

DPU セキュリティ モードの Cisco スマート スイッチ トラブルシューティング ガイド、リリース 10.6（x）

最終更新：2026 年 10 月 28 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



目 次

Trademarks ?

第 1 章 **DPU セキュリティ モードのトラブルシュート スマート スイッチ** 1

DPU セキュリティ モードのトラブルシュート スマート スイッチ 1

第 2 章 **DPU の起動** 3

DPU の起動 3

第 3 章 **Hypershield コントローラから Hypershield Agent への接続の問題** 7

Hypershield コントローラから Hypershield Agent への接続の問題 7

第 4 章 **ロード バランサ モード検証** 11

ロード バランサ モード検証 11

対称ハッシュ 11

ロードバランスモードのピン接続 13

第 5 章 **ファイアウォールの立ち上げ前のネットワーク構成** 15

ファイアウォールの立ち上げ前のネットワーク構成 15

第 6 章 **ファイアウォールの立ち上げの NPU パケット フロー** 19

ファイアウォールの立ち上げの NPU パケット フロー 19

第 7 章 **ファイアウォールの起動** 23

ファイアウォールの起動 23

第 8 章 パケット転送 25
パケット転送 25

第 9 章 Hypershield エージェントから NX-OS への連携動作 29
Hypershield エージェントから NX-OS への連携動作 29

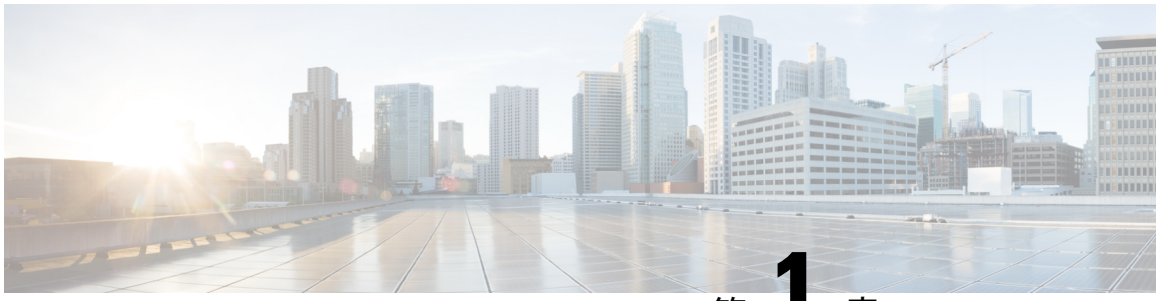
第 10 章 NPU から DPU へのリダイレクトの問題 31
NPU から DPU へのリダイレクトの問題 31

第 11 章 DPU パケット フローを投稿 37
DPU パケット フローを投稿 37

第 12 章 パケット トレーサのサポート 39
パケット トレーサのサポート 39

第 13 章 VRF 間トラフィック インスペクション 43
VRF 間トラフィック インスペクション 43

第 14 章 高可用性 45
高可用性 45
両方のピアが非サービス モードです 48
一方のピアがインサービス モードであり、もう一方のピアは、インサービス モードでは、ありません 50
両方のピアがインサービス モードです 54
メンバーシップの障害 59



第 1 章

DPUセキュリティ モードのトラブルシュート スマート スイッチ

• DPU セキュリティ モードのトラブルシュート スマート スイッチ （1 ページ）

DPU セキュリティ モードのトラブルシュート スマート スイッチ

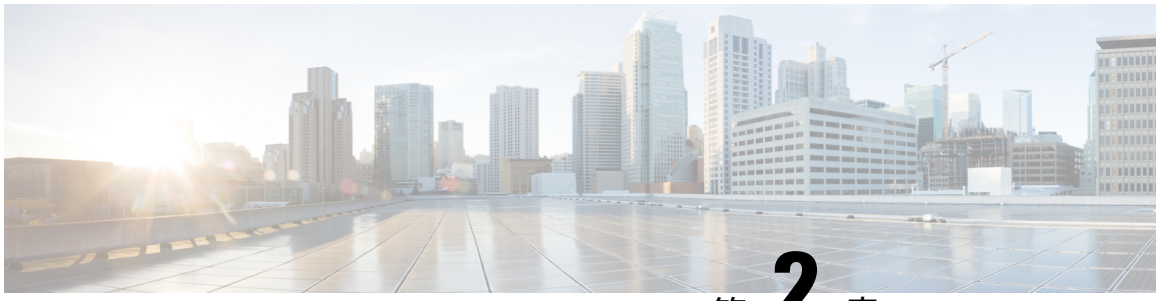
このガイドの各セクションでは、NPU ハードウェア プログラミングから DPU ベースの検査と高可用性（HA）状態の同期に至るまでのエンドツーエンドのパケット フローについて説明しています。また、Hypershield と統合した場合のスマート スイッチ環境内の問題を特定し、切り分けて解決するための体系的な手順も説明しています。

Hypershield では、データ処理ユニット（DPU）と NPU からのリダイレクションを活用する高度なトラフィック リダイレクションおよび検査機能が導入されているため、トラブルシューティングには多層型のアプローチが必要です。

このガイドの内容は、network-admin と netsecops-admin の両方のロールを持つユーザーを対象としています。これらのユーザー ロールの詳細については、「DPU セキュリティ モードの Cisco スイッチ スマート構成ガイド」の「スイッチ スマートのユーザアカウントおよびRBAC」の章を参照してください。ユーザーは NX-OS、 VRF-Lite アーキテクチャ、およびサービス アクセラレーション機能の実用的な知識を持っていることを前提としています。

（注） ここで提供されるコマンドと出力は、現在の NX-OSリリースに基づいています。詳細なトラブルシューティングを実行する前に、環境がサポートされているソフトウェア バージョンを実行していることを必ず確認してください。

DPU セキュリティ モードのトラブルシュート スマート スイッチ



第 2 章

DPU の起動

• DPU の起動 （3 ページ）

DPU の起動

スマート スイッチがセキュリティ機能を提供するには、DPU の正常な起動が必要です。これらのコマンドは、サービス アクセラレーション機能を有効にした後、DPU のステータスを確認します。

手順

ステップ 1 サービス アクセラレーション機能が有効化されていることを確認します。

例：

```
switch# show run service-acceleration | grep feature feature service-acceleration
```

ステップ 2 （オプション）**show feature** コマンドを使用して、機能ステータスを確認します。

例：

```
show feature | grep service-acceleration service-acceleration 1 enabled
```

ステップ 3 DPU の電源がオンでオンラインであることを確認します。

例：

```
switch# show module | begin DPU

Mod DPU   Module-Type      Model          Status
--- ---  ------------- ----------------- --------
1    1       DPU          N9324C-SE1U-DPU    ok
1    2       DPU          N9324C-SE1U-DPU    ok
1    3       DPU          N9324C-SE1U-DPU    ok
1    4       DPU          N9324C-SE1U-DPU    ok
```

リストされているすべての DPU の [ステータス（Status）] が ok であることを確認します。

ステップ 4 DPU ソフトウェアとハードウェアのバージョンの確認します。

例：

```
switch# show module  | begin dpu
Mod DPU     Sw             Hw      Serial-Num   Online Diag Status
--- ---  -------------- ---------- ------------ ------------------
1   1     1.150.2      JI         FDO283707WH   Pass
1   2     1.150.2      JI         FDO283707WH   Pass
1   3     1.150.2      JI         FDO283707WG   Pass
1   4     1.150.2      JI         FDO283707WG   Pass
```

各 DPU に記載されているソフトウェア（Sw）とハードウェア（Hw）のバージョンを確認します。

ステップ 5 現用系 DPU ファームウェア パッケージを確認します。

例：

```
switch# show install active | grep dpu_fw dpu_fw-1.150.2-10.6.3q.x86_64
```

ステップ 6 DME の DPU 初期化状態を確認します。

例：

```
switch# show system internal dme running-config all dn sys/sas/dpu/ext | grep -i initState "initState":
 "inventory-done",
```

`initState` が `inventory-done` であることを確認します。

ステップ 7 DPU からサービス イーサネット インターフェイスへのマッピング、および DPU IP アドレスを確認します。

例：

```
switch# show dpu interface
*************** DPU interface info **************

Number of DPUs: 4
Total number of DPU <-> NPU links: 4

DPU-1:
Number of links to NPU: 1 NPU port number: 96
Service Ethernet Interface(NPU): SEth1/1 DPU-1 IP address: 169.254.28.1

DPU-2:
Number of links to NPU: 1 NPU port number: 100
Service Ethernet Interface(NPU): SEth1/2 DPU-2 IP address: 169.254.24.1

DPU-3:
Number of links to NPU: 1 NPU port number: 104
Service Ethernet Interface(NPU): SEth1/3 DPU-3 IP address: 169.254.36.1

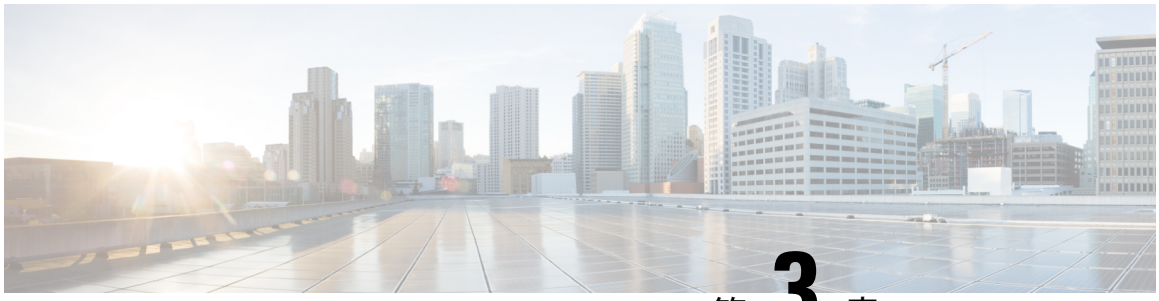
DPU-4:
Number of links to NPU: 1 NPU port number: 108
Service Ethernet Interface(NPU): SEth1/4 DPU-4 IP address: 169.254.32.1
```

DPU の数と DPU <-> NPU リンクの合計数を確認します。リストされている各 DPU（DPU-1 など）については、NPU へのリンク数が 1、サービス イーサネット インターフェイス（NPU）が正しいインターフェイスにマッピングされること（たとえば、DPU-1 の場合は SEth1/1）、一意の DPU-N IP アドレス（169.254.xx の範囲）が割り当てられます。

次のタスク

これらのチェックを実行した後、DPUの電源が正常にオンになり、動作状態にあることを確認できます。

DPU の起動



第 3 章

Hypershield コントローラから Hypershield Agent への接続の問題

• Hypershield コントローラから Hypershield Agent への接続の問題 （7 ページ）

Hypershield コントローラから Hypershield Agent への接続の問題

スイッチ上の Hypershield Agent（HSA）が Hypershield Controller（HSC）との接続を確立できない問題を診断し、解決します。HSC から HSA への接続をトラブルシューティングするための主要なツールは、一連のチェックを実行する **service system hypershield test controller connection** コマンドです。

手順

ステップ 1 コントローラ接続テスト電力事業を実行します。

例：

```
switch# service system hypershield test controller connection
==============================
 Running config checks
==============================
Using source-interface loopback100 for controller connection
Controller connection token is configured
Controller connection status: [success]
Controller reason: [connected ok with Hypershield controller]
Controller endpoint: 172.31.147.51:6443
================================================
Starting network connectivity checks on the switch
================================================
Not using proxy for controller connection
Using curl to check connection to 172.31.147.51 port 6443
Curl successfully connected to 172.31.147.51:6443.
Collect 'show tech service-acceleration' to debug any agent connectivity failure
```

このコマンドは、いくつかのチェックを実行して、接続失敗のステータスと考えられる理由を表示します。

Hypershield コントローラから Hypershield Agent への接続の問題

正常に接続されたら、次のことを確認します。

- エージェント ステータスは、firewall-ready、redirect-installed（完全なオンボーディング後）や同様の正常な状態など、準備ができていることを示します。
- コントローラ接続のステータスは「成功」です。
- ネットワーク接続チェック（DNS 解決、ping、curl）が成功しました。

例：

```
switch# service system Hypershield test controller connection
==============================
Running config checks
==============================
HypershieldAgent not running Configure 'service system hypershield'
```

エージェントが実行されていない場合、そのことが出力に明示的に表示されます。

これを解決するには、**service system hypershield** コマンドが構成されていることを確認します。

また、**source-interface loopback** <*idx*> が **service system hypershield** の下で構成されており、構成されたループバック インターフェイスにデフォルトの VRF で有効な /32 IP アドレスがあることを確認します。

show system internal service-acceleration agent status コマンドを使用してエージェント状態を確認できます。[開始済み（started）] と表示されます。

ステップ 2 ファイアウォール サブシステムが [サービス中（in-service）] でない場合は、出力を解釈します。

例：

```
switch(config-svc-sys)# service system hypershield test controller connection
==============================
Running config checks
==============================
Enable firewall service by configuring 'in-service'
```

ファイアウォール サービスが有効になっていない場合、[サービス中（in-service）] を構成するように出力に求められます。

これを解決するには、サービス システム ハイパーシールド サービス ファイアウォール コンフィギュレーション モードで **in-service** を構成します。

ステップ 3 トークンが構成されていないか、無効なトークンが構成されている場合、出力を解釈します。

例：

```
switch(config-svc-sys-fw)# service system hypershield test controller connection

==============================
 Running config checks
==============================
Controller connection token Invalid! Configure using 'service system hypershield register <token>'
```

OTP が構成されていない場合、 出力にはトークンが欠落していることが示されます。

これを解決するには、Hypershield 管理ポータル（HS MP）から OTP を取得し、**service system hypershield register** <*token*> EXEC コマンドを使用してスイッチ上で構成します。

Hypershield コントローラから Hypershield Agent への接続の問題

トークンが構成されているかどうか（トークン自体ではない）は、 **show system internal dme running-config all dn sys/sas/volatiledata/agent-hypershield | grep connToken** を使用して確認できます。

ステップ 4 これは、HSA がハンドシェイクを完了し、すべての DPU と同期した場合の出力です。

例：

```
switch# service system hypershield test controller connection

==============================
 Running config checks
==============================
Hypershield Agent <-> DPU handshake pending. Collect 'show tech-support service-acceleration'
```

HSA が 1 つ以上の DPU と通信または同期できない場合、`[正常性ステータス（Health Status）]` は `[機能不全（failed）]` と表示され、出力は保留中のハンドシェイクを示すか、DPU 診断を提供します。

DPU 診断内：

- `InSync false` は、ファイアウォール ポリシーが DPU と HSA の間で同期していないことを示します。
- `Healthy false` は、DPU と HSA 間の定期的なハンドシェイクが失敗していることを示します。

このシナリオでさらにデバッグするには、 **show tech-support service-acceleration** コマンドの出力を収集することを推奨します。

ステップ 5 コントローラへのルートがない場合、 出力には詳細なネットワーク接続チェックとルーティング検証が表示されます。

例：

```
switch(config-if)# service system hypershield test controller connection

==============================
 Running config checks
==============================
Using source-interface loopback100 for controller connection
Controller connection token is configured
Controller connection status: [success]
Controller reason: [connected ok with Hypershield controller]
Controller endpoint: 172.31.147.51:6443

================================================
 Starting network connectivity checks on the switch
================================================
Not using proxy for controller connection
Using curl to check connection to 172.31.147.51 port 6443
Failed to connect to host.

Running ping tests to check connectivity.
Pinging 172.31.147.51 to check network connectivity.
PING 172.31.147.51 (172.31.147.51) 56(84) bytes of data.
From 127.253.254.1 icmp_seq=1 Destination Net Unreachable

--- 172.31.147.51 ping statistics ---
4 packets transmitted, 0 received, +1 errors, 100% packet loss, time 3037ms

Could not ping 172.31.147.51.

Checking for a valid route for 172.31.147.51
RTNETLINK answers: Network is unreachable
```

Hypershield コントローラから Hypershield Agent への接続の問題

```
Could not reach 172.31.147.51 from host.
Check 'show ip route 172.31.147.51' for a valid route

switch(config-if)# show ip route 172.31.147.51
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
Route not found
```

ステップ 6 （オプション）ping を使用して HSA コンテナからの到達可能性をテストします。

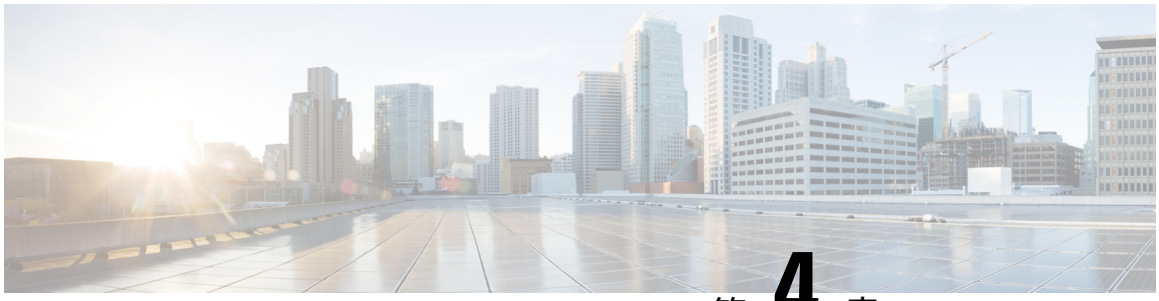
例：

```
switch# service system hypershield test ping 171.70.33.31 PING 171.70.33.31 (171.70.33.31) 56(84)
bytes of data.
64 bytes from 171.70.33.31: icmp_seq=1 ttl=53 time=2.93 ms
...
--- 171.70.33.31 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev =
1.540/2.357/2.931/0.525 ms
```

このコマンドは、pingがコンテナ内から実行されるため、HSAの観点から基本的なIP接続を確認します。ping を送信するコントローラの IP アドレスまたはホスト名を指定します。

---

service system hypershield test controller connection コマンドの出力を分析し、HSA コンテナから追加の ping テストを実行することで、HSA から HSC への接続を妨げている一般的な構成またはネットワークの問題を特定できます。



第 4 章

ロード バランサ モード検証

• ロード バランサ モード検証 （11 ページ）

ロード バランサ モード検証

構成および動作しているロードバランスの構成を確認します。ロード バランス モードのサービス ポート チャネル インターフェイスが想定どおりに作成されていることを確認します。

ここでは、次のトラブルシューティングについて説明します：

対称ハッシュ

手順

ステップ 1 サービス アクセラレーションのロードバランス構成を特定してください。この例では、ロードバランスの設定はデフォルト値の対称ハッシュです。

例：

```
switch# show run service-acceleration
!Command: show running-config service-acceleration
!Running configuration last done at: Fri May  8 07:35:41 2026
!Time: Sat May  9 23:02:10 2026
version 10.6(3q) Bios:version 01.17
feature service-acceleration
service system hypershield
  source-interface loopback2
  service firewall
    vrf tenant1 module-affinity dynamic
    vrf tenant2 module-affinity dynamic
    vlan id 2003,2005 bridged-traffic module-affinity dynamic
```

ステップ 2 サービス ファイアウォールが作成され、アウトオブサービス状態であることを確認します。

例：

```
switch# show run service-acceleration | grep firewall service firewall
```

これにより、ファイアウォール サービスが構成されていることを確認します。

ステップ 3 サービス ファイアウォールが作成されいることを確認します。これがアウトオブサービスとして正しく表示され、ロードバランス モードが対称ハッシュのデフォルト モードに設定されていることを確認します。

例：

```
show run service-acceleration  | grep firewall
  service firewall
switch# show service-acceleration status
  Service System: hypershield
    Source Interface: loopback2 (10.29.251.4)
    DPU Load-balance Mode: symmetric-hash  --> default load-balance mode
    Agent Status: firewall-disable
    Agent Health Status: ok
    Controller Connection Status: init
    Agent HA Status: not-initialized
    Services:
      Firewall: out-of-service             --> by default out-of-service
```

ステップ 4 サービス ポートチャネルの作成と対称ハッシュのメンバーシップを確認します。

例：

```
switch(config)# show port-channel summary interface service-port-channel 512
<<snip>>
--------------------------------------------------------------------------------
Group Port-Channel Type     Protocol  Member Ports
--------------------------------------------------------------------------------
512   SPo512(RU)  Eth      NONE      SEth1/1(P)   SEth1/2(P)   SEth1/3(P)
                                     SEth1/4(P)
```

（注） 上記の例では、SPO 512 のみが、各 DPU に関連する 4 つのサービス イーサネット リンクをすべて持っています。

ステップ 5 サービス用ポートチャネルに関する問題が発生した場合は、ポートチャネルの consistency-checker を使用してください。

例：

```
switch# show consistency-checker membership port-channels interface service-port-channel 512
Checks: Pif, vifstate, localmultipath, ucpcconfig and ucpcmember tables.
Performing Consistency-checker for Service-Port-Channel512
Checking hardware for Module 1
Module 1 Consistency Check: PASSED
['Service-Ethernet1/1', 'Service-Ethernet1/2', 'Service-Ethernet1/3', 'Service-Ethernet1/4']
```

ステップ 6 Hypershield エージェントがロードバランス モードを正しく識別していることを確認してください。

例：

```
switch# app-hosting connect appid HypershieldAgent session /usr/src/app/agwctl device show | grep
'LB Mode'
  LB Mode:               symmetric-hash
```

ロードバランスモードのピン接続

手順

ステップ 1 サービス アクセラレーションのロードバランス構成を特定してください。この例では、ロードバランス構成は ピン接続として構成されています。

例：

```
switch(config)# show run service-acceleration
!Command: show running-config service-acceleration
!Running configuration last done at: Sun May 10 00:14:30 2026
!Time: Sun May 10 00:18:06 2026
version 10.6(3q) Bios:version 01.17
feature service-acceleration
service dpu load-balance pinning         --> Pinning load-balance mode
service system hypershield
  source-interface loopback2
  service firewall
    vrf tenant1 module-affinity 1
    vrf tenant2 module-affinity dynamic
    vlan id 2003 bridged-traffic module-affinity 3
    vlan id 2005 bridged-traffic module-affinity dynamic
```

ステップ 2 サービス ファイアウォールが作成されいることを確認します。これがアウトオブサービスとして正しく表示されていること、およびロードバランス モードがピン接続モードを表示していることを確認します。

例：

```
show run service-acceleration  | grep firewall
  service firewall
switch# show service-acceleration status
  Service System: hypershield
Source Interface: loopback2 (10.29.251.4)
    DPU Load-balance Mode: pinning         -->  Pinning load-balance mode
    Agent Status: firewall-disable
    Agent Health Status: ok
    Controller Connection Status: init
    Agent HA Status: not-initialized
    Services:
      Firewall: out-of-service             --> by default out-of-service
```

ステップ 3 サービスの DPU ポート チャネルごとの作成とピン接続モードのメンバーシップを確認します。ここでキャプチャされた N9324C-SE1U の出力は、各 DPU に 1 つずつ、合計 4 つのサービス ポートチャネルが作成されたことを示しています。これらのポートチャネルのそれぞれには、メンバー リンクとして単一のサービスイーサネット インターフェイスがあります。

例：

```
switch(config)# show port-channel summary interface service-port-channel 1
<<snip>>
--------------------------------------------------------------------------------
Group Port-Channel Type     Protocol  Member Ports
--------------------------------------------------------------------------------
SPo1(RU)    Eth      NONE      SEth1/1(P)
--> Service-ethernet interfaces pertaining to each DPU in per-DPU SPOs
switch(config)# show port-channel summary interface service-port-channel 2
<<snip>>
```

```
--------------------------------------------------------------------------------
Group Port-Channe Type     Protocol  Member Ports
--------------------------------------------------------------------------------
2     SPo2(RU)    Eth      NONE      SEth1/2(P)
switch(config)# show port-channel summary interface service-port-channel 3
<<snip>>
--------------------------------------------------------------------------------
Group Port-Channel Type     Protocol  Member Ports
--------------------------------------------------------------------------------
3     SPo3(RU)    Eth      NONE      SEth1/3(P)
switch(config)# show port-channel summary interface service-port-channel 4
<<snip>>
--------------------------------------------------------------------------------
Group Port-Channel Type     Protocol  Member Ports
--------------------------------------------------------------------------------
4     SPo4(RU)    Eth      NONE      SEth1/4(P)
```

N9348Y2C6D-SE1U では、DPU ごとに 1 つずつの 2 つのサービスポートチャネルが作成されます。各サービス ポートチャネルには、メンバーリンクとして 2 つのサービスイーサネット インターフェイスがあります。

ステップ 4 サービス用ポートチャネルに関する問題が発生した場合は、ポートチャネルの consistency-checker を使用してください。

例：

```
switch# show consistency-checker membership port-channels interface service-port-channel 1
Checks: Pif, vifstate, localmultipath, ucpcconfig and ucpcmember tables.
Performing Consistency-checker for Service-Port-Channel1
Checking hardware for Module 1
Module 1 Consistency Check: PASSED
['Service-Ethernet1/1']
```

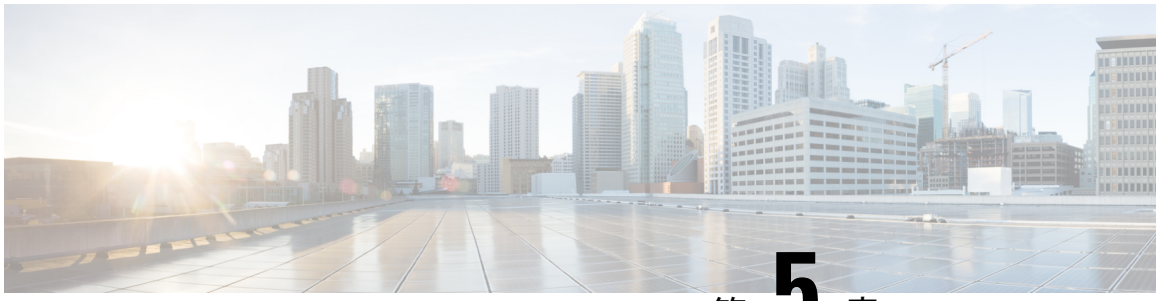
ステップ 5 Hypershield エージェントがロードバランス モードを正しく識別していることを確認してください。

例：

```
switch# app-hosting connect appid HypershieldAgent session /usr/src/app/agwctl device show | grep
'LB Mode'
  LB Mode:               pinning
```

次のタスク

これらのチェックを実行した後、システムが構成に従って正しいロードバランス モードを検出し、有効にしていることを確認できます。



第 5 章

ファイアウォールの立ち上げ前のネットワーク構成

• ファイアウォールの立ち上げ前のネットワーク構成 （15 ページ）

ファイアウォールの立ち上げ前のネットワーク構成

ファイアウォールサービスが構成されているものの、アクティブになっていない場合に、システムが想定どおりの状態であることを確認します。この状態では、サービスアクセラレーション用に構成された VRF は分離される必要があり、VLAN はパケットをドロップするように設定する必要があります。トラフィックは DPU にリダイレクトされず、ドロップされる必要があります。VRF が分離されている状態で、トラフィックが予期せず DPU へ、あるいはボックス外へ転送される場合、または、VLAN がドロップとして設定されている場合、このセクションのチェックを実行します。

手順

ステップ 1 サービス ファイアウォールが作成され、アウトオブサービス状態であることを確認します。

例：

```
switch# show run service-acceleration | grep firewall service firewall
```

これにより、ファイアウォール サービスが構成されていることを確認します。

ステップ 2 ファイアウォール サービスの動作ステータスを確認します。

例：

```
switch# show service-acceleration status
  Service System: hypershield
    Source Interface: loopback2 (10.29.251.7)
    DPU Load-balance Mode: symmetric-hash
    Agent Status: firewall-disable
    Agent Health Status: ok
    Controller Connection Status: init
    Agent HA Status: not-initialized
```

ファイアウォールの立ち上げ前のネットワーク構成

```
    Services:
      Firewall: out-of-service    --> by default out-of-service
```

ファイアウォールの 状態は out-of-serviceである必要があります。

ステップ 3 サービス アクセラレーション用に有効になっている VRF および VLAN を特定します。

例：

```
switch# show  running-config service-acceleration

!Command: show running-config service-acceleration
!Running configuration last done at: Thu May  7 06:04:18 2026
!Time: Thu May  7 06:04:33 2026

version 10.6(3q) Bios:version 01.17
feature service-acceleration

service system hypershield
  source-interface loopback2
  service firewall
    vrf tenant1 module-affinity dynamic
    vrf tenant2 module-affinity dynamic
    vlan id 2003,2005 bridged-traffic module-affinity dynamic
```

service firewall セクションで vrf <name> で始まる行をチェックして、サービス アクセラレーション用に構成された VRF を特定します。

service firewall セクションで vlan <id> で始まる行をチェックして、サービス アクセラレーション用に構成された VLAN を特定します。

ステップ 4 識別された VRF が 分離 状態にあり、識別された VLAN がドロップするように設定されていることを確認します。

例：

```
switch# show service-acceleration status details
  Service System: hypershield
    Source Interface: loopback2 (10.29.251.4)
    DPU Load-balance Mode: symmetric-hash
    Agent Status: firewall-disable
    Agent Health Status: ok
    Controller Connection Status: init
    Agent HA Status: not-initialized
    Services:
      Firewall: out-of-service

      VRF                  Operational State       Affinity(DPU)
      ============================================================
      tenant1               isolated                n/a      --> isolated state
      tenant2               isolated                n/a

      VLAN                 Operational State       Affinity(DPU)
      ============================================================
      2003                  VLAN set to drop        n/a
      2005                  VLAN set to drop        n/a
```

VRFのルーティング プロトコルによってアドバタイズされたルートが、プロトコル分離中にサポートされている動作と一致することを確認します。

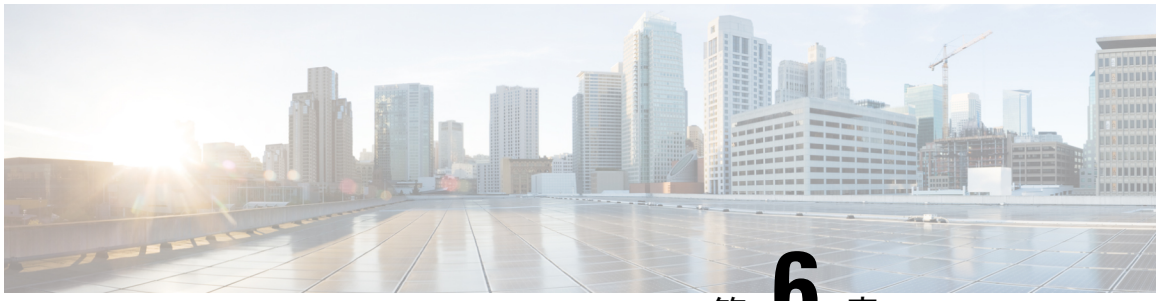
ファイアウォールの立ち上げ前のネットワーク構成

（注） VRF 分離動作は、現在 OSPF と BGP でサポートされています。

次のタスク

これらのチェックを実行した後、サービス アクセラレーション用に構成された VRF がシステムおよびルーティング プロトコルによって分離されていると正しく識別されることを確認できるはずです。これは、ファイアウォール サービスが起動（インサービス）になる前の予想される状態です。サービス アクセラレーション用に設定された VLAN の予想される状態を確認できます。

ファイアウォールの立ち上げ前のネットワーク構成



第 6 章

ファイアウォールの立ち上げのNPUパケット フロー

• ファイアウォールの立ち上げの NPU パケット フロー （19 ページ）

ファイアウォールの立ち上げの NPU パケット フロー

ファイアウォールサービスがアクティブでない（サービス停止状態）場合、ファイアウォール VRF 宛てのトラフィックは、（BFDやマルチキャストなどの特定のプロトコルについては）ドロップまたはバイパスする必要があり、DPUにリダイレクトしないでください。次の手順で、この動作を確認します。VRF の状態が正しく、クリーンな整合性チェックを行っているにもかかわらず、トラフィックが予期せず DPU に転送されるか、またはボックス外の場合は、このセクションの確認手順を実行します。ファイアウォール VLAN 宛てのトラフィックは、（マルチキャストおよびブロードキャストトラフィックの場合）ドロップまたはバイパスする必要があり、DPU にリダイレクトしないでください。

手順

ステップ 1 トラフィックがスイッチに到達することが予想されるが、ドロップしていないか、直接ルーティングされていない問題を確認するには、まず VRF の整合性チェッカーを実行します。

例：

```
switch(config)# show consistency-checker service-acceleration vrf tenant1
=======================================
PROCESSING VRF CONSISTENCY CHECK REQUEST
=======================================
VRF 'tenant1' is configured in Service-acceleration
Executing Service-acceleration consistency check for VRF 'tenant1'
**************************************
SERVICE-ACCELERATION CONFIG CONSISTENCY
**************************************
 SUCCESS: Firewall admin state is out-of-service.
 SUCCESS: VRF 'tenant1' is configured with dynamic module affinity (0)
 SUCCESS: Module affinity matches for VRF 'tenant1' - Configured: 0, Programmed: n/a
**************************************
SAS OPERATIONAL CONSISTENCY
```

ファイアウォールの立ち上げの NPU パケット フロー

```
****************************************
 SUCCESS: VRF 'tenant1' operational state 'isolated' is consistent with admin state 'out-of-service'
****************************************
SAS REDIRECT CONSISTENCY
****************************************
 SUCCESS: Pass-1 ACLs in VRF tenant1 have consistent redirect ports: None
 SUCCESS: Pass-2 ACLs in VRF tenant1 have consistent redirect ports: None
 WARNING: ACL: No interfaces found with redirect rules for VRF tenant1
****************************************
POLICY ENFORCEMENT CONSISTENCY
****************************************
 SUCCESS: All data-plane interfaces for vrf tenant1 are present in configured interfaces of Pass-1
 ACL '__epbr_ip_dpu_inside'

 SUCCESS: All data-plane interfaces for vrf tenant1 are present in active interfaces for Pass-1 ACL
 '__epbr_ip_dpu_inside'

 SUCCESS: All data-plane interfaces for vrf tenant1 are present in configured interfaces of Pass-1
 ACL '__epbr_ipv6_dpu_inside'

 SUCCESS: All data-plane interfaces for vrf tenant1 are present in active interfaces for Pass-1 ACL
 '__epbr_ipv6_dpu_inside'
```

`tenant1` を VRF 名に置き換えます。このチェックでは、構成と動作状態に一貫性があるかどうか、および必要なポリシー適用ポイントが配置されているかどうかを確認します。[アウトオブサービス（out-of-service）] 状態で、動作状態が [隔離（isolated）] であることを確認します。

ステップ 2 トラフィックがスイッチに到達すると予想されているのに、ドロップまたは直接転送していない問題を確認するには、まず VLAN の整合性チェッカーを実行します。

例：

```
switch# show consistency-checker service-acceleration vlan 2005
==========================================
PROCESSING VLAN CONSISTENCY CHECK REQUEST
==========================================
VLAN '2005' is configured in Service-acceleration
Executing Service-acceleration consistency check for VLAN '2005'
****************************************
SERVICE-ACCELERATION CONFIG CONSISTENCY
****************************************
 SUCCESS: Firewall admin state is out-of-service.
****************************************
SAS MODULE AFFINITY CONSISTENCY
****************************************
 SUCCESS: VLAN '2005' is configured with dynamic module affinity (0)
 SUCCESS: Module affinity matches for VLAN '2005' - Configured: 0, Programmed: n/a
****************************************
SAS OPERATIONAL CONSISTENCY
****************************************
 SUCCESS: VLAN '2005' operational state 'VLAN set to drop' is consistent with admin state
'out-of-service'
****************************************
SAS VLAN ACCESS MAP CONSISTENCY
****************************************
 SUCCESS: VLAN access map '__epbr_ip_dpu_inside_drop' for Vacl '__epbr_dpu_inside_catchall' and
action 'drop' is consistent
****************************************
SAS VLAN FILTER CONSISTENCY
****************************************
 SUCCESS: VLAN filter __epbr_dpu_inside_catchall for VLAN '2005'
****************************************
SAS VLAN TCAM REDIRECT CONSISTENCY
```

ファイアウォールの立ち上げの NPU パケット フロー

```
**************************************
 WARNING: No redirect entries found for VLAN 2005
```

2005 をVLAN番号に置き換えます。このチェックでは、構成と動作状態に一貫性があるかどうか、および必要なポリシー適用が配置されていることを確認します。ファイアウォールが アウトオブサービス 状態になると、VLAN の動作状態はドロップに設定されます。

ステップ 3 VRFのインターフェイスに対して生成された内部ポリシーがBFDエコーおよびマルチキャスト トラフィックを許可し、他のすべての IPトラフィックをドロップすることを確認します。

例：

```
switch# show access-lists  epbr_ip_dpu_inside dynamic IP access list  epbr_ip_dpu_inside statistics
 per-entry
 1 permit udp any any eq 3785 ttl 255 [match=402393] --> Bypass for BFD
 2 permit ip any 224.0.0.0 15.255.255.255 [match=0] --> Bypass for mcast
4294967295 permit ip any any redirect Null0 [match=417359] --> catchall drop
```

この例は、内部で生成されたIPv4ポリシーを示しています。ACLカウンタを確認して、アクセスリストと一致するパケットがあるかどうかを検出します。

ステップ 4 VLAN に対して生成された内部ポリシーがマルチキャストおよびブロードキャスト トラフィックを許可し、すべての IP トラフィックをドロップすることを確認します。

例：

```
switch# show vlan access-map __epbr_dpu_inside_catchall
Vlan access-map __epbr_dpu_inside_catchall 1
        match ip: __epbr_ip_dpu_inside_bypass
        action: forward         --> Regular forwarding for IP broadcast and multicast traffic
        statistics per-entry
Vlan access-map __epbr_dpu_inside_catchall 2
        match ip: __epbr_ip_dpu_inside_drop
        action: drop            --> Drop all other IPv4 traffic
        statistics per-entry
Vlan access-map __epbr_dpu_inside_catchall 3
        match ipv6: __epbr_ipv6_dpu_inside_bypass
        action: forward         --> Regular forwarding for IPv6 multicast traffic
        statistics per-entry
Vlan access-map __epbr_dpu_inside_catchall 4
        match ipv6: __epbr_ipv6_dpu_inside_drop
        action: drop            --> Drop all other IPv6 traffic
        statistics per-entry
```

ステップ 5 VLAN アクセスマップが FW VLAN に接続されていることを確認します。

例：

```
switch# show vlan filter access-map __epbr_dpu_inside_catchall
vlan map __epbr_dpu_inside_catchall:
        Configured on VLANs:    2003,2005  --> Attached to both FW VLANs
```

ステップ 6 ACL カウンタを確認して、VLAN 内のブリッジド トラフィックがドロップ アクションでアクセスリストと一致しているかどうかを検出します。

例：

```
switch# show vlan access-list __epbr_dpu_inside_catchall
VLAN access-map __epbr_dpu_inside_catchall 1
        IP access list __epbr_ip_dpu_inside_bypass
        2 permit ip any 224.0.0.0 15.255.255.255 [match=0]
        3 permit ip any 255.255.255.255/32 [match=0]
```

```
VLAN access-map __epbr_dpu_inside_catchall 2
        IP access list __epbr_ip_dpu_inside_drop
        4294967295 permit ip any any [match=23755974033]  --> Unicast bridged traffic is dropped
VLAN access-map __epbr_dpu_inside_catchall 3
        IPv6 access list __epbr_ipv6_dpu_inside_bypass
        2 permit ipv6 any ff00:: ff:ffff:ffff:ffff:ffff:ffff:ffff:ffff [match=0]
VLAN access-map __epbr_dpu_inside_catchall 4
        IPv6 access list __epbr_ipv6_dpu_inside_drop
        4294967295 permit ipv6 any any [match=12237925993]
```

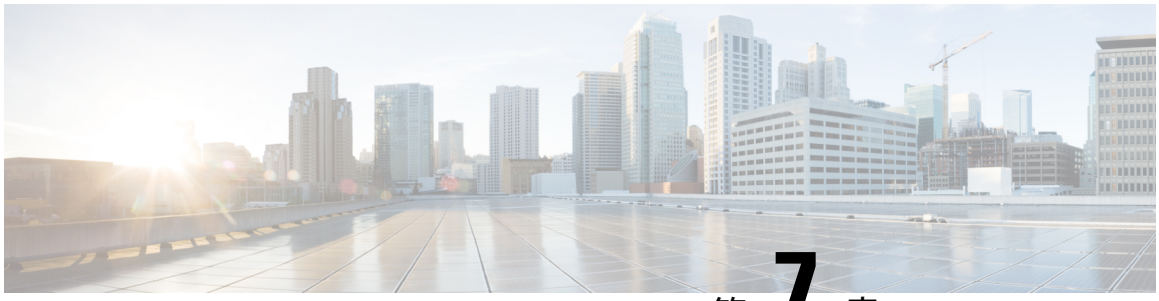
ステップ 7 （オプション）サービスイーサネットインターフェイスのカウンタをチェックして、トラフィックがDPUに送信されていないことを確認します。

例：

```
switch# Show interface service-ethernet 1/1 counters
switch# Show interface service-ethernet 1/2 counters
switch# Show interface service-ethernet 1/3 counters
switch# Show interface service-ethernet 1/4 counters
```

アウトオブサービス状態のDPUにトラフィックを送信してはならないため、これらのインターフェイスのカウンタがゼロのままであるか、または最小限の制御トラフィックだけを表示することを確認します。

これらのチェックを実行することにより、NPU がアウトオブサービス状態ファイアウォール VRF および VLAN のトラフィックを正しく処理していること、プログラムされたポリシーに従ってトラフィックがドロップまたはバイパスしていること、およびトラフィックが DPU に送信されていないことを確認できます。



第 7 章

ファイアウォールの起動

• ファイアウォールの起動 （23 ページ）

ファイアウォールの起動

ファイアウォール サービスと構成済みの VRF が、有効になった後に、予想される動作状態に遷移したことを確認します。サービス ファイアウォールは、**in-service** コマンドの実行後、非同期的に準備完了になります。次の手順により、システムがファイアウォールのためにトラフィックを引き付けて処理する準備が整っていることが確認されます。

手順

ステップ 1 in-service コマンドがファイアウォール サービス用に構成されていることを確認します。

例：

```
switch(config)# show run service-acceleration | section 'service firewall'
  service firewall
    vrf tenant1 module-affinity dynamic
    vrf tenant2 module-affinity dynamic
    vlan id 2003,2005 bridged-traffic module-affinity dynamic
    in-service
```

in-service 行が サービス ファイアウォール 構成の下にあることを確認します。

ステップ 2 HSA と構成された VRF および VLAN の最終状態を確認します。

例：

```
switch# show service-acceleration status details
  Service System: hypershield
    Source Interface: loopback2 (10.29.251.4)
    DPU Load-balance Mode: symmetric-hash
    Agent Status: firewall-ready,redirect-installed --> no firewall-agent-connection-pending status

    Agent Health Status: ok
    Controller Connection Status: success --> should successfully connect to controller
    Agent HA Status: not-initialized
    Services:
      Firewall: in-service
```

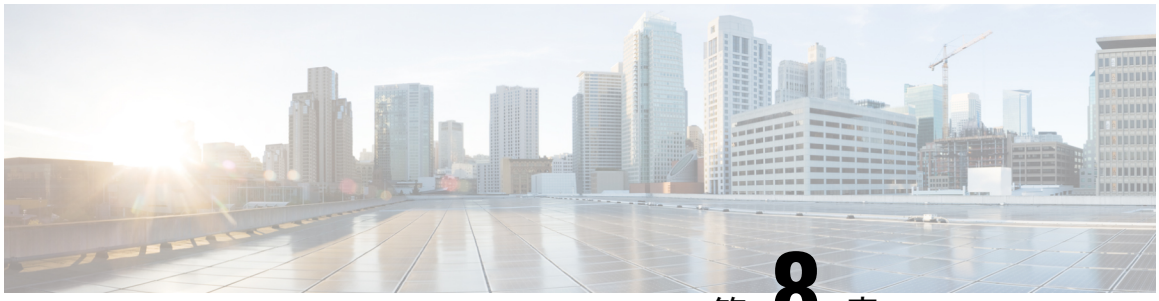
```
VRF                       Operational State       Affinity(DPU)
==========================================================================
tenant1                   forwarding ready        1-4
tenant2                   forwarding ready        1-4

VLAN                      Operational State       Affinity(DPU)
==========================================================================
2003                      forwarding ready        1-4
2005                      forwarding ready        1-4
```

このコマンドは詳細なステータスを提供します。次を検証します：

- エージェントのステータスは 、 `firewall-ready`、 `redirect-installed`など、準備状況を示します。
- ファイアウォール サービスのステータスは `in-service`です。
- 構成された各 VRFと VLAN は、 `forwarding ready` の 動作状態を示します。
- 各 VRF の アフィニティ（DPU）は、ピン接続のロードバランス モードで有効な DPU 番号を表示するか、対称ハッシュ ロードバランス モードが使用されている場合はすべての DPU を表示します。

これらのチェックを実行すると、ファイアウォール サービスがアクティブであり、HSA と構成済みの VRF を含むシステムが、ファイアウォールのトラフィックの処理を開始するために必要な動作状態に達していることを確認できます。



第 8 章

パケット転送

• パケット転送 （25 ページ）

パケット転送

show troubleshoot l3 コマンドを使用して、サービス アクセラレーション リダイレクションを含む、特定の IP フローの転送パスを確認します。このコマンドは、さまざまなソフトウェアおよびハードウェア テーブルのルーティング情報をチェックし、リダイレクションの問題のトラブルシュートに役立つサービス アクセラレーション整合性チェックを含めます。

手順

ステップ 1 特定の IPv4 フローに対して レイヤ 3 トラブルシューティング コマンドを実行します。

例：

```
switch# show troubleshoot l3 ipv4 165.1.1.9 src-ip 166.1.1.9 vrf tenant1
==========================================
PROCESSING VRF CONSISTENCY CHECK REQUEST
==========================================
VRF 'tenant1' is configured in Service-acceleration
Executing Service-acceleration consistency check for VRF 'tenant1'
**************************************
SERVICE-ACCELERATION CONFIG CONSISTENCY
**************************************
 SUCCESS: Firewall admin state is in-service.
 SUCCESS: VRF 'tenant1' is configured with dynamic module affinity (0)
 SUCCESS: Module affinity matches for VRF 'tenant1' - Configured: 0, Programmed: 1-4
**************************************
SAS OPERATIONAL CONSISTENCY
**************************************
 SUCCESS: VRF 'tenant1' operational state 'forwarding ready' is consistent with admin state
'in-service'
**************************************
SAS REDIRECT CONSISTENCY
**************************************
 SUCCESS: Interface Service-Port-Channel512.13 state check passed
 SUCCESS: Pass-1 ACLs in VRF tenant1 have consistent redirect ports: SPo512.13
 SUCCESS: Pass-2 ACLs in VRF tenant1 have consistent redirect ports: SPo512.13
 SUCCESS: ACL: Interface Vlan656 has 2 redirect rule(s) for VRF tenant1
```

パケット転送

```
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ip_dpu_inside) on interface Vlan656 in VRF
 tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ipv6_dpu_inside) on interface Vlan656 in
VRF tenant1 has valid Redirect interface SPo512.13 in HW
SUCCESS: ACL: Interface Vlan657 has 2 redirect rule(s) for VRF tenant1
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ip_dpu_inside) on interface Vlan657 in VRF
 tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ipv6_dpu_inside) on interface Vlan657 in
VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: Interface Ethernet1/12.101 has 2 redirect rule(s) for VRF tenant1
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ip_dpu_inside) on interface Ethernet1/12.101
 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ipv6_dpu_inside) on interface Ethernet1/12.101
 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: Interface Ethernet1/16/4.101 has 2 redirect rule(s) for VRF tenant1
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ip_dpu_inside) on interface Ethernet1/16/4.101
 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-1(__epbr_ipv6_dpu_inside) on interface
Ethernet1/16/4.101 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: Interface Service-Port-Channel512 has 4 redirect rule(s) for VRF tenant1
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-2(__epbr_ip_dpu_post_fwd) on interface
Service-Port-Channel512 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-2(__epbr_ip_dpu_post_fwd) on interface
Service-Port-Channel512 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-2(__epbr_ipv6_dpu_post_fwd) on interface
Service-Port-Channel512 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: policy: SVC Redir L3 Policy Pass-2(__epbr_ipv6_dpu_post_fwd) on interface
Service-Port-Channel512 in VRF tenant1 has valid Redirect interface SPo512.13 in HW
 SUCCESS: ACL: Found redirect rules on 5 interface(s) for VRF tenant1
**************************************
POLICY ENFORCEMENT CONSISTENCY
**************************************
 SUCCESS: All data-plane interfaces for vrf tenant1 are present in configured interfaces of Pass-1
 ACL '__epbr_ip_dpu_inside'
 SUCCESS: All data-plane interfaces for vrf tenant1 are present in active interfaces for Pass-1 ACL
 '__epbr_ip_dpu_inside'
 SUCCESS: All data-plane interfaces for vrf tenant1 are present in configured interfaces of Pass-1
 ACL '__epbr_ipv6_dpu_inside'
 SUCCESS: All data-plane interfaces for vrf tenant1 are present in active interfaces for Pass-1 ACL
 '__epbr_ipv6_dpu_inside'
**********************************
HARDWARE ASIC TYPE: sone
**********************************
SWITCH TYPE: TOR
**********************************
1. CHECK ROUTE IN PI RIB
**********************************
<<snip>>
**********************************
2.  CHECK ROUTE IN PD FIB
**********************************
<<snip>>

**********************************
CHECK ROUTE IN UFIB
**********************************
<<snip>>
**********************************
3. CHECK HOST ROUTE IN FIB AND HARDWARE
**********************************
<<snip>>
**********************************
4. CHECK ROUTE,NEXTHOP IN HARDWARE
**********************************
```

```
<<snip>>
**********************************
RUNNING CONSISTENCY CHECKER
**********************************
**********************************
CHECKING HARDWARE ASIC TYPE
**********************************
Please wait, consistency checker may take a while...

Consistency checker passed for 165.1.1.0/24
```

トラブルシューティングするフローの接続先 IP （165.1.1.9）、送信元 IP （166.1.1.9）、および VRF 名（tenant1）を指定します。

次の項目が含まれる出力を分析します：

- 指定された VRF のサービス アクセラレーション整合性チェックします。
- アクセスリストのハードウェア プログラミング整合性チェック。
- プロトコル独立 RIB（PI RIB）、プロトコル依存 FIB （PD FIB）、および統合 FIB （UFIB）でのルートルック アップ。
- ハードウェアのホスト ルートとネクストホップをチェックします。

整合性チェックで SUCCESS メッセージが表示され、ルート ルックアップで予想されるネクストホップまたはリダイレクション パスが特定されていることを確認します。

ステップ 2 （オプション）特定の IPv6 フローに対して レイヤ 3 トラブルシューティング コマンドを実行します。

例：

```
switch# show troubleshoot l3 ipv6 1:11:: src-ip 1:10:: vrf red
```

このコマンドを活用、IPv6 パケット転送の問題をトラブルシュート、必要に応じて IP アドレスと VRF 名を置き換えます。

show troubleshoot l3 コマンドが正常に完了し、ルートについて「Consistency checker passed」というメッセージが表示される場合は、DPU へのリダイレクションを含め、指定されたパケット フローを転送するために必要なルーティングおよびサービス アクセラレーション構成がシステムにあることを示しています。

ステップ 3 FW VLAN の整合性チェッカーを実行して、ブリッジド トラフィックのリダイレクトの問題を検出します。

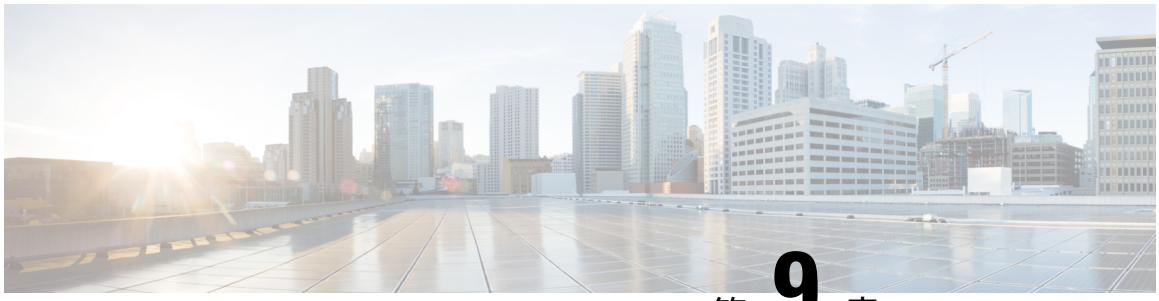
例：

```
switch# show consistency-checker service-acceleration vlan 2005
==========================================
PROCESSING VLAN CONSISTENCY CHECK REQUEST
==========================================
VLAN '2005' is configured in Service-acceleration
Executing Service-acceleration consistency check for VLAN '2005'
**************************************
SERVICE-ACCELERATION CONFIG CONSISTENCY
**************************************
 SUCCESS: Firewall admin state is in-service.
**************************************
SAS MODULE AFFINITY CONSISTENCY
**************************************
 SUCCESS: VLAN '2005' is configured with dynamic module affinity (0)
```

パケット転送

```
 SUCCESS: Module affinity matches for VLAN '2005' - Configured: 0, Programmed: 1-4
****************************************
SAS OPERATIONAL CONSISTENCY
****************************************
 SUCCESS: VLAN '2005' operational state 'forwarding ready' is consistent with admin state 'in-service'
****************************************
SAS VLAN ACCESS MAP CONSISTENCY
****************************************
 SUCCESS: VLAN access map '__epbr_dpu_inside___dpu_all_dpu_vlan_redir' matches policy
'__dpu_all_dpu_vlan_redir' for VLAN '2005'
****************************************
SAS VLAN FILTER CONSISTENCY
****************************************
 SUCCESS: VLAN filter '__epbr_dpu_inside___dpu_all_dpu_vlan_redir' matches policy
'__dpu_all_dpu_vlan_redir' for VLAN '2005'
****************************************
SAS VLAN TCAM REDIRECT CONSISTENCY
****************************************
 SUCCESS: ACL: Vlan 2005 has 2 redirect rule(s)
 SUCCESS: ACL: policy: SVC Redir L2 Policy Pass-1(__epbr_dpu_inside___dpu_all_dpu_vlan_redir) on
vlan 2005 has valid Redirect interface Service-Port-Channel512 in HW
 SUCCESS: ACL: policy: SVC Redir L2 Policy Pass-2(__epbr_ip_dpu_post_fwd_all) on interface
Service-Port-Channel512 has valid Redirect interface Service-Port-Channel512 in HW
 SUCCESS: ACL: policy: SVC Redir L2 Policy Pass-2(__epbr_ipv6_dpu_post_fwd_all) on interface
Service-Port-Channel512 has valid Redirect interface Service-Port-Channel512 in HW
 SUCCESS: ACL: L2 Pass 2 ACL (Service-Port-Channel512) has 2 redirect rule(s)
```

整合性チェッカー コマンドが VLAN に対して正常に完了した場合は、VLAN のブリッジド トラフィックに対して必要な DPU リダイレクション ルールがシステムに構成されていることを示します。



第 9 章

Hypershield エージェントから NX-OS への連携動作

• Hypershield エージェントから NX-OS への連携動作 （29 ページ）

Hypershield エージェントから NX-OS への連携動作

Hypershield Agent（HSA）が、ePBR を使用したトラフィック リダイレクションに必要な構成オブジェクトをデータ管理エンジン（DME）を介して NX-OS に正常にプッシュしたことを確認します。クリーンな整合性チェックにもかかわらず、トラフィックがスイッチに到着し、DPU をドロップまたはバイパスする場合は、このセクションの手順を使用してスイッチのリダイレクション情報を確認します。

手順

エージェントがリダイレクト ポリシーとサービス構成を NX-OS に送信したかどうかを確認します。

例：

```
switch# show system internal service-acceleration dynamic configuration --> agent driven config
isolated from user driven config
<snip>>
vlan 2003
  epbr policy __dpu_all_dpu_vlan_redir
vlan 2005
  epbr policy __dpu_all_dpu_vlan_redir  --> enforce redirection policy on VLAN
vrf context tenant1
  epbr policy __tenant1_dpu_redir       --> enforce redirection policy on VRF
vrf context tenant2
  epbr policy __tenant2_dpu_redir

<<snip>>

epbr service __dpu_all_dpu_vlan_redir type dpu-bridge
 service-end-point module all            --> send to all DPU with symmetric hash for bridged traffic


epbr service __tenant1_dpu_redir type dpu
```

Hypershield エージェントから NX-OS への連携動作

```
  vrf tenant1                                --> VRF specific service
  service-end-point module all vlan 13    --> Encap VLAN ID for VRF and send to all DPU with symmetric
 hash

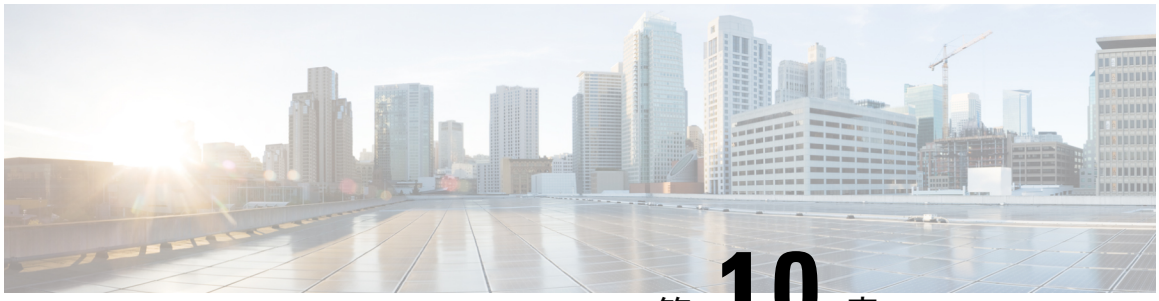
epbr service __tenant2_dpu_redir type dpu
  vrf tenant2
  service-end-point module all vlan 12

<<snip>>

epbr policy __dpu_all_dpu_vlan_redir
  statistics
  match ipv6 address __dpu_ipv6_redir          --> match all v4 traffic
    10 set service __dpu_all_dpu_vlan_redir fail-action drop    --> redirect to service
  match ip address __dpu_redir                 --> match all v6 traffic
    10 set service __dpu_all_dpu_vlan_redir fail-action drop
epbr policy __tenant1_dpu_redir
  statistics
  match ipv6 address __dpu_ipv6_redir          --> match all v4 traffic
    10 set service __tenant1_dpu_redir fail-action drop   --> redirect to service
  match ip address __dpu_redir                 --> match all v6 traffic
    10 set service __tenant1_dpu_redir fail-action drop
epbr policy __tenant2_dpu_redir
  statistics
  match ipv6 address __dpu_ipv6_redir
    10 set service __tenant2_dpu_redir fail-action drop
  match ip address __dpu_redir
    10 set service __tenant2_dpu_redir fail-action drop
```

Hypershield Agent によってプッシュされたダイナミック リダイレクション構成を確認します。リダイレクション ポリシーが正しい VRF と VLAN に関連付けられていること、およびリダイレクション サービスが VRF とVLAN の正しい DPU モジュールと各 VRF のカプセル化 VLAN ID を定義していることを確認します。

これらのチェックを実行することにより、Hypershield Agentが必要なリダイレクション構成オブジェクトをDMEを介してNX-OSに正常にプッシュしていることを確認し、ファイアウォールVRFおよびVLANのトラフィックを適切なDPUにリダイレクトする方法を定義できます。



第 10 章

NPU から DPU へのリダイレクトの問題

• NPU から DPU へのリダイレクトの問題 （31 ページ）

NPU から DPU へのリダイレクトの問題

リダイレクション ポリシーが NPU ハードウェア（TCAM）で正しくプログラムされていること、および VRF と VLAN のトラフィックがサービス ポートチャンネル サブインターフェイスおよびサービス ポートチャンネル インターフェイスを通じて適切な DPU に正常にリダイレクトされていることを確認します。これらのチェックは、ポリシーがエージェントによって正しくプッシュされている場合でも、トラフィックが着信しているが DPU にリダイレクトされていないか、または誤った DPU に送信されている場合に、原因を特定するのに役立ちます。

手順

ステップ 1 VRF ごとに作成されたサービス ポートチャンネル サブインターフェイスを識別して、 VRF トラフィックを DPU にリダイレクトし、それらのステータスを確認します。各 VLAN に使用されているサービス ポート チャネルを識別して、 VLAN 内のブリッジド トラフィックを DPU にリダイレクトし、ステータスを確認します。

例：

```
switch# show service-acceleration redirect-policy brief
VRF                              AF Type Interface[Status]  Affinity Redirect Status
================================================================================================
tenant1                          IPv4    SPo512.13[UP]      1-4      Enabled
tenant2                          IPv4    SPo512.12[UP]      1-4      Enabled
tenant1                          IPv6    SPo512.13[UP]      1-4      Enabled
tenant2                          IPv6    SPo512.12[UP]      1-4      Enabled
VLAN                             AF Type Interface[Status]  Affinity Redirect Status
================================================================================================
2003                             IPv4    SPo512[UP]         1-4      Enabled
2005                             IPv4    SPo512[UP]         1-4      Enabled
2003                             IPv6    SPo512[UP]         1-4      Enabled
2005                             IPv6    SPo512[UP]         1-4      Enabled
```

VRF およびアドレス ファミリごとに作成されたサービス ポートチャンネル サブインターフェイス（`Interface[Status]`）を識別します。インターフェイスのステータスが `[UP]` であること、および `[リダイ`

NPU から DPU へのリダイレクトの問題

レクト ステータス（Redirect Status）] が [有効（Enabled）] であることを確認します。各 VLAN で使用されているサービス ポート チャネル インターフェイスと、[リダイレクト ステータス（Redirect Status）] が **[有効（Enabled）]** であることを確認します。

ステップ 2 特定の サービスイーサネット ポートチャンネル サブインターフェイスの構成の詳細を確認します。

例：

```
switch# show interface service-port-channel 512.13 br --> verify intf state and encap
------------------------------------------------------------------------------------------
Service      VLAN    Type Mode   Status  Reason                                Speed   Protocol
Port-Channel
------------------------------------------------------------------------------------------
SPo512.13    13      eth  routed up      none                                   a-200G(D)    --
```

前のステップで特定したサブインターフェイス（SPO 512.13）を指定します。VLAN ID が VRF で構成されたものと一致すること、[モード（Mode）] が [ルーテッド（routed）] であること、および [ステータス（Status）] が **[アップ（up）]** であることを確認します。

ステップ 3 特定の VRF の ePBR で詳細なポリシー プログラミング情報を確認します。

例：

```
switch# show service-acceleration redirect-policy vrf tenant1
  VRF: tenant1
  Policy-map: __tenant1_dpu_redir
  Default Traffic Action: Redirect
  Match clause:
    ip address(access-lists): __dpu_ipv6_redir
    action: Redirect              --> information matches DME objects
    status(inside): CREATED/ENABLED         status(post_fwd): CREATED/ENABLED --> created/enabled
states
      service __tenant1_dpu_redir, sequence 10, fail-action Drop
        service-module 1-4 vlan 13 [UP] [SPo512.13]    --> correct interface, state, and vlan
  Match clause:
    ip address(access-lists): __dpu_redir
    action: Redirect
    status(inside): CREATED/ENABLED         status(post_fwd): CREATED/ENABLED
      service __tenant1_dpu_redir, sequence 10, fail-action Drop
        service-module 1-4 vlan 13 [UP] [SPo512.13]
```

tenant1 を VRF 名に置き換えます。match 句の [ステータス（内部）（status(inside)）] と [ステータス（post_fwd）（status（post/fwd））] が [作成/有効（CREATED/ENABLED）] と表示されていることを確認します。service-module、vlan,、およびサービス インターフェイス（SPo512.13）の情報が正しく、この VRF で想定される DPU およびサブインターフェイスと一致していることを確認します。

ステップ 4 VLAN 内のブリッジド トラフィックの ePBR で詳細なポリシー プログラミング情報を確認します。

例：

```
switch# show service-acceleration redirect-policy vlan 2005
  VLAN: 2005
  Policy-map: __dpu_all_dpu_vlan_redir
   Default Traffic Action: Redirect
  Match clause:
    ip address(access-lists): __dpu_redir
    action: Redirect       --> information matches DME objects
    status(inside): CREATED/ENABLED         status(post_fwd): CREATED/DISABLED --> created/enabled
 states
      service __dpu_all_dpu_vlan_redir, sequence 10, fail-action Drop
        service-module 1-4 [UP] [SPo512]   --> correct interface, state
```

NPU から DPU へのリダイレクトの問題

```
  Match clause:
    ip address(access-lists): __dpu_ipv6_redir
    action: Redirect
    status(inside): CREATED/ENABLED         status(post_fwd): CREATED/DISABLED
      service __dpu_all_dpu_vlan_redir, sequence 10, fail-action Drop
        service-module 1-4 [UP] [SPo512]
```

2005 を VLAN 番号に置き換えます。[ステータス（内部）（status(inside)）]が [作成/有効（CREATED/ENABLED）] で、[ステータス（post_fwd）（status（post/fwd））] が [作成/有効（CREATED/ENABLED）] であることを確認します。service-module、およびサービス インターフェイス（SPo512）の情報が正しく、VLAN で想定される DPU と一致していることを確認します。

ステップ 5 VRF の内部で生成されたポリシーと一致するパケット カウンタを確認します。

例：

```
(IPv4 traffic)
switch# show access-lists  __epbr_ip_dpu_inside dynamic
IP access list __epbr_ip_dpu_inside    --> IPv4 traffic
        statistics per-entry
        1 permit udp any any eq 3785 ttl 255 [match=0]
        2 permit ip any 224.0.0.0 15.255.255.255 [match=0]
        26201 permit ip any any nve vni 4 redirect Service-Port-Channel512.13 [match=105469965]
--> VNI 4 matches IPv4 table ID for VRF tenant1 mapped to SPO 512.13
        31101 permit ip any any nve vni 5 redirect Service-Port-Channel512.12 [match=105473341]
        4294967295 permit ip any any redirect Null0
```

例：

```
(IPv6 traffic)
switch# show access-lists  __epbr_ipv6_dpu_inside dynamic
IPv6 access list __epbr_ipv6_dpu_inside
        statistics per-entry
        1 permit udp any any eq 3785 ttl 255 [match=0]
        2 permit ipv6 any ff00:: ff:ffff:ffff:ffff:ffff:ffff:ffff:ffff [match=0]
        25901 permit ipv6 any any nve vni 4 redirect Service-Port-Channel512.13 [match=56821638]
 --> VNI 4 matches IPv4 table ID for VRF tenant1 mapped to SPO 512.13
        30801 permit ipv6 any any nve vni 5 redirect Service-Port-Channel512.12 [match=56823422]
        4294967295 permit ipv6 any any redirect Null0
```

上記のルールで VNI として使用される **show vrf** *vrf* **detail** コマンドを介して VRF のテーブル id を特定して、対象の VRF に関連するルールを特定します。ルールに、VRF の適切なサブインターフェイスへのリダイレクションが表示されていることを確認します。VRF ルールのパケット ヒット カウンタを確認します。

ステップ 6 VLAN アクセス マップが作成され、ブリッジされた IPv4 または IPv6 トラフィック用の VLAN に接続されていることを確認します。

例：

```
switch# show vlan filter
vlan map __epbr_dpu_inside___dpu_all_dpu_vlan_redir:
       Configured on VLANs:    2003,2005  --> shared VACL attached to FW VLANs with symmetric hash
switch# show vlan access-map __epbr_dpu_inside___dpu_all_dpu_vlan_redir
Vlan access-map __epbr_dpu_inside___dpu_all_dpu_vlan_redir 1
        match ip: __epbr_ip_dpu_inside_bypass  --> same bypasses for multicast/broadcast
        action: forward
        statistics per-entry
Vlan access-map __epbr_dpu_inside___dpu_all_dpu_vlan_redir 3
        match ipv6: __epbr_ipv6_dpu_inside_bypass
```

NPU から DPU へのリダイレクトの問題

```
        action: forward
        statistics per-entry
Vlan access-map __epbr_dpu_inside___dpu_all_dpu_vlan_redir 19801
        match ip: __epbr_dpu_inside_ip___dpu_all_dpu_vlan_redir
        action: redirect Service-Port-Channel512     --> Redirect ipv4 traffic to SPO
        statistics per-entry
Vlan access-map __epbr_dpu_inside___dpu_all_dpu_vlan_redir 20101
        match ipv6: __epbr_dpu_inside_ipv6___dpu_all_dpu_vlan_redir
        action: redirect Service-Port-Channel512     --> Redirect ipv6 traffic to SPO
        statistics per-entry
```

ステップ 7 アクセスマップ内および VACL カウンタ内で使用されるアクセスリストを確認する。

例：

```
switch# show access-lists __epbr_dpu_inside_ip___dpu_all_dpu_vlan_redir  dynamic
IP access list __epbr_dpu_inside_ip___dpu_all_dpu_vlan_redir
        19801 permit ip any any       --> all ipv4 traffic except bypassed traffic
switch# show access-lists __epbr_dpu_inside_ipv6___dpu_all_dpu_vlan_redir  dynamic
IPv6 access list __epbr_dpu_inside_ipv6___dpu_all_dpu_vlan_redir
        20101 permit ipv6 any any     --> all ipv6 traffic except bypassed traffic
```

ステップ 8 （オプション）サービス アクセラレーション リダイレクト ポリシーのリソース使用率を確認します。

例：

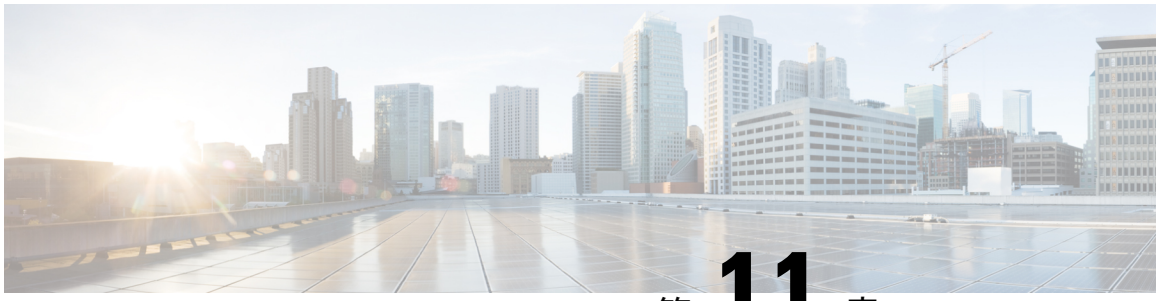
```
switch# show system internal access-list resource utilization | grep -i pass
Ingress SVC Redir L3 Policy Pass-1-IPV4                          6       7050    0.08
Ingress SVC Redir L3 Policy Pass-1-IPV6                          6       3522    0.17
Ingress SVC Redir L3 Policy Pass-2-IPV4                          6       7050    0.08
Ingress SVC Redir L3 Policy Pass-2-IPV6                          6       3522    0.17
Ingress SVC Redir L2 Policy Pass-1-IPV4                          5       7051    0.07
Ingress SVC Redir L2 Policy Pass-1-IPV6                          4       3524    0.11
Ingress SVC Redir L2 Policy Pass-2-IPV4                          2       7054    0.02
Ingress SVC Redir L2 Policy Pass-2-IPV6                          2       3526    0.05
Ingress SVC Redir L2 Policy Pass-1-MAC                           0       7040    0.00
Ingress SVC Redir L3 Policy Pass-1-IPV4                          6       7050    0.08
Ingress SVC Redir L3 Policy Pass-1-IPV6                          6       3522    0.17
Ingress SVC Redir L3 Policy Pass-2-IPV4                          6       7050    0.08
Ingress SVC Redir L3 Policy Pass-2-IPV6                          6       3522    0.17
Ingress SVC Redir L2 Policy Pass-1-IPV4                          5       7051    0.07
Ingress SVC Redir L2 Policy Pass-1-IPV6                          4       3524    0.11
Ingress SVC Redir L2 Policy Pass-2-IPV4                          2       7054    0.02
Ingress SVC Redir L2 Policy Pass-2-IPV6                          2       3526    0.05
Ingress SVC Redir L2 Policy Pass-1-MAC                           0       7040    0.00
Label LBL AO,  Ingress IPv4 SVC Redir L3 Policy Pass-1
       2       125     1.57
Label LBL AP,  Ingress IPv6 SVC Redir L3 Policy Pass-1
       2       125     1.57
Label LBL AQ,  Ingress IPv4 SVC Redir L3 Policy Pass-2
       2       125     1.57
Label LBL AR,  Ingress IPv6 SVC Redir L3 Policy Pass-2
       2       125     1.57
Label LBL AY,  Ingress IPv4 SVC Redir L2 Policy Pass-1 / Ingress IPv6 SVC Redir L2 Policy Pass-1
/ Ingress MAC SVC Redir L2 Policy Pass-1 2       125     1.57
Label LBL BA,  Ingress IPv4 SVC Redir L2 Policy Pass-2
       2       125     1.57
Label LBL BB,  Ingress IPv6 SVC Redir L2 Policy Pass-2
       2       125     1.57
```

NPU から DPU へのリダイレクトの問題

`Pass-1` および `Pass-2` リダイレクト ポリシーおよび L2 ポリシーを含む ACL ポリシーのハードウェアウェア リソースの使用状況を確認します。高い使用率またはエラーは、リソースの枯渇を示している可能性があります。

これらのチェックを実行することにより、ファイアウォール VRF および VLAN のトラフィックをサービス ポートチャンネル サブインターフェイスまたは、サービス ポートチャンネル インターフェイスを介して適切な DPU にリダイレクトするように NPU が正しくプログラムされていることを確認し、トラフィックが予想されるハードウェア ルールにヒットしていることを確認できます。

NPU から DPU へのリダイレクトの問題



第 11 章

DPU パケット フローを投稿

• DPU パケット フローを投稿 （37 ページ）

DPU パケット フローを投稿

サービス ポートチャンネル インターフェイスに適用される Pass-2 ACL をチェックし、インターフェイス構成の詳細を確認して、DPU から戻るトラフィックが接続先への転送のために NPU によって正しく処理されていることを確認します。トラフィックが NPU でドロップしているか、DPUから戻った後にルーティングされない場合は、このセクションの確認手順を実行します。

手順

ステップ 1 フローを学習する前に、検査の2番目のパスでDPUにリダイレクトするVRFの内部で生成されたポリシーと一致するパケット カウンタを確認します。

例：

```
(IPv4 traffic)
switch#  show access-lists __epbr_ip_dpu_post_fwd dynamic
IP access list __epbr_ip_dpu_post_fwd
        statistics per-entry
        26201 permit ip any any nve vni 4 redirect Service-Port-Channel512.13 [match=117821124]
        31101 permit ip any any nve vni 5 redirect Service-Port-Channel512.12 [match=117826975]
        4294967295 permit ip any any [match=0]
```

例：

```
(IPv6 traffic)
switch# show access-lists __epbr_ipv6_dpu_post_fwd dynamic
IPv6 access list __epbr_ipv6_dpu_post_fwd
        statistics per-entry
        25901 permit ipv6 any any nve vni 4 redirect Service-Port-Channel512.13 [match=60695847]
        30801 permit ipv6 any any nve vni 5 redirect Service-Port-Channel512.12 [match=60698895]
        4294967295 permit ipv6 any any [match=0]
```

上記のルールで VNI として使用される **show vrf** <> **detail** を介して VRF のテーブル ID を特定して、対象の VRF に関連するルールを特定します。ルールに DPU から返されるトラフィックに一致する permit エントリが含まれていることを確認し、そのトラフィックを VRF の正しいサービス ポートチャンネル サブイ

DPU パケット フローを投稿

ンターフェイスにリダイレクトします。これらの VRF ルールを使用して新しいフロー学習時のパケット ヒット カウンタを確認します。

ステップ 2 フローを学習する前に、検査の 2 番目のパスで DPU にリダイレクトする VLAN の内部で生成されたポリシーと一致するパケット カウンタを確認します。

例：

```
switch# show access-lists __epbr_ip_dpu_post_fwd_all dynamic

IP access list __epbr_ip_dpu_post_fwd_all
        statistics per-entry
        4294967295 permit ip any any redirect Service-Port-Channel 512 [match=0] --> resend to DPU
 for Pass2
switch# show access-lists __epbr_ipv6_dpu_post_fwd_all dynamic

IPv6 access list __epbr_ipv6_dpu_post_fwd_all
        statistics per-entry
        4294967295 permit ipv6 any any redirect Service-Port-Channel 512 [match=0]
```

ピン接続モードの場合、DPU ごとに一意の ACL が作成されます。

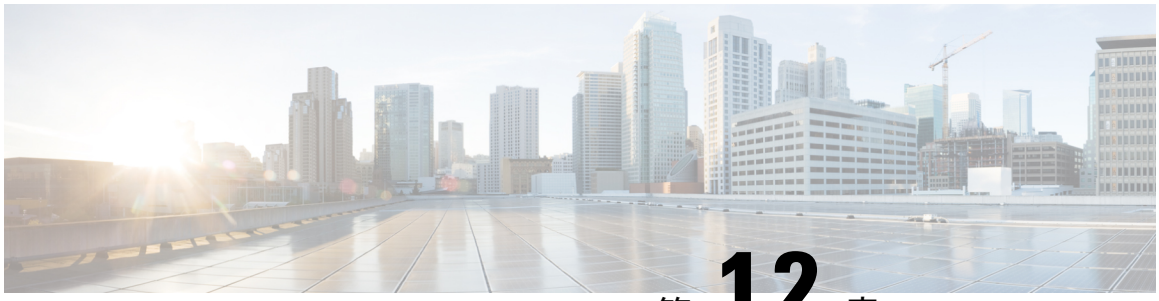
ステップ 3 DPU 接続サービス イーサネット ポートの統計を表示します。

例：

```
switch# show interface service-ethernet 1/1-4
switch# show interface service-ethernet 1/2 counters
switch# show interface service-port-channel 1-4
switch# show interface service-port-channel 512
switch# show int service-ethernet 1/2 counters detailed
switch# show interface service-ethernet <subinterface> counters
switch# show int service-ethernet <> counters errors
switch# show int service-ethernet 1/1-4 counters brief
```

これらのコマンドは、パケット/バイト カウンタ、詳細統計情報、エラー統計情報、平均レートなど、DPU に接続されているサービス イーサネット インターフェイスのさまざまな統計情報を提供します。これらのカウンタをチェックすると、トラフィックが予想どおりに DPU に到達しているかどうかを判断できます。

これらのチェックを実行することにより、NPU が DPU からの戻りトラフィックを処理するように Pass-2 ACL を正しくプログラムしていること、およびサービスポート チャンネル インターフェイスとサブインターフェイスが転送用の正しいパラメータで構成されていることを確認できます。



第 12 章

パケット トレーサのサポート

• パケット トレーサのサポート （39 ページ）

パケット トレーサのサポート

パケット トレーサ電力事業を活用、エンドツーエンドの NPU から DPU への NPU パケット フローのさまざまなポイントでパケットをキャプチャして分析します。これにより、さまざまな段階でトラフィック処理の詳細なトラブルシューティングが可能になります。

これらの手順は、特定のポイントでパケットをキャプチャする方法の概要を示しています。

- NPU 入力
- NPU から DPU TX へ
- DPU から NPU RX へ：最初のパケット
- DPU から NPU RX へ：後続のパケット
- NPU の出力

手順

ステップ 1 入力 レイヤ 3 インターフェイス（NPU 入力）で受信されたパケットをキャプチャします。

例：

```
switch# packet-trace
switch(packet-trace)# trigger init rxpp
switch(packet-trace-init)# packet-format eth-ipv4-tcp
switch(packet-trace-init-pkt)# set outer ipv4 src-ip 10.1.0.2 dst-ip 16.1.0.2
switch(packet-trace-init-pkt)# start
...
switch(packet-trace-init-pkt)# status
switch(packet-trace-init-pkt)# report
switch(packet-trace-init-pkt)# exit
```

これは、DPUにリダイレクトする前に、入力レイヤ3インターフェイスでNPUが受信したパケットをキャプチャします。

ステップ 2 サービス イーサネット インターフェイス（SETH TX）上の NPU から DPU に送信されたパケットをキャプチャします。

例：

```
switch# packet-trace
switch(packet-trace)# trigger init txpp
switch(packet-trace-init)# packet-format eth-ipv4-tcp
switch(packet-trace-init-pkt)# set outer ipv4 src-ip 10.1.0.2 dst-ip 16.1.0.2
switch(packet-trace-init-pkt)# start
...
switch(packet-trace-init-pkt)# status
switch(packet-trace-init-pkt)# report
switch(packet-trace-init-pkt)# exit
```

これは、NPU からサービス イーサネット インターフェイス上の DPU に送信されたパケットをキャプチャします。



（注） スナップショットは DPU ヘッダーのカプセル化が行われる前に取得されるため、この時点では DPU ヘッダーの詳細を追跡またはキャプチャすることはできません。

ステップ 3 パスビットが設定された（SETH RX dpu pass 0）状態で NPU が DPU から受信した最初のパケットをキャプチャします。

例：

```
switch# packet-trace
switch(packet-trace)# trigger init rxpp
switch(packet-trace-init)# packet-format eth-dpu-ipv4-tcp
switch(packet-trace-init-pkt)# set dpu pass-bit 0 service-vlan 10
switch(packet-trace-init-pkt)# set outer ipv4 src-ip 10.1.0.2 dst-ip 16.1.0.2
switch(packet-trace-init-pkt)# start
...
switch(packet-trace-init-pkt)# status
switch(packet-trace-init-pkt)# report
switch(packet-trace-init-pkt)# exit
```

これは、サービスイーサネット インターフェイスの DPU から NPU が受信した最初のパケット、特に DPU パスビット 0 でマークされたパケット（通常、DPU のコントロール プレーンにパントされるフローの最初のパケット）をキャプチャします。



（注） スナップショットは DPU のカプセル化が解除される前に取得されますが、受信した DPU ヘッダーのインサイトを得ることできます。ルーテッド トラフィックの場合、フィルタ処理するサービス VLAN は、という **show service-acceleration redirect-policy vrf** *name* の VLAN 情報から取得できます。ブリッジド トラフィックの場合は、パケットの転送用 VLAN をサービス VLAN として使用します。

ステップ 4 パスビットが設定された状態（SETH RX dpu pass 1）で DPU から NPU が受信した後続のパケットをキャプチャします。

例：

```
switch# packet-trace
switch(packet-trace)# trigger init rxpp
switch(packet-trace-init)# packet-format eth-dpu-ipv4-tcp
switch(packet-trace-init-pkt)# set outer ipv4 src-ip 10.1.0.2 dst-ip 16.1.0.2
switch(packet-trace-init-pkt)# set dpu pass-bit 1 service-vlan 10
switch(packet-trace-init-pkt)# start
...
switch(packet-trace-init-pkt)# status
switch(packet-trace-init-pkt)# report
switch(packet-trace-init-pkt)# exit
```

これは、サービス イーサネット インターフェイスの DPU から NPU が受信したフローの後続パケットをキャプチャします。具体的にそれらはDPUのデータ プレーン（P4）によって直接処理され、DPUパスビット 1 でマークされます。



（注） スナップショットはDCPUのカプセル化が解除される前に取得されますが、受信したDPUヘッダーのインサイトを得ることできます。

ステップ 5 ルーティング（NPU 出力）後に NPU から出力 L3 インターフェイスに送信されたパケットをキャプチャします。

例：

```
switch# packet-trace
switch(packet-trace)# trigger init txpp
switch(packet-trace-init)# packet-format eth-dpu-ipv4-tcp
switch(packet-trace-init-pkt)# set outer ipv4 src-ip 10.1.0.2 dst-ip 16.1.0.2
switch(packet-trace-init-pkt)# start
...
switch(packet-trace-init-pkt)# status
switch(packet-trace-init-pkt)# report
switch(packet-trace-init-pkt)# exit
```

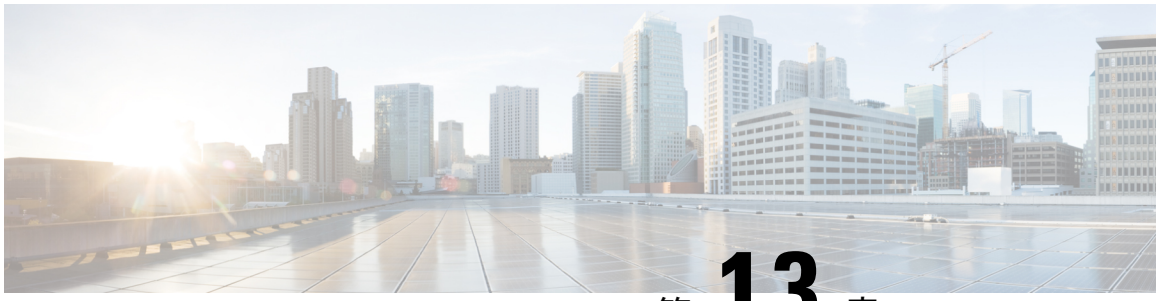
これは、DPU 後に処理およびルーティングされた後に、出力レイヤ 3 インターフェイスに向けて NPU によって送信されたパケットをキャプチャします。



（注） スナップショットは DPU ヘッダーのカプセル化が行われる前に取得されるため、この時点では DPU ヘッダーの詳細を追跡またはキャプチャすることはできません。

これらのパケットキャプチャ手順を実行した後、キャプチャされたパケットを分析して、NPU から DPU への NPU フローのさまざまなポイントでトラフィックがどのように処理されているかのインサイトを得ることができます。

パケット トレーサのサポート



第 13 章

VRF 間トラフィック インスペクション

• VRF 間トラフィック インスペクション （43 ページ）

VRF 間トラフィック インスペクション

ルート リークの詳細を使用して VRF 間トラフィック インスペクションのトラブルシューティングを行う場合、ルートは最初に送信元VRF(赤色など)で学習され、次にターゲットVRF（緑色など）にリークされます。ネクストホップ情報を含むルートエントリで示されます。送信元 VRF を参照するために使用されます。

show troubleshoot コマンドを実行すると、ルート リークの包括的なビューが表示されます。出力には、PI RIB、 FIB、およびハードウェア レイヤからのルート情報が表示されます。これにより、VRF 全体でルートの存在とネクストホップの詳細が確認され、適切な転送のためにハードウェアで設定されていることを検証します。この階層型の検査は、ルート リークが正常に機能している場所、または VRF 間トラフィック パスで問題が発生している可能性がある場所を特定するのに役立ちます。

この手順を活用、 VRF 間トラフィック インスペクションのルートリークの詳細を確認し、それに応じてトラブルシュート。

手順

ステップ 1 送信元 VRF（VRF red など）に対して **show ip route** *ip-address* **vrf** *vrf-name* コマンドを使用します。

例：

```
show ip route 12.10.1.0/24 vrf red
IP Route Table for VRF "red"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

12.10.1.0/24, ubest/mbest: 1/0
*via 1.10.1.2, [1/0], 00:02:58, static
```

ステップ 2 ターゲット VRF（VRF Green など）に対して **show ip route** *ip-address* **vrf** *vrf-name* コマンドを使用します。

VRF 間トラフィック インスペクション

例：

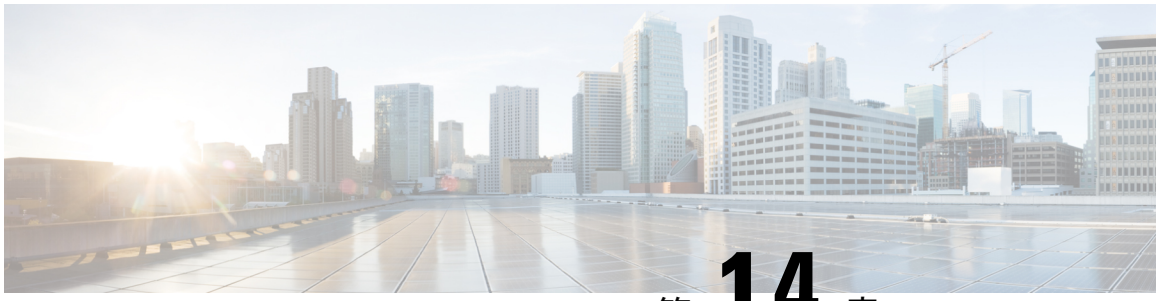
```
show ip route 12.10.1.0/24 vrf green
IP Route Table for VRF "green"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

12.10.1.0/24, ubest/mbest: 1/0
*via 1.10.1.2%red, [20/0], 00:13:58, bgp-100, external, tag 100
```

ステップ 3 ルート リークの詳細を表示するには、 **troubleshoot** コマンドを活用。ルートの詳細は、URIB、 FIB、およびハードウェアから表示されます。

例：

```
show troubleshoot l3 ipv4 12.10.1.0/24 vrf green
************************************
1. CHECK ROUTE IN PI RIB
************************************
show ip route 12.10.1.0/24 vrf green
prefix : 12.10.1.0
mask length : 24
IP Route Table for VRF "green"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
12.10.1.0/24, ubest/mbest: 1/0
*via 1.10.1.2%red, [20/0], 00:10:15, bgp-100, external, tag 100
************************************
3. CHECK HOST ROUTE IN FIB AND HARDWARE
************************************
show forwarding route 12.10.1.0/24 platform vrf green module 1
Prefix 12.10.1.0/24, No of paths: 1, Update time: Fri May 1 04:37:41 2026
SGT: 0
DPI: 0
Vobj id: 1 Partial Install: No
1.10.1.2 Ethernet1/10
HH:0x80b78700 Flags:0x0 Extended Flags:0x100 Holder:0x1 Next_obj_type:9
Hw-idx vobj: unit-0:0x40001 unit-1:0x0 unit-2:0x0, cmn-index: 500009, LIF:16394 buf-idx 0(0)
************************************
4. CHECK ROUTE,NEXTHOP IN HARDWARE
************************************
dchal module 1 "route show 0 4 12.10.1.0 24"
IP Address: b'12.10.1.0'
Length: 24
Unit: 0
VRF: 4
VRF Redirect Id: 0x6
```



第 14 章

高可用性

• 高可用性 （45 ページ）

高可用性

次の手順を使用し、高可用性（HA）の詳細を確認し、それに応じてこれらのシナリオの問題をトラブルシュート。

- 接続の問題
- 両方のピアが 非サービス モードである
- 一方のピアがインサービスモードで、もう一方のピアがインサービスモードではない
- 両方のピアがインサービス モードである
- メンバーシップの失敗

高可用性接続の問題

Hypershield Agent 間の高可用性（HA）接続は、次の場合にのみ実現されます：

- HA 設定が完全かつ正しく対称である
- HA が有効になっていて、および
- ファイアウォール サービスが構成されていることを確認します。

接続の問題をトラブルシューティングするには、次の手順を実行します：

- HA 設定を確認するには、次の手順を実行します。
- ピアとコンテナ間のネットワーク接続を確認します。
- 高可用性の Hypershield Agent の状態を確認します。

手順

ステップ 1 高可用性ステータスとロールを確認します。

例：

```
show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.1)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: not-ready
    Agent HA Status: not-ready
    Peers:
      PeerIP              Peer Service State  HA State with Peer  Reason
      ------------------- ------------------  ------------------  --------------
      192.1.1.2           unknown             no-ha               no peer connectivity
```

ステップ 2 各ピアでのサービス アクセラレーション構成とネットワーク構成とルートを確認します。

- HA 設定が完全かつ正しく対称であること
- HA が有効になっています
- ファイアウォール サービスが構成されていることを確認します。

例：

```
switch# show run service-acceleration
<<snip>>
version 10.6(3q) Bios:version 01.17
feature service-acceleration
service system hypershield
  source-interface loopback2
  high-availability
    source-interface loopback1
    peer 192.1.1.2
    no shutdown
  service firewall
    vrf tenant1 module-affinity dynamic
    vrf tenant2 module-affinity dynamic
    vlan id 2003,2005 bridged-traffic module-affinity dynamic
```

ステップ 3 ローカル HA IP から設定されたピアへの HA 接続用にネットワーク設定が設定されていることを確認します。この例では、ループバック インターフェイスは正しい IP アドレスおよび OSPF 設定で構成されています。ルーティング テーブルには、イーサネット インターフェイスを介して OSPF を使用して到達可能な接続先へのルートが表示されています。

例：

```
switch# show run interface loopback 1
<<snip>>
version 10.6(3q) Bios:version 01.17
interface loopback1
  ip address 192.1.1.1/32
  ip ospf cost 1
  ip router ospf 10 area 0.0.0.0
  ipv6 router ospfv3 10 area 0.0.0.0
switch# show ip route 192.1.1.2
IP Route Table for VRF "default"
```

```
<<snip>>
192.1.1.2/32, ubest/mbest: 1/0
    *via 192.1.1.2, Eth1/16/3, [110/2], 00:22:46, ospf-10, intra
     via 192.1.1.2, Eth1/16/3, [250/0], 00:20:51, am
```

ステップ 4 各ピアで HA 整合性チェッカーを実行し、Hypershield Agent の駆動状態で NX-OS構成を検証し、不一致を検出します。

例：

```
switch# show consistency-checker service-acceleration high-availability
=====================================================
PROCESSING HIGH-AVAILABILITY CONSISTENCY CHECK REQUEST
=====================================================
**************************************
HA FIREWALL STATE CONSISTENCY
**************************************
  [PASS] Firewall configured and internal states match: out-of-service --> Firewall is created
  [PASS] Agent's firewall readiness state matches internal readiness state: not-ready
  [PASS] Agent's firewall readiness state matches published readiness state: not-ready
**************************************
FW VLAN OPERATIONAL STATE CONSISTENCY
**************************************
FW L2, L3 VLAN Set Consistency Checks
======================================
  Expected L3 FW VLANs (from VRFs): 656-657,659,755,859
  Expected L2 FW VLANs : 2003,2005
  Expected Combined L2+L3 VLANs: 656-657,659,755,859,2003,2005
  L3 VLAN Comparison:
    [PASS] L3 VLANs match published FW L3 VLANs
  L2 VLAN Comparison:
    [PASS] L2 VLANs match published FW L2 VLANs
  Combined L2+L3 VLAN Comparison:
    [PASS] Combined L2+L3 FW VLANs identified as expected
**************************************
HA PEER CONSISTENCY
**************************************
HA Configuration and Peer State Checks
======================================
  HA Admin State Comparison:
    [PASS] HA admin state matches with internal state: no-shutdown  --> HA is enabled
  HA Source interface Comparison:
    [PASS] HA Source interface matches: loopback1
  HA Source IP Address Comparison:
    [PASS] HA source IP address matches: 192.1.1.2
  HA Peer Configuration Validation:
    [PASS] Peer 192.1.1.1 found internally.
    HA Peer State Validation:
    [PASS] Internal Peer service state for peer 192.1.1.1 matches service state published by agent:
 unknown
            --> Peer is configured
    [PASS] Peer 192.1.1.1 derived firewall state matches: 'unknown'
  [NOTE] HA Troubleshooting Suggestion:
    Detected 1 peer(s) with service state unknown:
      - Peer 192.1.1.1: unknown
    To identify HA peer connectivity issues, run:
      service system hypershield test high-availability
HA VPC Peer Consistency Checks
==============================
  Validating HA Peer Info:
  Internal Peer state validation:
    VPC peer is alive
    [PASS] Peer 192.1.1.1 is being detected as an alive VPC peer
  VPC Peer Firewall State Validation:
```

```
    [PASS] Internally known HA VPC peer firewall state is 'unknown' (VPC peer exists)
    [PASS] Published HA VPC peer firewall state is 'unknown' (VPC peer exists)
VPC State Consistency Checks
============================
  Validating 4 VPC(s)
  VPC 60 (Po60):
    [Pass] Internal details for VPC 60 matches configuration
    [PASS] VPC 60 is of interest and allows 3 FW l2/l3 VLAN(s): 657,659,2005
  VPC 61 (Po61):
    [Pass] Internal details for VPC 61 matches configuration
    [PASS] VPC 61 is of interest and allows 2 FW l2/l3 VLAN(s): 656,2005
  VPC 62 (Po62):
    [Pass] Internal details for VPC 62 matches configuration
    [PASS] VPC 62 is of interest and allows 2 FW l2/l3 VLAN(s): 755,2003
  VPC 63 (Po63):
    [Pass] Internal details for VPC 63 matches configuration
    [PASS] VPC 63 is of interest and allows 1 FW l2/l3 VLAN(s): 2003
**************************************
HA VRF/VLAN OPERATIONAL STATE CONSISTENCY
    [PASS] 2 VRF(s) were validated and are in 'isolated' state
    [PASS] VLANs 2003,2005 were validated and are in 'VLAN set to drop' state
    [SKIP] VRF/VLAN vpc peer consistency checks skipped - one or both firewalls not ready
    [SKIP] VLAN peer consistency checks skipped - one or both firewalls not ready
================================================================================================
HIGH-AVAILABILITY CONSISTENCY CHECK COMPLETED - ALL CHECKS PASSED
================================================================================================
```

ステップ 5 ネットワーク接続のトラブルシューティング ツールを実行して、ピアの Hypershield Agent へのネットワーク接続の問題を検出します。

例：

```
switch# service system hypershield test high-availability
==============================
Running HA config checks
==============================
Using loopback 1 as the HA source-interface.
1 HA peers configured.
HA admin state is enabled.
================================================
Running HA operational checks
================================================
local svc is not fully functional : criteria not met: in_service
Hypershield peer 192.1.1.1 not functional: print peer HA svc state reason.
================================================
Starting network connectivity checks for the peers
================================================
Using curl to check connection to 192.1.1.1 port 28416
curl: (1) Received HTTP/0.9 when not allowed
Curl successfully connected to 192.1.1.1:28416. Collect 'show tech service-acceleration' to debug
any agent connectivity failure
HA network connectivity check completed for peer with IP 192.1.1.1
```

両方のピアが非サービス モードです

両方のピアが vPC の インサービス トラフィックなし であり、ブリッジド トラフィックが両方の vPC ピアでオフになっている場合、レイヤ 3 またはレイヤ 2ファイアウォールVLAN である VLAN を伝送する vPC は一時停止されません。

VRFは両方のピアで分離された状態のままになります。詳細については、「ファイアウォールの立ち上げ前のネットワーク構成 （15 ページ）」を参照してください。

VRF または VLAN 宛のトラフィックはすべてドロップされます。詳細については、「ファイアウォールの立ち上げ前のネットワーク構成 （15 ページ）」を参照してください。

（注） ファイアウォールが稼働していない場合、DPUのキープアライブと同期は無効になります。現時点では、Hypershield Agent のみが HA 接続を確立します。

手順

ステップ 1 両方のピアは、ローカルの状態をnot-readyと報告し、ピアサービスの状態をnot-readyとして報告する必要があります。ピアの HA 状態が両側で使用できない。

例：

```
switch(config)# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.1)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: not-ready   --> local service is not ready
    Agent HA Status: unavailable
    Peers:
      PeerIP              Peer Service State  HA State with Peer  Reason
      ------------------- ------------------  ------------------  --------------
      192.1.1.2           not-ready           ha-unavailable      local and peer service failure
```

ステップ 2 Hypershield エージェント HA 情報/構成を確認します。

例：

```
switch # service system hypershield connect session /usr/src/app/agwctl ha info
Client got: ok
Data:
=== HA Info ===
Admin State:        enabled
Oper State:         ha-ready
Leader:             false  --> After HA connectivity is established peer with lower IP/ready is
leader
HA IP:              192.1.1.2
HA Port:            28416
Policy Check:
Policy Rev:
Configured Peers:   192.1.1.1
<<snip>>
```

例：

HA ピアでの出力

```
switch(config)# service system hypershield connect session /usr/src/app/agwctl ha info
Client got: ok
Data:
=== HA Info ===
Admin State:        enabled
```

```
Oper State:          ha-ready
Leader:              true     --> After HA connectivity is established peer with lower IP/ready is
leader
HA IP:               192.1.1.1
HA Port:             28416
Policy Check:
Policy Rev:
Configured Peers:    192.1.1.2
<<snip>>
```

一方のピアがインサービス モードであり、もう一方のピアは、インサービス モードでは、ありません

一方のピアが [非インサービス（no in-service）] で、もう一方のピアが [インサービス（in-service）] である場合、トラフィックはインサービスのピアの方向に変更する必要があります。

- Hypershield Agent と NXOS の FW サービスが、 で [インサービス（in-service）] いるピアで準備ができていることを確認します。
- ピア間の状態の可視性を確認します。
- FW準備ができているピアでVPCおよびブリッジドトラフィックの変更がオフになっていることを確認します。
- VRF が分離されなくなり、トラフィックが FW 対応のピアの DPU にリダイレクトできることを確認します。詳細については、「パケット転送 （25 ページ）」を参照してください。
- FW の準備ができていないピアで、vPC およびブリッジド トラフィックの変更が有効になっていることを確認します。
- DPU キープアライブと同期は、インサービスではないピアでは引き続き無効です。

手順

ステップ 1 HA 状態を検証します。

例：

準備ができていないピアでの出力

```
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.1)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: not-ready
    Agent HA Status: unavailable
    Peers:
      PeerIP         Peer Service State  HA State with Peer  Reason
      -------------- ------------------  ------------------  --------------
      192.1.1.2      ready               ha-unavailable      local service failure
```

例：

準備ができているピアでの出力

```
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.2)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: ready
    Agent HA Status: not-ready
    Peers:
      PeerIP         Peer Service State  HA State with Peer  Reason
      -------------- ------------------  ------------------  --------------
      192.1.1.1      not-ready           ha-unavailable      peer service failure
```

サービス中のピアは、ローカル状態を Ready と報告し、リモート状態を not-ready と報告します。同様に、インサービスではないピアは、ローカル状態を not-ready 、リモート状態を Ready と報告します。

オンボーディングされたピアで HA 状態が準備されておらず、他のピアで使用できません。

ステップ 2 各ピアでHA整合性チェッカーを実行し、NX構成およびエージェント駆動状態で状態を検証し、トラフィックの偏差の予想値を検証します。

例：

準備ができていないピアでの出力

```
switch# show consistency-checker service-acceleration high-availability
=======================================================
PROCESSING HIGH-AVAILABILITY CONSISTENCY CHECK REQUEST
=======================================================
****************************************
HA FIREWALL STATE CONSISTENCY
****************************************
  [PASS] Firewall configured and internal states match: out-of-service
                  --> HA Peer that is not in-service
  [PASS] Agent's firewall readiness state matches internal readiness state: not-ready
  [PASS] Agent's firewall readiness state matches published readiness state: not-ready
****************************************
FW VLAN OPERATIONAL STATE CONSISTENCY
****************************************
FW L2, L3 VLAN Set Consistency Checks
====================================
  Expected L3 FW VLANs (from VRFs): 656-657,659,755,859
  Expected L2 FW VLANs : 2003,2005
  Expected Combined L2+L3 VLANs: 656-657,659,755,859,2003,2005
  L3 VLAN Comparison:
    [PASS] L3 VLANs match published FW L3 VLANs
  L2 VLAN Comparison:
    [PASS] L2 VLANs match published FW L2 VLANs
  Combined L2+L3 VLAN Comparison:
    [PASS] Combined L2+L3 FW VLANs identified as expected
****************************************
HA PEER CONSISTENCY
****************************************
HA Configuration and Peer State Checks
======================================
  HA Admin State Comparison:
    [PASS] HA admin state matches with internal state: no-shutdown
  HA Source interface Comparison:
    [PASS] HA Source interface matches: loopback1
  HA Source IP Address Comparison:
    [PASS] HA source IP address matches: 192.1.1.1
  HA Peer Configuration Validation:
```

```
    [PASS] Peer 192.1.1.2 found internally.
  HA Peer State Validation:
    [PASS] Internal Peer service state for peer 192.1.1.2 matches service state published by agent:
 ready
    [PASS] Peer 192.1.1.2 derived firewall state matches: 'ready'
HA VPC Peer Consistency Checks
==============================
  Validating HA Peer Info:
  Internal Peer state validation:
    VPC peer is alive
    [PASS] Peer 192.1.1.2 is being detected as an alive VPC peer --> vPC peer is being detected
  VPC Peer Firewall State Validation:
    [PASS] Internally known HA VPC peer firewall state is 'ready' (VPC peer exists)
    [PASS] Published HA VPC peer firewall state is 'ready' (VPC peer exists)
VPC State Consistency Checks
============================
  Validating 4 VPC(s)
  VPC 60 (Po60):
    [Pass] Internal details for VPC 60 matches configuration
    [PASS] VPC 60 is of interest and allows 3 FW l2/l3 VLAN(s): 657,659,2005
    [PASS] VPC 60 state is 'down' (local FW not-ready, peer FW ready)
      State reason: suspended by service-acceleration
  VPC 61 (Po61):
    [Pass] Internal details for VPC 61 matches configuration
    [PASS] VPC 61 is of interest and allows 2 FW l2/l3 VLAN(s): 656,2005
    [PASS] VPC 61 state is 'down' (local FW not-ready, peer FW ready)
      State reason: suspended by service-acceleration
  VPC 62 (Po62):
    [Pass] Internal details for VPC 62 matches configuration
    [PASS] VPC 62 is of interest and allows 2 FW l2/l3 VLAN(s): 755,2003
    [PASS] VPC 62 state is 'down' (local FW not-ready, peer FW ready)
      State reason: suspended by service-acceleration
  VPC 63 (Po63):
    [Pass] Internal details for VPC 63 matches configuration
    [PASS] VPC 63 is of interest and allows 1 FW l2/l3 VLAN(s): 2003
    [PASS] VPC 63 state is 'down' (local FW not-ready, peer FW ready)
      State reason: suspended by service-acceleration
**************************************
HA VRF/VLAN OPERATIONAL STATE CONSISTENCY
**************************************
    [PASS] 2 VRF(s) were validated and are in 'isolated' state
    [PASS] VLANs 2003,2005 were validated and are in 'VLAN set to drop' state
    [SKIP] VRF/VLAN vpc peer consistency checks skipped - one or both firewalls not ready
    [SKIP] VLAN peer consistency checks skipped - one or both firewalls not ready
================================================================================
HIGH-AVAILABILITY CONSISTENCY CHECK COMPLETED - ALL CHECKS PASSED
================================================================================
```

ステップ 3 vPCが、非サービス モードのピアで一時停止されず、インサービス モードのピアで一時停止されないことを確認します。

例：

準備ができていないピアでの出力

```
switch# show vpc brief
<<snip>>
vPC domain id      : 1
Peer status        : peer adjacency formed ok
vPC keep-alive status    : peer is alive
vPC role                          : primary
<<snip>>
vPC Peer-link status
---------------------------------------------------
```

```
id    Port   Status Active vlans
--    ----   ------ --------------------------
1 Po900  up        656-657,659,755,757-
                    759,859,2003,2005,2007,2009
vPC status
----------------------------------------------
Id    Port          Status Consistency Reason               Active vlans
--    ------------  ------ ----------- ------               ---------------
60    Po60          down*  success     success              -

61 Po61             down*  success     success            -
<<snip>>
switch# show interface port-channel 60-61 br
--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                           Speed   Protocol
Interface
--------------------------------------------------------------------------------
Po60         1       eth  trunk  down    suspended by service-acceleration     auto(D)  none
Po61         1       eth  trunk  down    suspended by service-acceleration     auto(D)  none
```

ステップ 4 準備ができていないピアで HSRP グループが INIT 状態のままになっている間、VRF は分離されなくなるため、 HSRP グループが準備ができているピアでアクティブに移行することを確認します。vPC は HSRP active-active を使用するため、準備ができていない HA vPC ピアで vPC が一時停止された結果、 VIP へのトラフィック偏差が発生します。

例：

準備ができていないピアでの出力

```
switch# show hsrp group 656
Vlan656 - Group 656 (HSRP-V2) (IPv4)
  Local state is Initial(VRF Isolation Enabled), priority 110 (Cfged 110), may preempt
    Forwarding threshold(for vPC), lower: 0 upper: 110
  Hellotime 3 sec, holdtime 10 sec
  Virtual IP address is 166.1.1.6 (Cfged)
  Active router is unknown
  Standby router is unknown
  Authentication text "cisco"
  Virtual mac address is 0000.abcd.0656 (Cfged MAC)
  3 state changes, last state change 1d14h
  IP redundancy name is hsrp-Vlan656-656 (default)
```

例：

準備ができているピアでの出力

```
switch# show hsrp group 656
Vlan656 - Group 656 (HSRP-V2) (IPv4)
  Local state is Active, priority 100 (Cfged 100), may preempt
    Forwarding threshold(for vPC), lower: 0 upper: 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 1.394000 sec(s)
  Virtual IP address is 166.1.1.6 (Cfged)
  Active router is local
  Standby router is unknown
  Authentication text "cisco"
  Virtual mac address is 0000.abcd.0656 (Cfged MAC)
  7 state changes, last state change 01:33:43
  IP redundancy name is hsrp-Vlan656-656 (default)
```

ステップ 5 Hypershield エージェント HA 情報/構成を確認します。準備ができているピアが、リーダーの役割を担います。

例：

```
switch# service system hypershield connect session /usr/src/app/agwctl ha info
Client got: ok
Data:
=== HA Info ===
Admin State:        enabled
Oper State:         ha-ready
Leader:             true            --> Role switches to leader since it is "ready"
HA IP:              192.1.1.2
HA Port:            28416
Policy Check:       false
Policy Rev:
Configured Peers:   192.1.1.1

switch# service system hypershield connect session /usr/src/app/agwctl ha info
Client got: ok
Data:
=== HA Info ===
Admin State:        enabled
Oper State:         ha-ready
Leader:             false        --> Role is follower since it is "not-ready"
HA IP:              192.1.1.1
HA Port:            28416
Policy Check:       false
Policy Rev:
Configured Peers:   192.1.1.2
```

両方のピアがインサービス モードです

両方のピアがインサービスモードの場合、両方のピアがFWの準備ができているときに、トラフィックの偏差をオフにする必要があります。

- 各ピアで FW の準備状況を確認します。
- ピア間の状態の可視性を確認します。
- vPC およびブリッジド トラフィック ディフレクションが両方のピアでオフになっていることを確認します(前のセクションを参照)。
- VRF の分離がなくなり、トラフィックが FW 対応のピアの DPU にリダイレクトできることを確認します（「パケット転送 （25 ページ） 」を参照）。
- ピア間のフロー同期を確認します。

手順

ステップ 1 両方のピアがローカルおよびピアの状態を Ready と報告することを確認します。HA 状態は両方のピアで準備完了です。

例：

1 つのピアでの出力

```
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.1)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: ready
    Agent HA Status: ready
    Peers:
      PeerIP         Peer Service State  HA State with Peer  Reason
      -------------- ------------------  ------------------  --------------
      192.1.1.2      ready               ha-ok               all criteria met
```

例：

HA ピアでの出力

```
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.2)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: ready
    Agent HA Status: ready
    Peers:
      PeerIP         Peer Service State  HA State with Peer  Reason
      -------------- ------------------  ------------------  --------------
      192.1.1.1      ready               ha-ok               all criteria met
```

ステップ 2 各ピアで HA 整合性チェッカーを実行し NX 構成、状態を Agent の駆動状態、およびトラフィック ディフレクション想定を検証します。

例：

```
switch# show consistency-checker service-acceleration high-availability
=====================================================
PROCESSING HIGH-AVAILABILITY CONSISTENCY CHECK REQUEST
=====================================================
**************************************
HA FIREWALL STATE CONSISTENCY
**************************************
  [PASS] Firewall configured and internal states match: in-service
  [PASS] Agent's firewall readiness state matches internal readiness state: ready
  [PASS] Agent's firewall readiness state matches published readiness state: ready
**************************************
FW VLAN OPERATIONAL STATE CONSISTENCY
**************************************
FW L2, L3 VLAN Set Consistency Checks
=====================================
  Expected L3 FW VLANs (from VRFs): 656-657,659,755,859
  Expected L2 FW VLANs : 2003,2005
  Expected Combined L2+L3 VLANs: 656-657,659,755,859,2003,2005
  L3 VLAN Comparison:
    [PASS] L3 VLANs match published FW L3 VLANs
  L2 VLAN Comparison:
    [PASS] L2 VLANs match published FW L2 VLANs
  Combined L2+L3 VLAN Comparison:
    [PASS] Combined L2+L3 FW VLANs identified as expected
**************************************
HA PEER CONSISTENCY
**************************************
HA Configuration and Peer State Checks
======================================
  HA Admin State Comparison:
    [PASS] HA admin state matches with internal state: no-shutdown
  HA Source interface Comparison:
    [PASS] HA Source interface matches: loopback1
  HA Source IP Address Comparison:
```

```
    [PASS] HA source IP address matches: 192.1.1.1
  HA Peer Configuration Validation:
    [PASS] Peer 192.1.1.2 found internally.
  HA Peer State Validation:
    [PASS] Internal Peer service state for peer 192.1.1.2 matches service state published by agent:
 ready
    [PASS] Peer 192.1.1.2 derived firewall state matches: 'ready'
HA VPC Peer Consistency Checks
==============================
  Validating HA Peer Info:
  Internal Peer state validation:
    VPC peer is alive
    [PASS] Peer 192.1.1.2 is being detected as an alive VPC peer
  VPC Peer Firewall State Validation:
    [PASS] Internally known HA VPC peer firewall state is 'ready' (VPC peer exists)
    [PASS] Published HA VPC peer firewall state is 'ready' (VPC peer exists)
VPC State Consistency Checks
============================
  Validating 4 VPC(s)
  VPC 60 (Po60):
    [Pass] Internal details for VPC 60 matches configuration
    [PASS] VPC 60 is of interest and allows 3 FW l2/l3 VLAN(s): 657,659,2005
  VPC 61 (Po61):
    [Pass] Internal details for VPC 61 matches configuration
    [PASS] VPC 61 is of interest and allows 2 FW l2/l3 VLAN(s): 656,2005
  VPC 62 (Po62):
    [Pass] Internal details for VPC 62 matches configuration
    [PASS] VPC 62 is of interest and allows 2 FW l2/l3 VLAN(s): 755,2003
  VPC 63 (Po63):
    [Pass] Internal details for VPC 63 matches configuration
    [PASS] VPC 63 is of interest and allows 1 FW l2/l3 VLAN(s): 2003
**************************************
HA VRF/VLAN OPERATIONAL STATE CONSISTENCY
**************************************
    [PASS] 2 VRF(s) were validated and are in 'forwarding ready/redirection installed' state
    [PASS] VLANs 2003,2005 were validated and are in 'forwarding ready' state
    [INFO] Both firewalls are ready - proceeding with VRF and VRF-ID validation
    [PASS] All VRF ID validations passed
    [PASS] All VLAN peer consistency checks passed - 2 VLAN(s) validated
================================================================================================
HIGH-AVAILABILITY CONSISTENCY CHECK COMPLETED - ALL CHECKS PASSED
================================================================================================
```

ステップ 3 FW VRF に使用されるカプセル化 VLAN は、両方のピアで一貫している必要があります。これらに一貫性がない場合は、CC がフラグを設定する必要があります。これらの ID は、2 つのスイッチの DPU で一致している必要があり、**show service-acceleration redirect-policy brief** コマンドを使用して NXOS で表示される値と比較することで確認できます。

例：

```
switch# slot 1 dpu 1 dpctl hs vrf show-map
VRF Table:
VRF Name                          VRF ID     Internal VRF ID
-----------------------------------------------------------
tenant1                           12         4
default                           1          1
tenant2                           13         3
Total VRFs: 3
```

ステップ 4 Hyper レート エージェントの HA 情報/設定を確認します。

例：

リーダーの Hypershield Agent HA ステータスの出力

```
switch# service system hypershield connect session /usr/src/app/agwctl ha show
Client got: ok
Data:
=== HA Status ===
Cluster State:   active/active
NX State:        ha-ready
--- Local ---
  Svc State:         ready since 2026-05-12 20:15:48 UTC
    Reason:          all criteria met
    Criteria:        [OK] since 2026-05-12 20:15:48 UTC
      dpu_healthy:   [OK]
      dpu_insync:    [OK]
      in_service:    [OK]
--- Peer: 192.1.1.1 ---
  HA State:              ha-ok since 2026-05-12 22:35:41 UTC
    Reason:              all criteria met
  Svc State:             ready since 2026-05-12 22:35:40 UTC
    Reason:              peer service ready
    Criteria:            [OK] since 2026-05-12 22:35:40 UTC
      peer_service:      [OK]
  Membership:            [OK] since 2026-05-12 23:52:45 UTC
    peer_compatible:     [OK]
    peer_dpu_keepalive:  [OK]
    peer_vrf_gid:        [OK]
  Adjacency:             [OK] since 2026-05-12 22:35:10 UTC
    peer_dpu_bulk_sync:  [OK]
    peer_policy:         [OK]
```

例：

準備ができているリーダーの Hypershield Agent HA ピア ステータスの出力

```
switch# service system hypershield connect session /usr/src/app/agwctl ha peers show
Client got: ok
Data:
=== HA Peers ===
--- Peer: 192.1.1.1 ---
HA State:        ha-ok since 2026-05-12 22:35:41 UTC
  Reason:        all criteria met
Svc State:       ready since 2026-05-12 22:35:40 UTC
  Reason:        peer service ready
IpConfigState:   success
Connected:       [OK] since 2026-05-12 23:57:40 UTC
Service Criteria Met:   [OK] since 2026-05-12 22:35:40 UTC
  peer_service:         [OK]
Member Criteria Met:    [OK] since 2026-05-12 23:57:44 UTC
  peer_compatible:      [OK]
  peer_dpu_keepalive:   [OK]
  peer_vrf_gid:         [OK]
Adjacency Criteria Met:   [OK] since 2026-05-12 22:35:10 UTC
  peer_dpu_bulk_sync:     [OK]
  peer_policy:            [OK]
Member Info:
  Serial:              FDO28370FGQ
  Model:               N9324C-SE1U
  SW Version:          10.6(3q)ISQ9(0.13)
  CPA Version:         v1.19.0-pre.8-151-g14b22c12
  Reported HA State:   ha-ready
  Service:             ready
  LB Mode:             symmetric-hash
  Policy Rev:
  Policy Check:        false
  DPUs:                dpu2(1.150.2), dpu4(1.150.2), dpu1(1.150.2), dpu3(1.150.2)
```

```
DPU HA Status:
  dpu1:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu2:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu3:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu4:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
```

ステップ 5 準備ができたフォロワーの Hypershield Agent HA ステータスを確認します。

例：

```
switch# service system hypershield connect session /usr/src/app/agwctl ha show
Client got: ok
Data:
=== HA Status ===
Cluster State:   active/active
NX State:        ha-ready
--- Local ---
  Svc State:         ready since 2026-05-12 20:15:48 UTC
    Reason:          all criteria met
    Criteria:        [OK] since 2026-05-12 20:15:48 UTC
      dpu_healthy:   [OK]
      dpu_insync:    [OK]
      in_service:    [OK]
--- Peer: 192.1.1.1 ---
  HA State:              ha-ok since 2026-05-12 22:35:41 UTC
    Reason:              all criteria met
  Svc State:             ready since 2026-05-12 22:35:40 UTC
    Reason:              peer service ready
    Criteria:            [OK] since 2026-05-12 22:35:40 UTC
      peer_service:      [OK]
  Membership:            [OK] since 2026-05-12 23:52:45 UTC
    peer_compatible:     [OK]
    peer_dpu_keepalive:  [OK]
    peer_vrf_gid:        [OK]
  Adjacency:             [OK] since 2026-05-12 22:35:10 UTC
    peer_dpu_bulk_sync:  [OK]
    peer_policy:         [OK]
```

ステップ 6 準備ができているピアの Hypershield Agent HA ピアのステータスを確認します。

例：

```
switch3# service system hypershield connect session /usr/src/app/agwctl ha peers show
Client got: ok
Data:
=== HA Peers ===
--- Peer: 192.1.1.2 ---
HA State:        ha-ok since 2026-05-12 22:35:20 UTC
  Reason:        all criteria met  --> Both peers are ready and sync is completed - HA is ready
Svc State:       ready since 2026-05-12 20:15:28 UTC
  Reason:        peer service ready
IpConfigState:   success
Connected:       [OK] since 2026-05-12 23:55:54 UTC
Service Criteria Met:   [OK] since 2026-05-12 20:15:28 UTC
  peer_service:         [OK]
Member Criteria Met:    [OK] since 2026-05-12 23:55:55 UTC
  peer_compatible:      [OK]
  peer_dpu_keepalive:   [OK]
  peer_vrf_gid:         [OK]
Adjacency Criteria Met:   [OK] since 2026-05-12 22:34:50 UTC
  peer_dpu_bulk_sync:     [OK]
  peer_policy:            [OK]
Member Info:
  Serial:              FDO28370FGZ
  Model:               N9324C-SE1U
```

```
  SW Version:          10.6(3q)ISQ9(0.13)
  CPA Version:         v1.19.0-pre.8-151-g14b22c12
  Reported HA State:   ha-ready
  Service:             ready
  LB Mode:             symmetric-hash
  Policy Rev:
  Policy Check:        false
  DPUs:                dpu2(1.150.2), dpu4(1.150.2), dpu1(1.150.2), dpu3(1.150.2)
DPU HA Status:
  dpu1:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu2:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu3:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
  dpu4:   keepalive=[OK]  bulk_sync_local=[OK]  bulk_sync_peer=[OK]
```

メンバーシップの障害

メンバーシップの障害は、スイッチオーバー/テイクオーバー シナリオをトリガー可能性があり、結果として、DPUキープアライブの障害、バージョンとプラットフォームの不一致、負荷分散モードの不一致が発生する可能性があります。

両方のスイッチがFW レディの場合、リーダーがトラフィックを引き継ぎ、フォロワーは 準備ができていないに移行します。

トラフィック回避メカニズムは、 インサービス 中にファイアウォールが 準備ができていないに移行すると有効になります。

手順

ステップ 1 リーダーとして選択されたピアがトラフィックを引き継ぎ、フォロワーはローカル状態を準備ができていないとして移行します。

例：

```
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.1)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: not-ready     --> not ready
    Agent HA Status: switchover                      --> switched to peer
    Peers:
      PeerIP              Peer Service State  HA State with Peer  Reason
      ------------------- ------------------  ------------------  --------------
     192.1.1.2          ready               ha-fail            membership failure: peer_compatible
switch# show service-acceleration high-availability status
  Service System: hypershield
    HA Source Interface: loopback1 (192.1.1.2)
    HA Admin State: no-shutdown
    Agent Status for Service Firewall: ready     --> ready
    Agent HA Status: takeover                    --> takes over from peer
    Peers:
      PeerIP              Peer Service State  HA State with Peer  Reason
      ------------------- ------------------  ------------------  --------------
     192.1.1.1          not-ready          ha-fail            membership failure: peer_compatible
```

ステップ 2 このコマンドを使用して、互換性障害の原因を特定します。

例：

```
switch# service system hypershield connect session /usr/src/app/agwctl ha compatibility
Client got: ok
Data:
=== HA Compatibility ===
--- Peer: 192.1.1.1 ---
Membership:
Field          Local                          Peer                           Status
model          N9324C-SE1U                    N9324C-SE1U                    [OK]
nxos_version   10.6(3q)ISQ9(0.13)              10.6(3q)ISQ9(0.13)             [OK]
cpa_version    v1.19.0-pre.8-151-g14b22c12    v1.19.0-pre.8-151-g14b22c12    [OK]
dpu_count      4                              4                              [OK]
lb_mode        symmetric-hash                 pinning                        [FAIL]
policy_check   false                          false                          [OK]
dpu:dpu1       1.150.2                        1.150.2                        [OK]
dpu:dpu2       1.150.2                        1.150.2                        [OK]
dpu:dpu3       1.150.2                        1.150.2                        [OK]
dpu:dpu4       1.150.2                        1.150.2                        [OK]
Verdict: [FAIL]
Adjacency:
Field             Local   Peer   Status
policy_revision                  [OK]
Verdict: [OK]
```

ステップ 3 VRF がリダイレクション *インストール済み* または *隔離* 状態に移行し、VRF 分離が有効になることを確認します。vPC トラフィック偏差も有効になります。

例：

```
switch# show service-acceleration status details
  Service System: hypershield
    Source Interface: loopback2 (10.29.251.101)
    DPU Load-balance Mode: pinning
    Agent Status: firewall-ready,redirect-installed
    Agent Health Status: ok
    Controller Connection Status: init
    Agent HA Status: switchover
    Services:
      Firewall: in-service
      VRF                              Operational State       Affinity(DPU)
      ================================================================================
      tenant1                          redirection installed   1
      tenant2                          redirection installed   2
      VLAN                             Operational State       Affinity(DPU)
      ================================================================================
      2003                             forwarding ready        1
      2005                             forwarding ready        3
```

ステップ 4 スイッチオーバーまたはテイクオーバー時に Hypershield Agent の HA ステータスを確認します。

例：

```
switch# service system hypershield connect session /usr/src/app/agwctl ha show
Client got: ok
Data:
=== HA Status ===
Cluster State:   active/standby (degraded)
NX State:        ha-takeover
--- Local ---
  Svc State:         ready since 2026-05-12 20:15:48 UTC
    Reason:          all criteria met
```

```
    Criteria:        [OK] since 2026-05-12 20:15:48 UTC
      dpu_healthy:   [OK]
      dpu_insync:    [OK]
      in_service:    [OK]
--- Peer: 192.1.1.1 ---
  HA State:               ha-fail since 2026-05-13 00:30:34 UTC
    Reason:               membership failure: peer_compatible
  Svc State:              not-ready since 2026-05-13 00:30:17 UTC
    Reason:               peer service not-ready
    Criteria:             [FAIL] since 2026-05-13 00:30:17 UTC
      peer_service:       [FAIL]
  Membership:             [FAIL] since 2026-05-13 00:30:20 UTC
    peer_compatible:      [FAIL]
    peer_dpu_keepalive:   [OK]
    peer_vrf_gid:         [OK]
  Adjacency:              [FAIL] since 2026-05-13 00:30:24 UTC
    peer_dpu_bulk_sync:   [FAIL]
    peer_policy:          [OK]
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。