順に移動し、右クリックしてポリシーを作成します。



L4-L7リダイレクトポリシー設定2

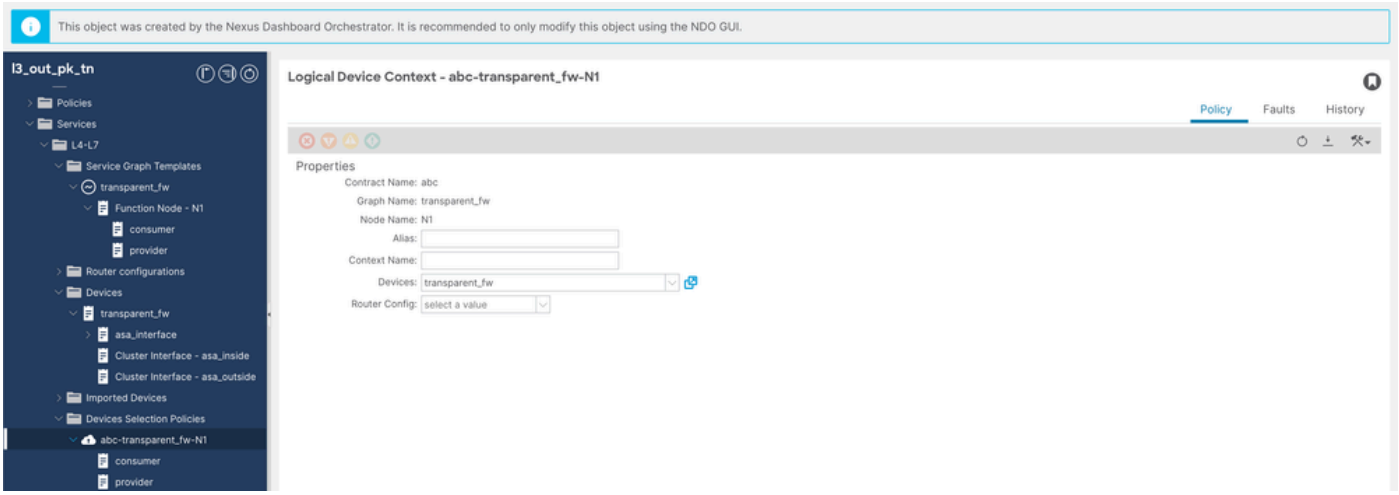
手順 6：サービスグラフテンプレートを設定します。

テナント>サービス>サービスグラフテンプレートに移動し、右クリックしてL4-L7サービスグラフテンプレートを作成します。



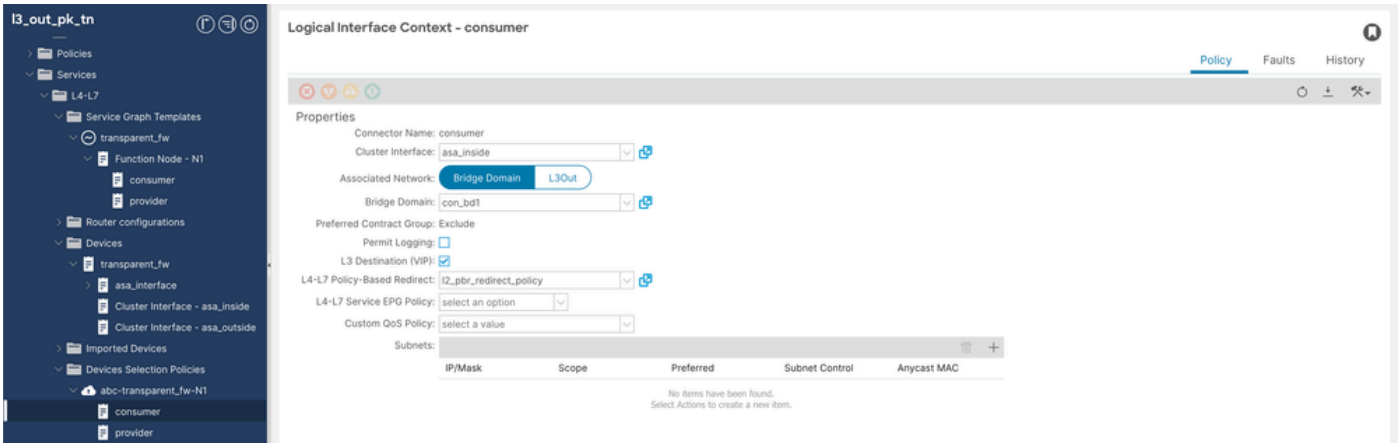
手順 7：デバイス選択ポリシーを設定します。

Tenant > Services > Device Selection Policyの順に移動し、右クリックしてDevice Selection Policyを作成します。



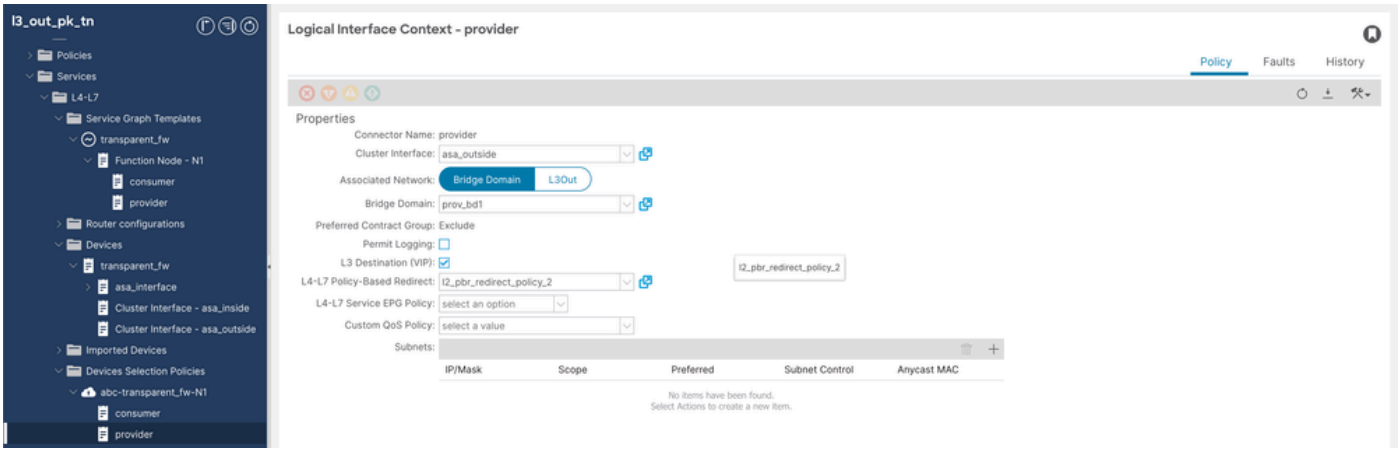
サービスグラフ構成2

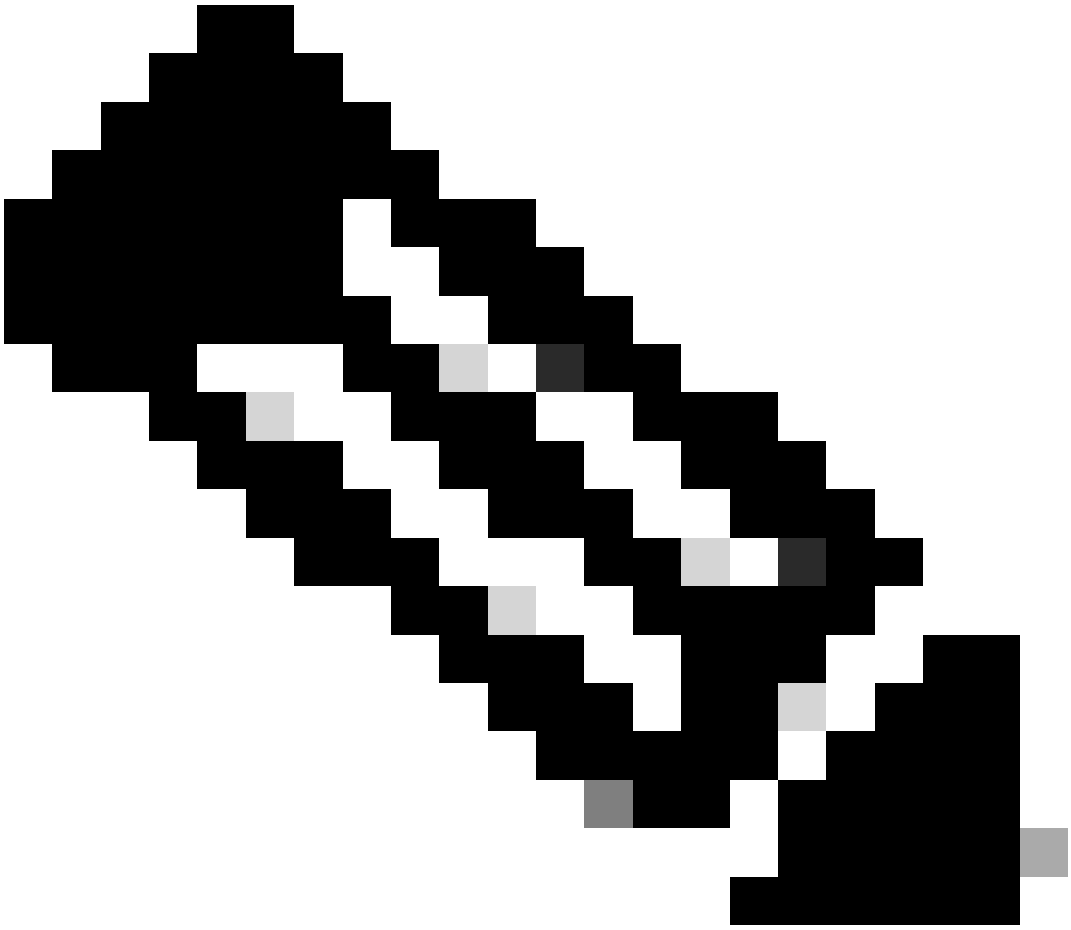
++コンシューマ論理インターフェイスコンテキスト



デバイス選択ポリシーコンシューマ構成

++プロバイダー論理インターフェイスコンテキスト



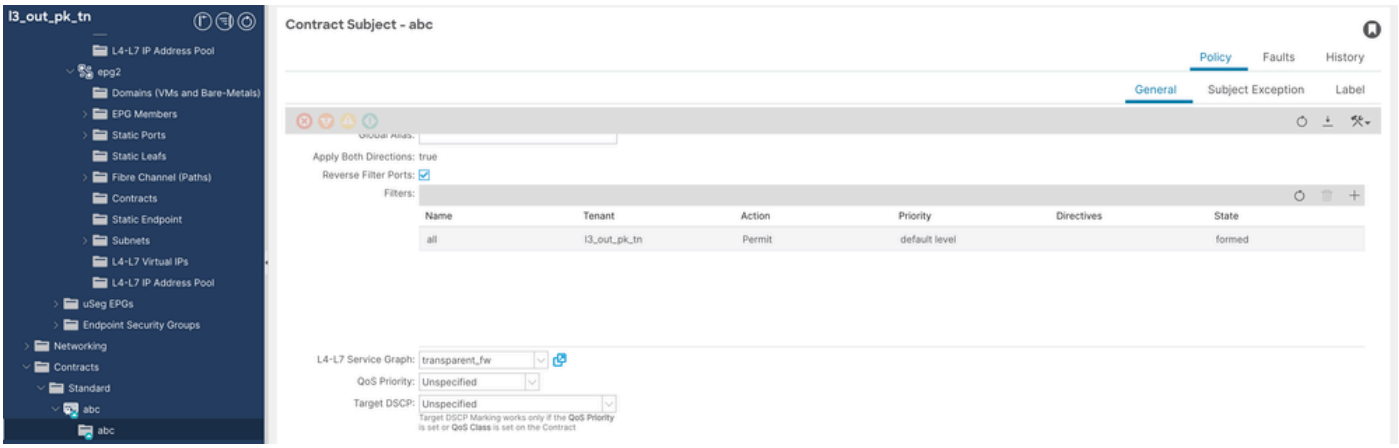


注：サービスグラフ適用オプションを使用する場合に自動的に作成するデバイス選択ポリシー。

ステップ 8：abc件名を契約するには、PBRを適用します。

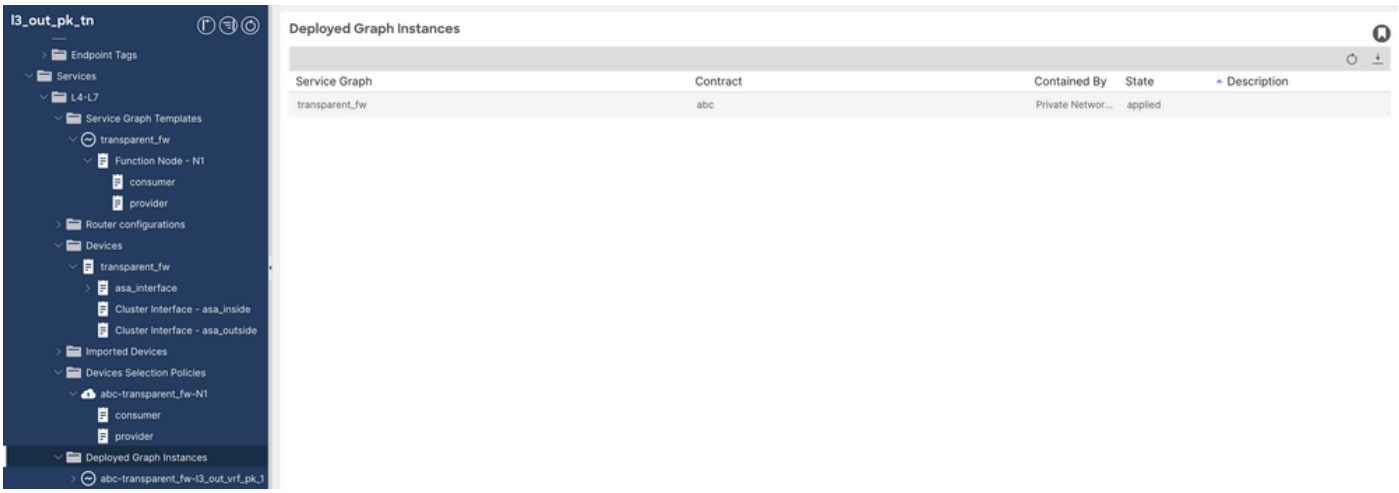
Tenant > Contract > Contract Subject > L4-L7 Service Graph > transparent_fwの順に移動します。

コン



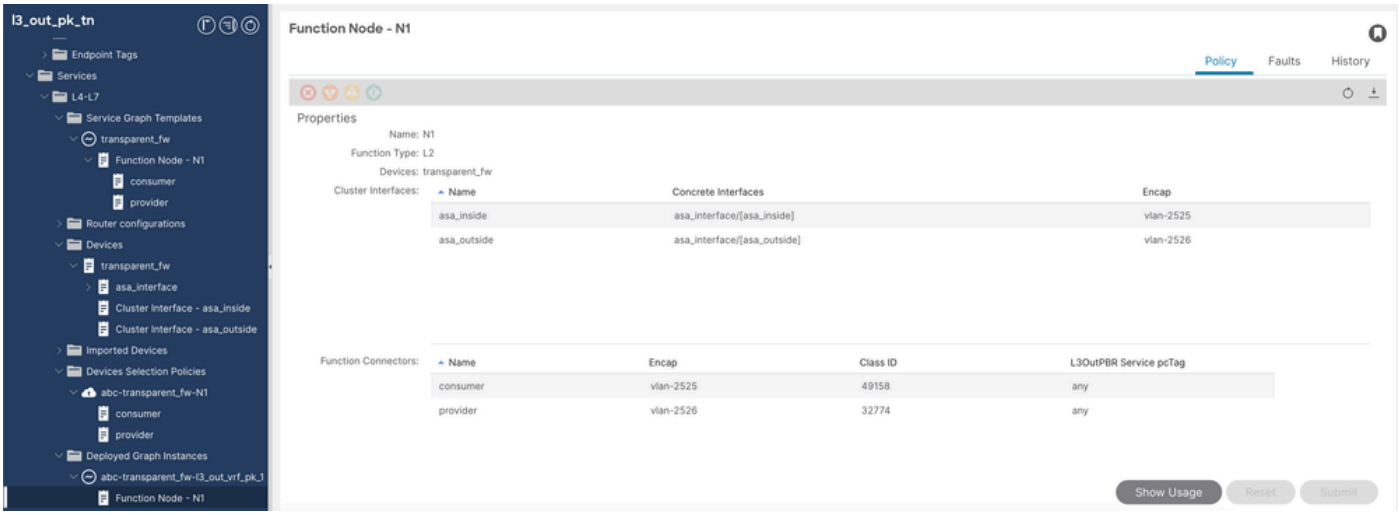
契約の構成

ステップ 9：正常に配備された場合は、「配備されたインスタンス」グラフで検証します（状態を検索）。



サービスグラフの検証

++クラスタインターフェイス、カプセル化VLAN、および機能コネクタクラスIDを検証します。



サービスグラフ検証2

ASAでのL2 PBRトラフィックの検証

Srcエンドポイントからdstエンドポイントへのセキュアシェル(SSH)（ASAのConnテーブルエントリで確認できます）

ASAの検証

リーフでのL2 PBRの確認

1. リーフノード102のVLANプログラミング

<#root>

```
PBR vlan 2525 and 2526 will get programmed on leaf node 102 and mac addresses will be statically tied t
```

```
bgl-aci07-apic100#
```

fabric 102 show endpoint

```
----------------------------------------------------------------------
Node 102 (bgl-aci07-leaf2)
----------------------------------------------------------------------
Legend:
S - static           s - arp              L - local            O - peer-attached
V - vpc-attached     a - local-aged       p - peer-aged        M - span
B - bounce           H - vtep             R - peer-attached-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
+-----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                          Encap           MAC Address       MAC Info/       Interface
      Domain                         VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
28/l3_out_pk_tn:l3_out_vrf_pk_1          vlan-2525    024a.e954.b591 LS                    eth1/14
1/l3_out_pk_tn:l3_out_vrf_pk_1           vlan-2526    02c0.282b.d1cf LS                    eth1/14
```

2. コンシューマ(101)ノードとプロバイダー(104)ノードのポリシーとゾーニングルールをリダイレクトします。

<#root>

```
++ Redirect policy on consumer node
```

```
bgl-aci07-apic100#
```

fabric 101 show service redir info

```
----------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
```

```
------------------------------------------------------------
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  T
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
8     destgrp-8       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2

List of destinations
Name                                                          bdVnid          vMac                vrf
====                                                          ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
HG-Name                                  HG-OperSt  HG-Dest
=======                                  =========  =======
l3_out_pk_tn::HG1                        enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                        enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx

List of Backup Destinations
Name                                                          primaryDestName
====                                                          ==============
List of AclRules
AclRuleVnid     DestGroup       OperSt   OperStQual
===========     =========       ======   ==========

++ Zoning rule on consumer Node

bgl-aci07-apic1OO#

fabric 101 show zoning-rule  | grep redir


|   4228  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4231  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
|   4230  | 32771  |   15   | default  |    uni-dir     | enabled | 2228224  |
|   4229  | 16386  | 32771  | default  |    uni-dir     | enabled | 2228224  |
```

<#root>

```
++ Redirect Policy on Provider Node
bgl-aci07-apic1OO#

fabric 104 show service redir info


------------------------------------------------------------
Node 104 (bgl-aci07-leaf4)
------------------------------------------------------------
================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  T
================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
```

```
3     destgrp-3       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
4     destgrp-4       dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  l3_out_pk_tn::HG2

List of destinations
Name                                                                bdVnid          vMac                vrf
====                                                                ======          ====                ===
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328  02:4A:E9:54:B5:91    l3_
dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vxlan-2228224]  vxlan-16056296  02:C0:28:2B:D1:CF    l3_

List of Health Groups
HG-Name                                     HG-OperSt  HG-Dest
=======                                     =========  =======
l3_out_pk_tn::HG1                           enabled    dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[v
l3_out_pk_tn::HG2                           enabled    dest-[143a:41d1:9c75:4973:8501:bcf:d12b:28c0]-[vx
List of Backup Destinations
Name                                                                primaryDestName
====                                                                ===============

++ Zoning rule on provider node
bgl-aci07-apic100#
```

fabric 104 show zoning-rule | grep redir

```
|   4220  | 32771  | 49157  | default  |     bi-dir     | enabled | 2228224  |
|   4221  | 49157  | 32771  | default  | uni-dir-ignore | enabled | 2228224  |
```

L2Pingが失敗した場合に見られる障害

PBRデバイスでL2pingが失敗した場合は、PBRが展開状態のままであり、障害F4203、F2833、およびF2911が発生し、トラック/ヘルスグループがダウンしていることが示されます。

L2 Pingのキャプチャ

L2Pingをキャプチャするには、tahoeインターフェイスでtcpdumpを使用して、L2Pingが正しく送受信されているかどうかを確認します。送信されたCPUのみが表示され、受信されていない場合は、前述の障害が予期されるため、ドロップされた理由についてASAでさらにトラブルシューティングを行う必要があります（「ASAの設定」の項を参照）。

<#root>

```
Capturing L2Pings using tcpdump on PBR Node 102

bgl-aci07-leaf2#
```

tcpdump -i tahoe0 -w /data/techsupport/l2_pbr1.pcap

```
tcpdump: listening on tahoe0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C4858 packets captured
4875 packets received by filter
0 packets dropped by kernel
```

In order to deocde the tcpdump

cat /data/techsupport/l2_pbr1.pcap | knet_parser.py --decode tahoe --pcap | less

** Search for mac 00ab.8752.3100

++ CPU transmit packets
Frame 505
Time: 2024-10-29T05:55:28.707136+00:00
Header: ieth

CPU Transmit

sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x207, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/

ethertype:0x721

Frame 506
Time: 2024-10-29T05:55:28.707297+00:00
Header: ieth CPU Transmit
sup_tx:1, ttl_bypass:0, opcode:0x0, bd:0x208, outer_bd:0x0, dl:0, span:0, traceroute:0, tclass:5
src_idx:0x0, src_chip:0x0, src_port:0x0, src_is_tunnel:0, src_is_peer:0
dst_idx:0x0, dst_chip:0x0, dst_port:0x0, dst_is_tunnel:0
Len: 72
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/

ethertype:0x721

++CPU recived packets

Frame 509
Time: 2024-10-10T20:16:37.580855+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH

(0x4d)
Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x209, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 024a.e954.b591

, len/ethertype:0x8100(802.1q)
802.1q:

vlan:2526

, cos:0, len/

ethertype:0x721

Frame 510
Time: 2024-10-10T20:16:37.580891+00:00
Header: ieth_extn

CPU Receive

sup_qnum:0x33, sup_code:0x4d, istack:

ISTACK_SUP_CODE_PBR_TRACK_REFRESH(0x4d)

Header: ieth
sup_tx:0, ttl_bypass:0, opcode:0x0, bd:0x20a, outer_bd:0x2, dl:0, span:0, traceroute:0, tclass:0
src_idx:0x32, src_chip:0x0, src_port:0x6, src_is_tunnel:0, src_is_peer:0
dst_idx:0x1, dst_chip:0x0, dst_port:0x3d, dst_is_tunnel:0
Len: 76
Eth:

00ab.8752.3100 > 02c0.282b.d1cf

, len/ethertype:0x8100(802.1q)
802.1q:

vlan:2525

, cos:0, len/

ethertype:0x721

送信元から宛先エンドポイントへのトラフィックフロー

<#root>

++ Endpoint X.1.1.10 want to send traffic to X.1.2.15
++ If destination is not learned on consumer/source leaf, PBR will be performed on destination leaf
++ For this case we are assuming endpoint X.1.2.15 is learned on Leaf 101 so PBR/Redirection will be pe

bgl-aci07-apic100#

fabric 101 show endpoint

```
--------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
--------------------------------------------------------------------
Legend:
S - static           s - arp              L - local            O - peer-attached
V - vpc-attached     a - local-aged       p - peer-aged        M - span
B - bounce           H - vtep             R - peer-attached-rl D - bounce-to-proxy
E - shared-service   m - svc-mgr
```

```
+-----------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                            Encap           MAC Address       MAC Info/       Interface
      Domain                           VLAN            IP Address        IP Info
+-----------------------------------+---------------+-----------------+--------------+-------------+
l3_out_pk_tn:l3_out_vrf_pk_1                               X.1.2.15                      tunnel6 ===> |
17                                     vlan-3516    10b3.d514.3516 L                     eth1/5 ===>
l3_out_pk_tn:l3_out_vrf_pk_1           vlan-3516        X.1.1.10 L                      eth1/5

++ EPM entry to get the PC TAG
bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.1.10

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 10b3.d514.3516 ::: Num IPs : 1
IP# 0 : X.1.1.10 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 17 ::: Vlan vnid : 11792 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 16744307 ::: VRF vnid : 2228224
Phy If : 0x1a004000 ::: Tunnel If : 0
Interface : Ethernet1/5
Flags : 0x80005c04 ::: sclass :
```

32771

```
 ::: Ref count : 5 ==> sclass
EP Create Timestamp : 10/11/2024 09:15:44.430334
EP Update Timestamp : 10/29/2024 10:45:35.458416
EP Flags : local|IP|MAC|host-tracked|sclass|timer|

bgl-aci07-apic100#
```

fabric 101 show system internal epm endpoint ip X.1.2.15

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
MAC : 0000.0000.0000 ::: Num IPs : 1
IP# 0 : X.1.2.15 ::: IP# 0 flags :  ::: l3-sw-hit: No
Vlan id : 0 ::: Vlan vnid : 0 ::: VRF name : l3_out_pk_tn:l3_out_vrf_pk_1
BD vnid : 0 ::: VRF vnid : 2228224
Phy If : 0 ::: Tunnel If : 0x18010006
Interface : Tunnel6
Flags : 0x80004400 ::: sclass :
```

49157

```
 ::: Ref count : 3 ==> sclass
EP Create Timestamp : 10/29/2024 10:38:34.949150
EP Update Timestamp : 10/29/2024 10:45:55.571786
EP Flags : IP|sclass|timer|

++ Traffic will be redirected based on redir(destgrp-7)
bgl-aci07-apic100#
```

fabric 101 show zoning-rule src-epg 32771 dst-epg 49157

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
+---------+--------+--------+----------+--------+---------+---------+------+-----------------+--------
```

```
| Rule ID | SrcEPG | DstEPG | FilterID |  Dir   |  operSt |  Scope  | Name |      Action      |    Prio
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------
|   4228  | 32771  | 49157  | default  | bi-dir | enabled | 2228224 |      | redir(destgrp-7) | src_dst_
+---------+--------+--------+----------+--------+---------+---------+------+------------------+--------

++ Based on redirect policy traffic will be redirected to mac
```

02:4A:E9:54:B5:91

```
bgl-aci07-apic100#
```

fabric 101 show service redir info

```
------------------------------------------------------------------
Node 101 (bgl-aci07-leaf1)
------------------------------------------------------------------
================================================================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |  T
================================================================================================================================
List of Dest Groups
GrpID Name            destination                                                    HG-name
===== ====            ===========                                                    ==============
7     destgrp-7       dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] l3_out_pk_tn::HG1
List of destinations
Name                                                          bdVnid          vMac                 vrf
====                                                          ======          ====                 ====
dest-[3d49:a399:3d4b:4ea1:8829:5991:b554:e94a]-[vxlan-2228224] vxlan-16744328
```

02:4A:E9:54:B5:91

```
    l3_out_pk_tn:l3_out_vrf_pk_1 enabled    no-oper-dest    l3_out_pk_tn::HG
1

++ PBR mac addresses are never learnt remotely as IP/MAC learning is disabled for PBR BD
++ PBR mac addresses are statically binded to interfaces where L4/L7 device is connected and reported t
++ Traffic will be forwarded to SPINE PROXY
++ Spine has an COOP entry for 02:4A:E9:54:B5:91

bgl-aci07-apic100#
```

fabric 201 show coop internal info repo ep key 16744328 02:4A:E9:54:B5:91

```
------------------------------------------------------------------
Node 201 (bgl-aci07-spine1)
------------------------------------------------------------------
Repo Hdr Checksum : 49503
Repo Hdr record timestamp : 10 29 2024 10:15:07 658496921
Repo Hdr last pub timestamp : 10 29 2024 10:15:07 661679296
Repo Hdr last dampen timestamp : 01 01 1970 00:00:00 0
Repo Hdr dampen penalty : 0
Repo Hdr flags : IN_OBJ ACTIVE
EP bd vnid : 16744328
EP mac :
```

02:4A:E9:54:B5:91

```
 <<<<========== ASA MAC
flags : 0x480
repo flags : 0x102
Vrf vnid : 2228224
PcTag : 0x100c006
```

```
EVPN Seq no : 0
Remote publish timestamp: 01 01 1970 00:00:00 0
Snapshot timestamp: 10 29 2024 10:15:07 658496921
Tunnel nh : 10.0.144.66
MAC Tunnel  : 10.0.144.66
IPv4 Tunnel : 10.0.144.66
IPv6 Tunnel : 10.0.144.66
ETEP Tunnel : 0.0.0.0
num of active ipv4 addresses : 0
num of anycast ipv4 addresses : 0
num of ipv4 addresses : 0
num of active ipv6 addresses : 0
num of anycast ipv6 addresses : 0
num of ipv6 addresses : 0
Primary Path:
Current published TEP :
```

10.0.144.66

```
Backup Path:
BackupTunnel nh : 0.0.0.0
Current Backup (publisher_id): 0.0.0.0
Anycast_flags : 0
Current citizen (publisher_id): 10.0.144.66
Previous citizen : 10.0.144.66
Prev to Previous citizen : 10.0.144.66
Synthetic Flags : 0x5
Synthetic Vrf : 411
Synthetic IP : X.X.83.223
Tunnel EP entry: 0x7f20900167a8
Backup Tunnel EP entry: (nil)
TX Status: COOP_TX_DONE\
Damp penalty: 0
Damp status: NORMAL
Exp status: 0
Exp timestamp: 01 01 1970 00:00:00 0
Hash: 3209430840 owner: 10.0.144.65

++ Spine will forward this to PBR Leaf Node 102 based on COOP entry
++ PBR Leaf Node will forward this to ASA FW on interface E1/14
++ ASA FW will forward the traffic based on mac address table and send it back to PBR Leaf Node 102
++ PBR Leaf Node will look for Dst IP in the traffic and route it to Leaf 104 if remote endpoint entry
++ Leaf 104 will get this traffic forwarded to actual EP X.1.2.15 (Leaf4 does not learn the client IP a
```

ASA の設定

ステップ 1：インターフェイス設定。

<#root>

```
ASA(config)#
```

show running-config interface

```
!
interface GigabitEthernet0/0
```

```
 bridge-group 1
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 bridge-group 1
 nameif outside
 security-level 0
!
interface BVI1
ip address 192.168.100.1 255.255.255.0 ==> In case BVI IP is not defined ASA will not switch the packet
!
```

ステップ 2：MACラーニングを無効にする必要があります。

<#root>

```
ASA(config)#
```

show run mac-learn

```
mac-learn inside disable
mac-learn outside disable
```

PBR:

ステップ 3：PBR MacのスタティックMACアドレステーブル

<#root>

```
The mac statically binded to inside interface is the PBR mac generated by provider and vice versa
ASA(config)#
```

show run mac-address-table

```
mac-address-table static outside 024a.e954.b591
mac-address-table static inside 02c0.282b.d1cf
```

ステップ 4：L2pingを渡すためにアクセスコントロールリスト(ACL)を設定します。

<#root>

```
ASA(config)#
```

show access-list

```
access-list L2_PBR ethertype permit 721

ASA(config)# show run access-group
```

```
access-group L2_PBR in interface inside
access-group L2_PBR in interface outside
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。