Cisco Nexus 9000 シリーズ NX-OS Intelligent Traffic Director 構成ガイド、リリース 10.4(x)

初版：2023 年 8 月 18 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。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

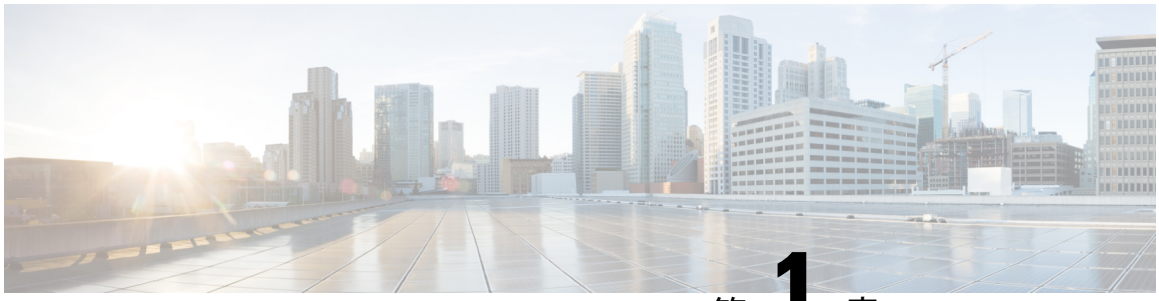
このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



第 1 章

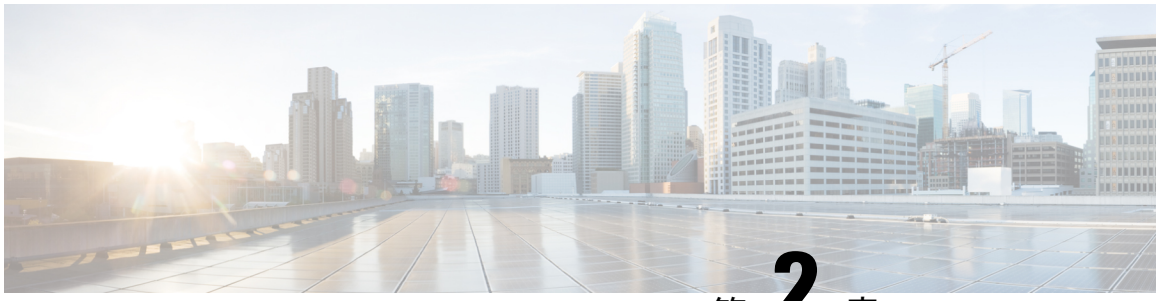
新機能と更新情報

新機能と更新情報

次の表は、『*Cisco Nexus 9000* シリーズ *NX-OS Intelligent Traffic Director* 構成ガイド リリース *10.4(x)*』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

特長	説明	変更が行われたリリース	参照先
トンネルインターフェイスのサポート	ITD はトンネル インターフェイスをサポートします。	10.4(1)F	ITD の注意事項と制約事項 （33 ページ）
トンネルを介したノードへのロードバランシング/リダイレクションのサポート	ITD は、トンネルインターフェイスを介して到達可能なレイヤ 3 ノードへのリダイレクションまたはロードバランシングをサポートします。	10.4(1)F	ITD の注意事項と制約事項 （33 ページ）
ACL でのポート演算子のサポート	ITD サービスは、包括 ACL のレイヤ 4 ポートオペレータをサポートします。	10.4(1)F	ITD の注意事項と制約事項 （33 ページ）

新機能と更新情報



第 2 章

ITD の構成

この章では、Cisco NX-OS デバイスで Intelligent Traffic Director（ITD）を構成する方法について説明します。

ITDについて

Intelligent Traffic Director（ITD）は、レイヤ 3 およびレイヤ 4 のトラフィック分散、ロードバランシング、およびリダイレクトのためのスケーラブルなアーキテクチャを構築できる、インテリジェントなハードウェア ベースのマルチテラビット ソリューションです。

ITD のメリット：

- ライン レートでのマルチテラビット ソリューション
- エンドデバイスへの透過性とステートレス プロトコルのメリット
- Web Cache Communication Protocol（WCCP）やポリシーベースのルーティングなどの代替機能のための複雑さとアーキテクチャのスケーリングの軽減
- プロビジョニングが簡素化され導入が容易
- レガシー サービス アプライアンスは新しいものと共存できます
- 高価な外部ロードバランサの要件を削除します。
- デバイスと Cisco NX-OS スイッチ間の認証 / 統合 / 認定が不要。
- 大幅な OPEX 削減の順序：構成の簡素化、展開の容易さ

- サービス モジュールまたは外部 L4 ロードバランサは不要すべての Nexus ポートをロードバランサとして使用可能

ITD の機能：

- ワイヤスピードでのハードウェアベースのマルチテラビット / 秒 L3 / L4 ロードバランシング
- ゼロ遅延のロードバランシング
- ラインレート トラフィックを任意のデバイスにリダイレクト、たとえば web cache エンジン、Web アクセラレータ エンジン（WAE）、ビデオキャッシュ、など）
- ファイアウォール、侵入防御システム（IPS）、または Web アプリケーション ファイアウォール（WAF）、Hadoop クラスタなどのデバイスのクラスタを作成する機能
- IP スティッキネス
- ワイヤスピードでのハードウェアベースのマルチテラビット / 秒 L3 / L4 ロードバランシング
- ゼロ遅延のロードバランシング
- ラインレート トラフィックを任意のデバイスにリダイレクト、たとえば web cache エンジン、Web アクセラレータ エンジン（WAE）、ビデオキャッシュ、など）
- ファイアウォール、侵入防御システム（IPS）、または Web アプリケーション ファイアウォール（WAF）、Hadoop クラスタなどのデバイスのクラスタを作成する機能
- IP スティッキネス
- 回復力（回復力のある ECMP など）、一貫したハッシュ
- 仮想 IP ベースの L4 ロードバランシング
- ノード間で加重負荷分散と Failaction がサポートされています
- 多数のデバイス / サーバーへの負荷分散
- リダイレクトおよびロードバランシングと同時の ACL
- 双方向のフロー一貫性。A–>B および B–>A からのトラフィックは同じノードに行きます
- サーバ/アプライアンスを Nexus スイッチに直接接続する必要なし
- IP SLA ベースのプローブを使用したサーバー / アプライアンスのヘルスの監視
- N + M 冗長（N ノード数、M ホットスタンバイ数）
- サーバー / アプライアンスの自動障害処理
- VRF サポート、vPC サポート
- デフォルトまたはデフォルト以外の VRF での入力インターフェイスと出力インターフェイスの両方のサポート。

（注） ITD NAT VRF 構成については、『**Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド**』の「*[IP ACL* の構成」セクションを参照してください。

- NAT GX スケールは、2K NAT 変換をサポートするために 2048 エントリをサポートしています。
- IPv4 と IPv6 の両方をサポート（すべてのプラットフォームは IPv6 をサポートしていません）
- ITD 機能によるスーパーバイザ CPU への負荷の追加なし
- 無制限のフロー数を処理。
- 無停止でのノードの追加または削除
- 同時リダイレクトと負荷分散
- 同じスイッチ内の複数の ITD サービス間でのレート共有

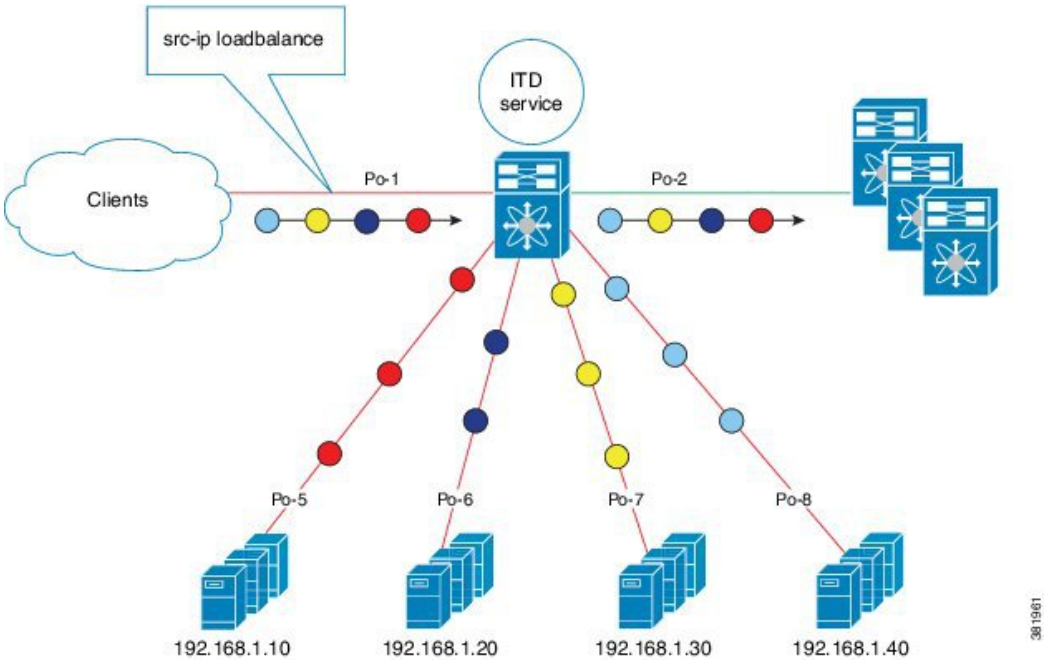
使用例：

- ファイアウォールのクラスタへの負荷分散。
- NX-OS デバイスへのロードバランシングにより、IPS、IDS、および WAF を拡張します。
- 低コストの VM / コンテナ ベースの NFV にロードバランシングすることにより、NFV ソリューションを拡張します。
- WAAS / WAE ソリューションをスケーリングします。Wide Area Application Services（WAAS）または Web Accelerator Engine（WAE）ソリューションのトラフィック リダイレクト メカニズム
- VDS-TC（ビデオ キャッシュ）ソリューションのスケーリング
- トラフィックを L7 LB に分散することにより、レイヤ 7 ロードバランサーをスケーリングします。
- ECMP またはポートチャネルを置き換えて、再ハッシュを回避します。ITD は復元力があり、ノードの追加 / 削除 / 失敗時に再ハッシュを引き起こしません
- DSR（Direct Server Return）モードでのサーバー負荷分散
- NX-OS デバイスへのロードバランシングにより、NG 侵入防御システム（IPS）と Web アプリケーション ファイアウォール（WAF）をスケールアップします。
- レイヤ 5 からレイヤ 7 のロードバランサへの負荷分散

ワンアーム展開モード

ワンアーム展開モードでサーバーをスイッチに接続できます。このトポロジでは、サーバーはクライアント トラフィックまたはサーバー トラフィックの直接パスに存在しないため、既存のトポロジやネットワークを変更することなく、サーバーをネットワークに接続できます。

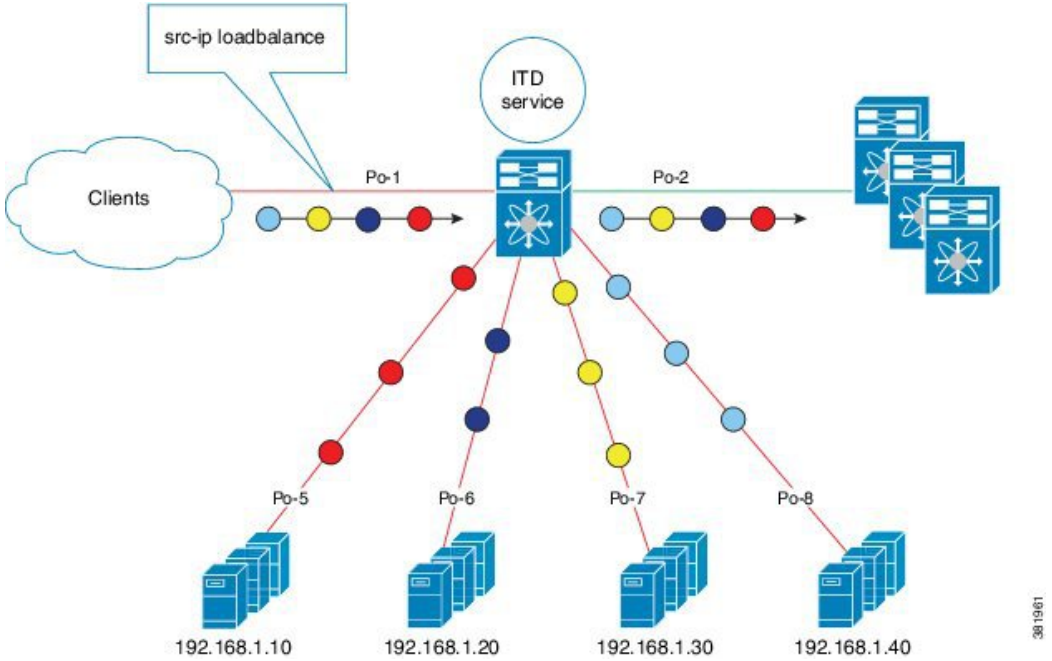
図 *1*: ワンアーム展開モード



ワンアーム展開モード

ワンアーム展開モードでサーバーをスイッチに接続できます。このトポロジでは、サーバーはクライアント トラフィックまたはサーバー トラフィックの直接パスに存在しないため、既存のトポロジやネットワークを変更することなく、サーバーをネットワークに接続できます。

図 *2:* ワンアーム展開モード

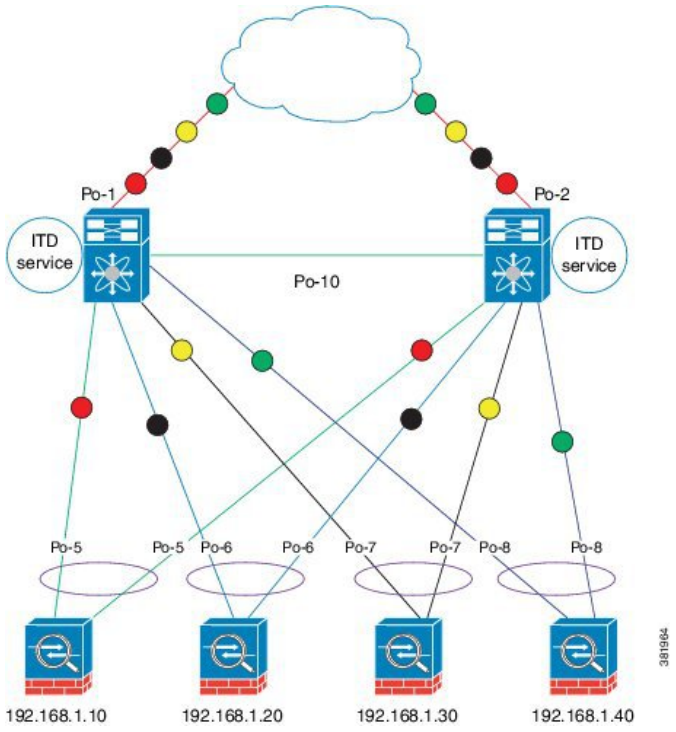


vPC でのワンアーム展開モード

ITD は、仮想ポートチャネル（vPC）に接続されたアプライアンスプールをサポートします。ITD サービスは各スイッチで実行されます。ITD は、フローがノードを通過する一貫したトラフィックを得られるように各スイッチをプログラムします。

（注） VPC シナリオ（ITD NAT を使用しない）に failaction バケット配布を使用して、VPC 経由で到達可能なノードの障害時にピア間で一貫した動作を維持することをお勧めします。

図 *3 : vPC* でのワンアーム展開モード



サンドイッチ展開モード

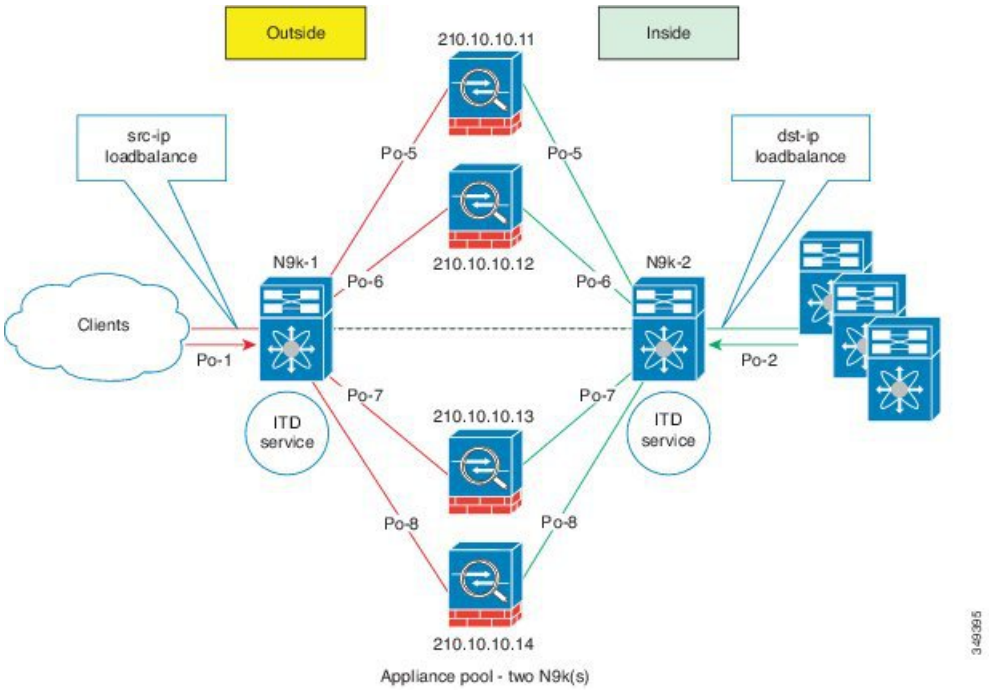
サンドイッチ展開モードでは、2 台のスイッチを使用してトラフィックをステートフルに処理します。

このモードの主な要件は、フローの転送トラフィックとリバーストラフィックの両方が同じアプライアンスを通過しなければならないことです。サンドイッチ展開の例としては、クライアントとサーバ間のトラフィックが同じアプライアンスを通過する必要があるファイアウォールおよびロード バランサの展開があります。

主な機能は次のとおりです。

- ネットワーク セグメントごとの ITD サービス（外部ネットワーク用に 1 つの ITD サービスおよび内部ネットワーク用にもう 1 つの ITD サービス）。
- 入力方向の外部に接続するインターフェイス上で ITD サービスが動作するソース IP アドレス ロードバランシング スキーム。
- 入力方向のサーバーに接続するインターフェイスで ITD サービスが動作する宛先 IP アドレスのロード バランシング スキーム。
- ユーザー定義のアクセス リスト（ACL を含む）が外部ネットワークの ITD サービスで使用されている場合、逆の ACE ルールを持つアクセス リストを作成し、内部ネットワークの ITD サービスのユーザー ACL として適用する必要があります。

図 *4 :* サンドイッチ展開モード

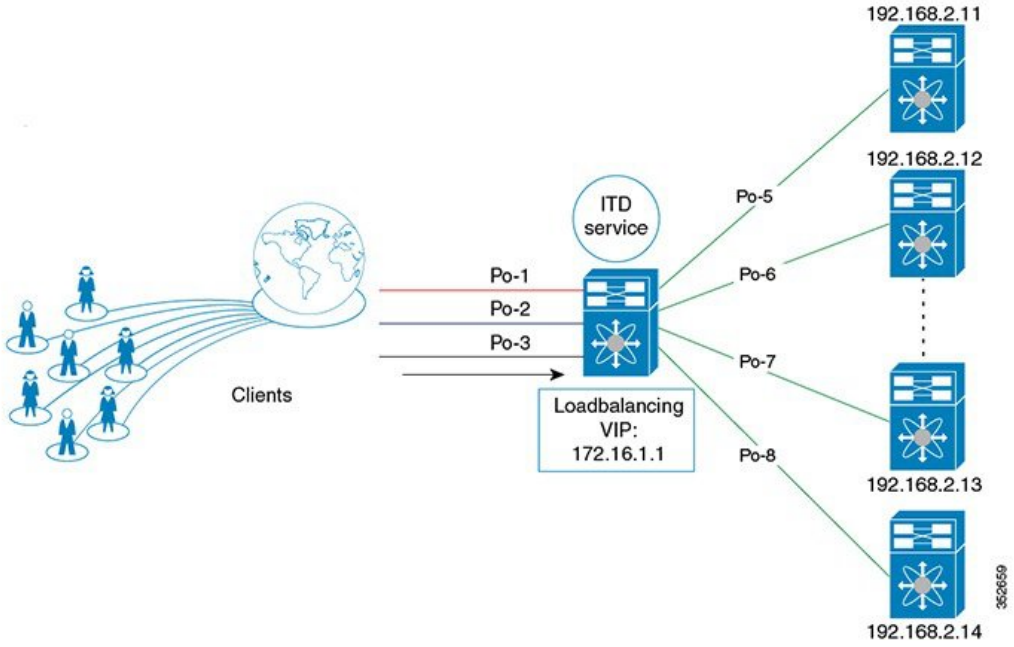


サーバー ロードバランシング展開モード

ITD サービスは、スイッチで仮想 IP（VIP）をホストするように構成できます。VIP を宛先とするインターネットトラフィックの負荷は、複数のアクティブなノードに分散されます。ITD サービスはステートフル ロードバランサではありません。

（注） 各スイッチで同様の方法で、ITD サービスを手動で設定する必要があります。

図 *5 : VIP* を使用した *ITD* 負荷分散



宛先 NAT

ネットワークアドレス変換（NAT）は、ロードバランシング、ファイアウォール、およびサービス アプライアンスで一般的に導入されている機能です。接続先 NAT は、ロードバランシングで使用される NAT のタイプの 1 つです。

接続先 NAT のメリット

ITD 展開で NAT を使用するメリットは次のとおりです。

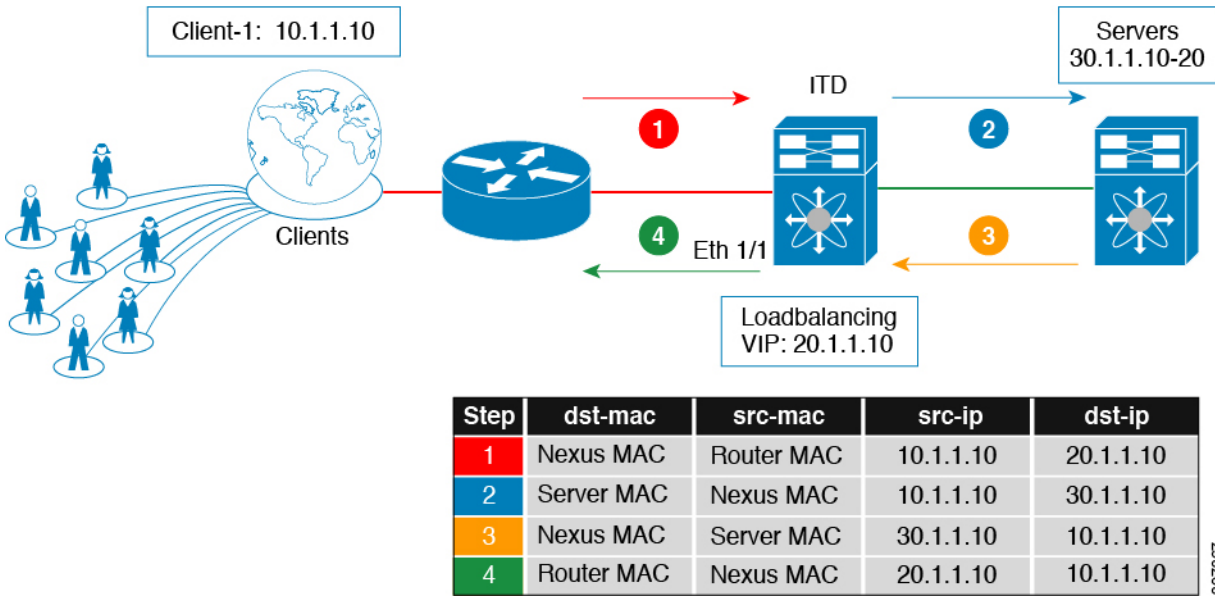
- DSR（Direct Server Return）モードの展開のように、サーバー プール内のすべてのサーバーが仮想 IP アドレスをホストする必要はありません。
- サーバー IP を認識する必要がないクライアントは、常にトラフィックを仮想 IP アドレスに送信します。
- ロードバランサはサーバーの障害を検出し、クライアントがプライマリサーバーのステータスを認識しなくても、トラフィックを適切なサーバーにリダイレクトします。
- NAT は、クライアントから実サーバーの IP を隠すことでセキュリティを提供します。
- NAT により、異なるサーバープール間で実サーバーを移動する際の柔軟性が向上します。

さまざまなタイプの NAT の中で、接続先 NAT は、次のメリットがあるため、負荷分散で一般的に展開されます。

- 送信元またはクライアントから仮想 IP アドレスへのトラフィックは書き換えられ、サーバーにリダイレクトされます。
- 送信先またはクライアントから宛先またはサーバーへのトラフィック（転送パス）は、次のように処理されます。送信先またはクライアントから仮想 IP アドレスへのトラフィックは、ソースから接続先またはサーバーへのトラフィックとして変換およびリダイレクトされます。
- 接続先から送信元またはクライアントへのトラフィック（リバース パス）は、仮想 IP アドレスを送信元 IP アドレスとして再変換されます。

次の図は、仮想 IP アドレスを使用した NAT を示しています。

図 *6*：仮想 *IP* アドレスによる *NAT*



Step	dst-mac	src-mac	src-ip	dst-ip
1	Nexus MAC	Router MAC	10.1.1.10	20.1.1.10
2	Server MAC	Nexus MAC	10.1.1.10	30.1.1.10
3	Nexus MAC	Server MAC	30.1.1.10	10.1.1.10
4	Router MAC	Nexus MAC	20.1.1.10	10.1.1.10

ポート アドレス変換（PAT）

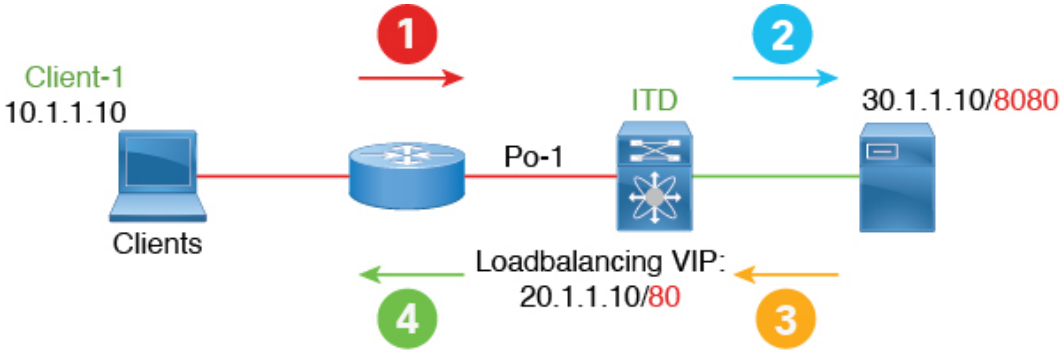
PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピング ポートに使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。PAT では単一のマッピング先のアドレスを使用するため、ルーティング可能なアドレスの使用を抑えることができます。

接続先 NAT および PAT

- ITD はレイヤ 3 / レイヤ 4 のロードバランシングを提供します

- NAT によるライン レート ロードバランシングがサポートされています。
- NAT と PAT の両方がサポートされています。
- 実サーバー IP をクライアントから隠すことにより、サーバー IP とネットワークを保護します。
- NAT と PAT は、Nexus 9000 プラットフォームでサポートされています。

図 *7:* 仮想 *IP* アドレスを使用した *NAT* および *PAT*



Step	dst-mac	src-mac	scr-ip	dst-ip
Step 1	Nexus MAC	Router MAC	10.1.1.10	20.1.1.10:80
Step 2	Server MAC	Nexus MAC	10.1.1.10	30.1.1.10:8080
Step 3	Nexus MAC	Server MAC	30.1.1.10:8080	10.1.1.10
Step 4	Router MAC	Nexus MAC	20.1.1.10:80	10.1.1.10

504063

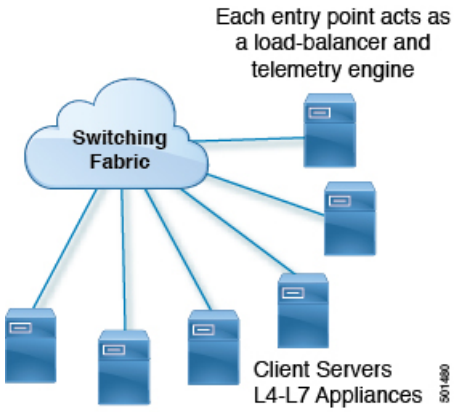
VXLAN 上の ITD

単一のスイッチ ソリューションであった ITD は、VxLAN ファブリックのロードバランサーとして機能するようになりました。

プログラム可能なファブリックでは、サーバー、仮想マシン（VM）、およびコンテナー（特定のサービスに固有）をファブリック全体に分散させ、さまざまな ToR またはリーフスイッチに接続できます。ITD Over VXLAN 機能により、ファブリック全体に分散されたサーバーへのロードバランシングが可能になります。

ITD Over VXLAN により、ファブリックは大規模なロードバランサーとして機能し、大規模なテレメトリと分析を提供できるようになります。ITD Over VXLAN をロードバランサとして使用すると、ファブリック内の任意の場所にあるレイヤ 4 アプライアンスとレイヤ 7 アプライアンス間を接続できます。これは、図「ファブリック全体のロードバランシング」に示されています。

図 *8 :* ファブリック全体のロードバランシング



データベース サーバー、アプリケーションサーバー、Web サーバー、ファイアウォール、WAAS、IPS、IDS、およびビデオキャッシュを含む多数のクライアント（ローカルおよびボーダーリーフを越えて）がある場合があります。トラフィックの高低に関する情報を含む、ファブリック内の各デバイスから各ファイアウォール、WAAS、IPS、IDS、およびサーバーに流れるトラフィックに関する情報は非常に貴重です。

ITD Over VXLAN は、クライアントとサーバーまたはレイヤ 4 およびレイヤ 7 サービス間のパス上にあり、トラフィック情報を認識します。この情報を使用して、貴重なトラフィック分析とテレメトリを提供します。

ロードバランシング機能では、仮想 IP（VIP）が、DC ファブリック全体に分散された物理サーバーファームによって提供されるサービスを抽象化します。さまざまなクライアント（ローカルからファブリックへ、またはリモート ロケーションから）が特定のサービスの要求を送信すると、これらの要求は常にこれらのサーバーの VIP に送信されます。

ToR またはリーフスイッチでは、ITD は送信元 IP アドレスのビットとマスク、宛先 IP アドレス（仮想 IP アドレス）、および関連するレイヤ 3 またはレイヤ 4 フィールドを照合して、これらの要求をサーバー間で負荷分散します。

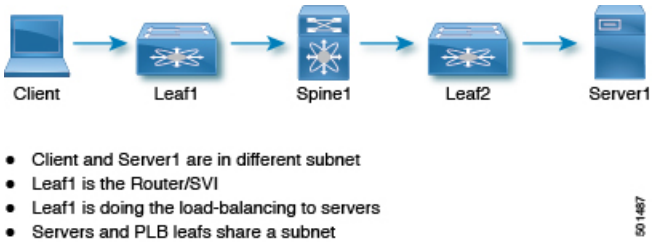
ITD Over VXLAN は、デバイス グループ内のサーバー（ノード）のクラスタを構成するためのインフラストラクチャを提供します。バケット（ビット マスク）に基づいてクライアント トラフィックと ITD サービスで構成されたテナント SVI を分離します。ノード（サーバー）とバケットの定義済みクラスタに基づいて、ITD は、クライアント IP トラフィックをバケット マスクに一致させるルールを自動的に作成し、一致したトラフィックを特定のサーバー ノードにリダイレクトします。

サーバーが応答しなくなった場合や動作不能になった場合、ITD はクライアント トラフィックを非動作ノードから単一または構成済みのスタンバイ ノードのグループに自動的に切り替えます。トラフィックの割り当ては、フローをスタンバイ ノードに自動的に変更することによって実現されます。

ITD Over VXLAN は現在、Direct Server Return（DSR）の概念と機能を使用しているため、サーバーの応答がクライアントに直接送信されます。これはファブリックに依存しませんが、現在 VXLAN EVPN ファブリックでサポートされており、VXLAN 経由の PBR をサポートする Cisco Nexus 9000 シリーズ スイッチで現在サポートされています。

ITD Over VXLAN は、ライン レートの速度で実現されます。

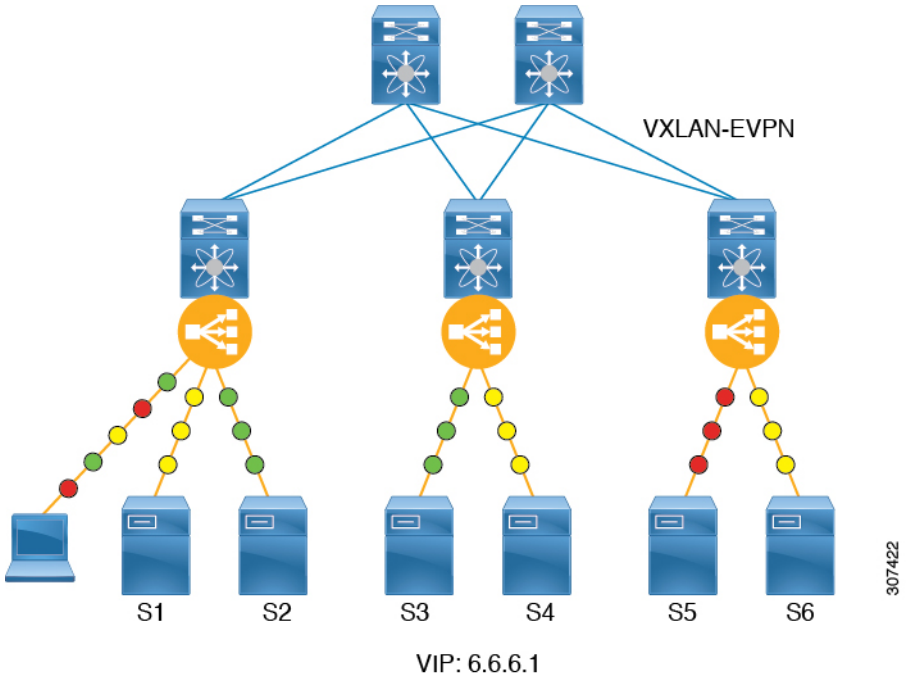
図 *9 : Direct Server Return*



VXLAN トポロジを介した ITD の設定の概要

ToR スイッチでの VXLAN 経由の ITD 設定の概要は次のとおりです。

- 負荷分散サーバーを特定し、デバイス グループを作成します。
- グループの ITD サービス インスタンスを作成し、以下を完了します。
  - 着信する ITD Over VXLAN トラフィックに仮想 IP アドレス（VIP）を関連付けます。VIP は、デバイス グループ内のサーバーを表します。
  - 他の負荷分散構成を有効にします。
  - サービスをアクティブにする必要があるインターフェイスを、サービスの入力インターフェイスとして構成します。ITD サービスをイネーブルにします。
  - サーバー（ITD ノード）が接続されているすべてのリーフスイッチに同一の ITD 設定を適用します。これらのリーフスイッチで、このサービスの入力インターフェイスとして L3 VNI を設定します。ITD サービスをイネーブルにします。



VXLAN 上での ITD のメリット

- ファブリック内の任意の場所に分散されたサーバー / VM / コンテナの負荷分散
- ハードウェアに依存しない
- 直接接続されたノードのデータプレーン内のノードのヘルスモニタリングとプローブの要約。
- 分析とテレメトリは、サーバー（つまり、VM / コンテナの生成）およびアプライアンス（エラスティック データセンター）の容量をいつ / どのように拡大するかについての詳細を提供します。
- エラスティック データセンターを構築します。
- VXLAN ネットワーク識別子（VNI）インターフェイス間の負荷分散。
- ファブリック内の複数のスイッチ間でのロードバランシングの同期。
- 障害情報の自動同期。
- 推奨システム
- 可能なすべてのデータセントートポロジーを備えたVXLAN-EVPNファブリックで動作します。

レイヤ 2 ロードバランシングについて

レイヤ 2（ITD-L2）ロードバランシングは、Cisco Nexus スイッチでのレイヤ 2 トラフィック分散、ロードバランシング、およびリダイレクトのためのハードウェア ベースのマルチテラビット ソリューションです。

（注） ITD-L2 機能は、Cisco 9500 EX/FX ラインカードではサポートされていません。

ITD-L2 は、単一の論理リンクを作成する複数の物理リンクの集合体です。複数の物理リンクをポート グループにバンドルして、帯域幅（複数の物理リンクの集合体）と冗長性を向上させることができます。

レイヤ 2 内の 1 つのポートに障害が発生すると、トラフィックはレイヤ 2 の残りのポートに切り替わります。

ITD-L2 を使用すると、透過モード アプライアンスのクラスタを作成できます。

レイヤ 2 ロード バランシング機能

ITD-L2 の機能は次のとおりです。

- ライン レートでのマルチテラビット ソリューション
- プロビジョニングが簡素化され導入が容易
- エンドデバイスへの透過性とステートレス プロトコルのメリット
- 高価な外部ロードバランサの要件を削除します。

ITD レイヤ 2 ロードバランシングのメリット

ITD レイヤ 2 ロードバランシングのメリットは次のとおりです。

- 同時リダイレクトおよびロードバランシング
- IP スティッキ性および復元力
- ポートのヘルス モニタリング
- 高価な外部ロードバランサの要件を削除します。
- ハッシングは、配線やポートの番号付けに依存しません
- スイッチのすべてのポートは、負荷分散とトラフィックのリダイレクトに使用されます

展開使用例

ITD-L2 機能の展開使用の例は次のとおりです。

- ファイアウォールのプールへの負荷分散。

- VDS-TC（ビデオ キャッシュ）ソリューションをスケーリングします。
- トランスペアレント モードのデバイスをスケーリングします。

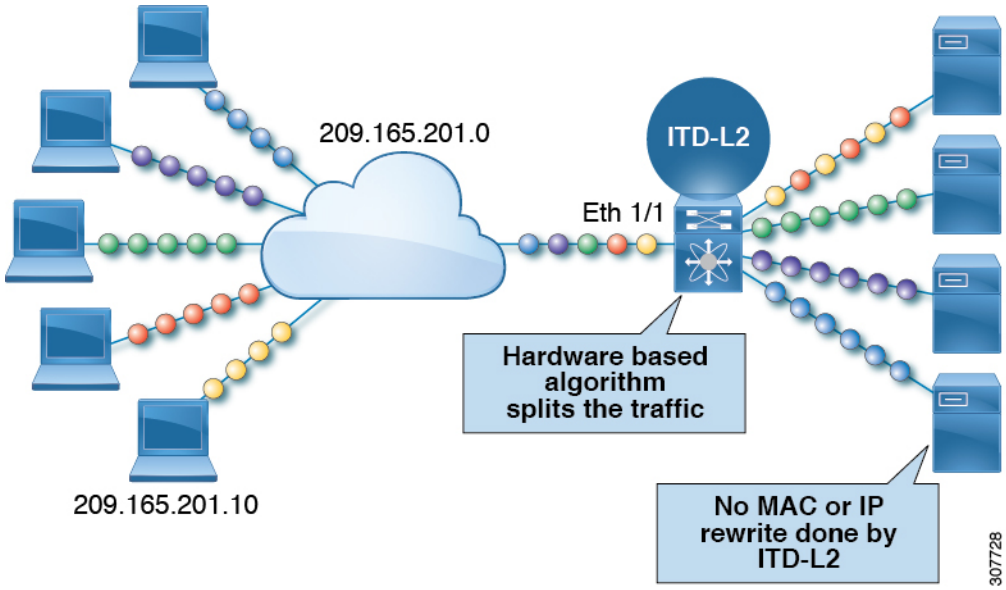
ITD-L2 のトポロジの例

このセクションには、次の例が表示されます。

- ITD-L2 の基本トポロジ
- ITD-L2 構成の使用例
- 回復力のあるハッシュの失敗アクション

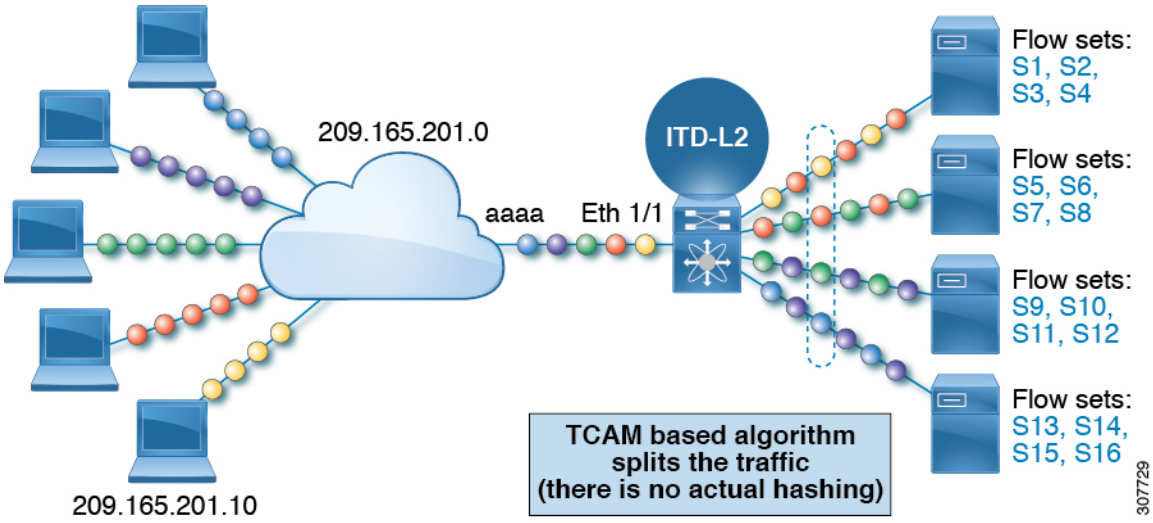
ITD-L2 機能を使用して、監視ネットワークで使用されるアプライアンスへのトラフィックを負荷分散できます。次の図は、IPS や IDS デバイスなどのトラフィックを負荷分散する必要があるアプライアンスにトラフィックが送信される基本的なトポロジを示しています。

図 *10*：レイヤ *2* ロード バランシングの標準トポロジ



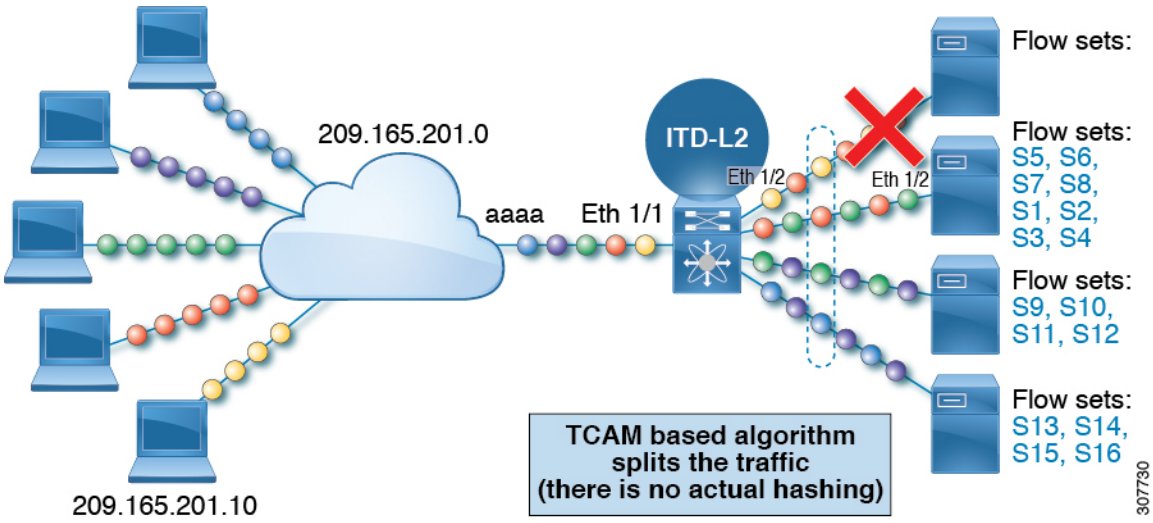
次の例は、トラフィックが本番環境から監視環境に及ぶネットワークでの ITD-L2 の一般的な使用例を示しています。この例では、Cisco Nexus Data Broker を使用して、監視トラフィックのコピーを送信し、監視ネットワークをスケーリングしています。

図 *11 :* レイヤ *2* ロード バランシング構成の使用例



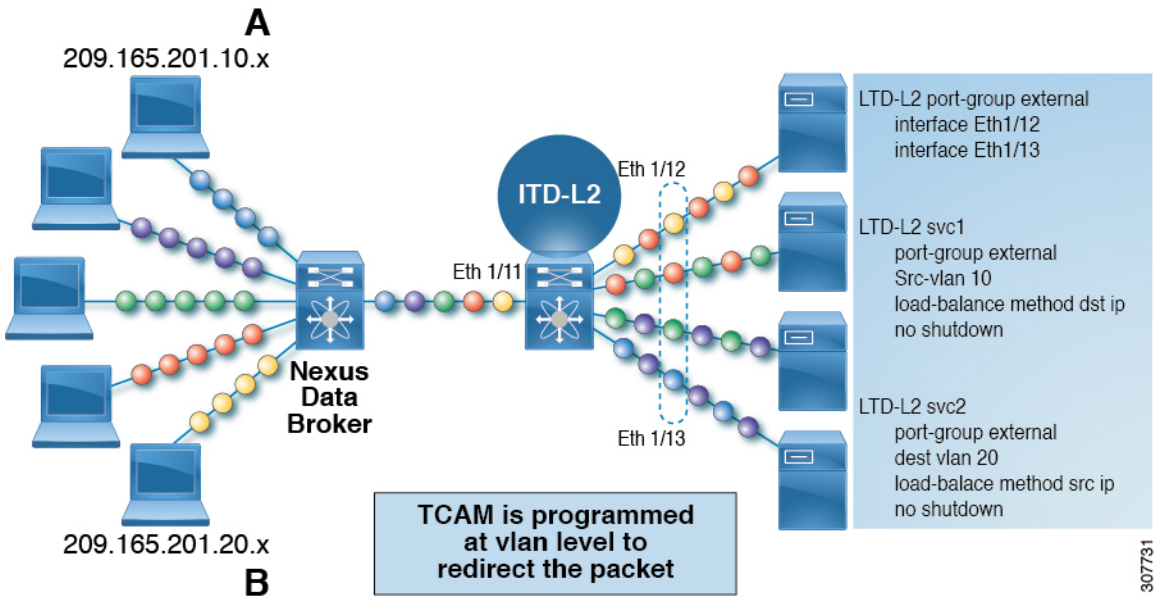
次の例は、ITD-L2 構成の失敗アクションを示しています。

図 *12 : ITD-L2* 構成の *Fail-Action*



次の例は、弾力性のあるハッシュを使用した ITD-L2 構成の失敗アクションを示しています。

図 *13* : 回復力のあるハッシュを使用した *ITD-L2* 構成の失敗アクション



レイヤ 2 ロードバランシングの前提条件

レイヤ 2 ロードバランシングには、次の前提条件があります。

- 十分な TCAM サイズが VACL に割り当てられていることを確認する必要があります。TCAM サイズを確認するには、 **sh hardware access-list tcam region** コマンドを使用します。適切な TCAM サイズが割り当てられていない場合は、 **hardware access-list tcam region** *VACL <256* の倍数のサイズ> コマンドを使用して、適切な TCAM サイズを割り当てます。

デバイス グループ（Device Groups）

ノードは、トラフィックを負荷分散できる物理サーバー、仮想サーバー、またはサービス アプライアンスにすることができます。これらのノードはデバイス グループの下にグループ化され、このデバイス グループをサービスにマップできます。

ITD はデバイス グループをサポートします。デバイス グループを構成するときは、次を指定できます。

- デバイス グループのノード
- デバイス グループのプローブ

プローブは、デバイス グループ レベルまたはノード レベルで構成できます。ノード レベルのプローブを行う場合、それぞれのノードは自身のプローブで構成可能なため、ノードごとにさらにカスタマイズすることができます。ノード レベルのプローブは、障害状態について各ノードを別々に監視する必要があるシナリオで役立ちます。

ITD クラスタリング

ITDは、同じデバイス グループに含まれるノードのクラスタリングをサポートします。ITDクラスタリングでは、ノードに障害が発生すると、接続テーブルがトラフィックを同じクラスタ内の機能しているノードにリダイレクトするため、トラフィックへの影響が軽減されます。クラスタリングは、トラフィックをデバイス グループのすべてのノード間で負荷分散する必要があるが、ノードのサブセットのみが相互に状態を同期してクラスタを形成する必要がある場合に役立ちます。

ITDクラスタリングを使用すると、デバイス グループ内のノードをクラスタにマッピングできます。クラスタに整数の識別子を割り当て、説明を追加できます。クラスタ定義により、ITDは最初に同じクラスタ内の他のノードへのフェールオーバーを試行します。クラスタ内のすべてのノードに障害が発生した場合にのみ、ITDは同じデバイス グループ内のクラスタ外のノードへのフェールオーバーを試みます。

デバイス グループが1つ以上のアクティブなサービスによって使用されている場合、セッションを介してクラスタに属するノードを削除できます。

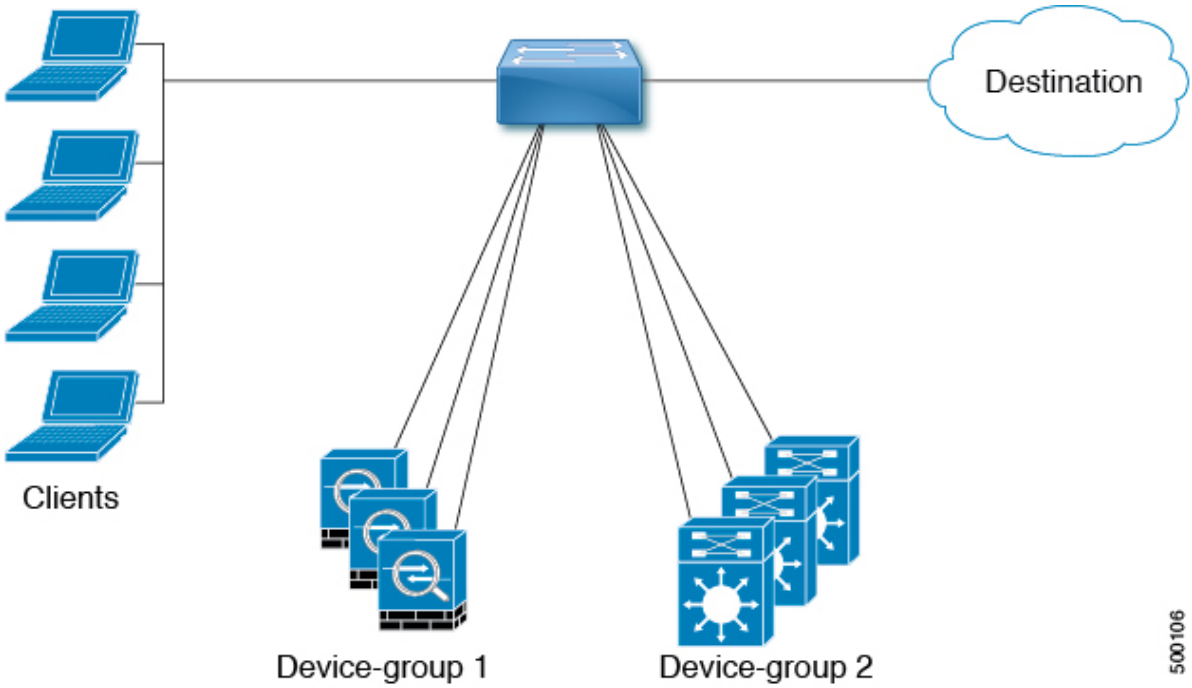
（注）
- ITD は、ノード レベルのスタンバイ ノードまたはホット スタンバイ ノードを持つデバイス グループによるクラスタリングをサポートしていません。
- ITD は、fail-action bucket-distribute でのみクラスタリングをサポートします。

ITD サービス内の複数のデバイス グループ

Cisco NX-OS リリース 7.0(3)I3(1) 以降、ITD サービスで複数の デバイス グループがサポートされています（下図を参照してください）。ITDサービスは、さまざまなデバイス グループを指すさまざまなシーケンスを持つ単一のルートマップを生成します。

各デバイス グループは、異なるサービスを必要としますが、同じ入力インターフェイスに到着する異なるタイプのトラフィックを表します。インターフェイス上のトラフィックは、仮想IPアドレスに基づいて適切なデバイス グループにリダイレクトされます。同じインターフェイスで ITD サービスごとに複数のデバイス グループをサポートすると、ITD を拡張できます。

図 *14 : ITD* サービス内の複数のデバイス グループ



ITD サービスで複数のデバイス グループを設定する方法を示す構成例については、ITD の構成例 （54 ページ） を参照してください。

サポートされるデバイス グループの数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

VRF のサポート

ITD サービスは、デフォルト VRF でもデフォルト以外の VRF でも構成できます。

入力インターフェイスは、ITD サービス用に設定された VRF に属している必要があります。サービスに VRF が構成されていない場合、入力インターフェイスはデフォルト VRF に属している必要があります。

Cisco NX-OS リリース 10.2(1) 以降では、ITD デバイス グループに対して VRF を構成できます。すべてのデバイス グループ ノード メンバーは、ITD デバイス グループ用に構成された VRF で到達可能である必要があります。デバイス グループに VRF が構成されていない場合、サービスのすべての入力インターフェイスと関連付けられたデバイス グループのノード メンバーが、サービスに構成された VRF で到達可能であることを確認する必要があります。デバイス グループとサービスに VRF が構成されていない場合、サービスのすべての入力インターフェイスと、関連付けられたデバイス グループのノード メンバーは、デフォルト VRF で到達可能である必要があります。

ルータ ACL

スイッチは、ITD を使用したルータ アクセス コントロール リスト（RACL）をサポートします。

同じ入力インターフェイスで ITD と RACL を構成できます。TCAM にダウンロードされる構成結果の RACL は、ITD によって生成された ACL とユーザ構成 RACL を合わせた成果物です。RACL で構成された permit ステートメントと deny ステートメントは、ITD によって作成された ACL 許可およびリダイレクト エントリと結合されます。この機能により、選択したトラフィックのフィルタリングおよび負荷分散を行うことができます。

（注）

- ITD 入力インターフェイスで RACL を構成すると、ITD 統計は機能しません。
- アクティブな ITD サービスをホストしている ITD 入力インターフェイスでルータ ACL を使用する必要がある場合、どちらの機能に対しても統計情報を有効にすることはできません。この制限の詳細については、『**Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング構成ガイド**』の「ポリシーベース ルーティング」の章にある「ポリシーベース ルーティングの注意事項と制限事項」の項を参照してください。

ACL の組み込みと除外

インクルード ACL

インクルード ACL 機能を使用すると、ITD サービスにアクセス制御リスト（ACL）を割り当てることができます。ACEに一致するトラフィックのみがノードに向かって負荷分散され、他のトラフィックはデフォルトのルーティング ルールに従います。

Cisco NX-OS リリース 9.3(3) 以降、1 つの ITD サービスで最大 8 つのアクセス リストを設定できます。各アクセス リストを独自のデバイス グループ（マルチ ACL）に関連付けることができます。特定のデバイス グループが 1 つのユーザー ACL に関連付けられている場合、そのデバイス グループが優先され、デフォルトのデバイス グループが上書きされます。この機能により、ITD はさまざまな ACL に一致するトラフィックをさまざまなデバイス グループにロードバランシングできます。

除外 ACL

除外 ACL を設定して、ITD が ITD ロードバランサから除外するトラフィックを指定できます。除外 ACL が選択するトラフィックは RIB ルーティングされ、ITD をバイパスします。除外 ACL は、送信元フィールドと接続先フィールドの両方に基づいてフィルタリングできます。除外 ACL は、仮想 IP アドレスの前にあります。

インクルードおよび除外 ACL によるノードの無停止の追加または削除

Cisco NX-OS リリース 10.1(1) 以降、マルチ ACL または除外 ACL を使用して、サービスによって使用されるデバイス グループにノードを中断することなく追加または削除できます。ノードを追加または削除するデバイス グループ名と同じデバイス グループ名で ITD セッションを作成できます。

異なるデバイス グループを使用しているマルチ ACL の場合、1 つの ITD サービスの下にある 1 つのデバイス グループにノードを追加または削除できます。この変更は、このデバイス グループを使用していない ACL のバケットの再割り当てには影響しません。

ITD サービスの除外 ACL を設定すると、ITD はノード間でバケットを再割り当てします。ITD サービスの除外 ACL 設定の場合、ノードを追加または削除しても、除外 ACL に一致するトラフィックには影響しません。このトラフィックはルーティングされたままです。

（注） マルチ ACL と除外 ACL の両方について、スタンバイ ノードとホット スタンバイ ノードを持つデバイス グループに対して無停止でノードを追加または削除することはできません。

ドロップ ACL

Cisco NX-OS リリース 10.3(1)F 以降、ドロップ ACL は ITD NAT サービスでサポートされます。

ドロップ ACL が ITD NAT サービスにのみ適用される場合、ドロップ ACL に一致するトラフィックはドロップされます。ITD NAT を使用したドロップ ACL は VRF 対応であり、VRF 間 NAT 構成で使用できます。

仮想 IP アドレスのフィルタリング

仮想 IP アドレスを使用して、ITD のトラフィックをフィルタリングできます。トラフィック フィルタリング用の仮想 IP アドレスとサブネット マスクの組み合わせは、宛先フィールドでのみサポートされます。

ポート番号ベースのフィルタリング

ポート番号付けを使用して、ITD のトラフィックをフィルタリングできます。レイヤ 4 ポート（たとえば、ポート 80）に基づいてトラフィックをフィルタリングするために、次の方法がサポートされています。

- 一致する宛先ポート

  宛先ポートが 80 の任意の送信元または宛先 IP アドレスが一致します。（例：仮想 IP アドレスは 0.0.0.0 0.0.0.0 tcp 80 として構成されています。）

- 一致する送信元ポート

  80 以外のポートは ITD をバイパスし、ポート 80 はリダイレクトされます。（例：除外 ACL は、permit tcp any neq 80 any として設定されます。）

- 複数のポート番号の一致

  ITD では、ポートごとに 1 つずつ、複数の仮想 IP アドレス行を設定できます。

ホットスタンバイ

ホットスタンバイ機能は、スイッチを再構成して、動作可能なホットスタンバイ ノードを探し、最初に使用可能なホットスタンバイ ノードを選択して、障害が発生したノードを置き換えます。ITDは、障害が発生したノードを当初宛先としていたトラフィック セグメントを、ホットスタンバイ ノードにリダイレクトするようにスイッチを再設定します。このサービスは、ホットスタンバイ ノードとアクティブ ノードとの固定マッピングを強要しません。

障害が発生したノードが再び動作可能になると、アクティブ ノードとして復元されます。動作中のホットスタンバイ ノードからのトラフィックは元のノードにリダイレクトされ、ホットスタンバイ ノードはスタンバイ ノードのプールに戻ります。

複数のノードで障害が発生した場合、それらすべてのノードを宛先とするトラフィックは、最初に使用可能なホットスタンバイ ノードにリダイレクトされます。

ホットスタンバイ ノードは、ノード レベルでのみ構成できます。ノード レベルで、関連付けられたアクティブ ノードが失敗した場合にのみホットスタンバイ ノードはトラフィックを受信します。

ITD は N + M 冗長性をサポートしており、M ノードは N アクティブ ノードのホットスタンバイ ノードとして機能できます。

複数の入力インターフェイス

複数の入力インターフェイスに対してトラフィック リダイレクト ポリシーを適用するようにITDサービスを構成できます。この機能では、単一のITDサービスを使用して、さまざまなインターフェイスに到着するトラフィックを一連のノードにリダイレクトできます。

Cisco NX-OS リリース 7.0(3)I7(3) 以降、同じ入力インターフェイスを 2 つの ITD サービスに含めることができ、1 つの IPv4 ITD サービスと 1 つの IPv6 ITD サービスが可能になります。

IPv4 と IPv6 の両方の ITD サービスに同じ入力インターフェイスを含めると、IPv4 と IPv6 の両方のトラフィックが同じ入力インターフェイスに到着することができます。IPv4 トラフィックをリダイレクトするために IPv4 ITD ポリシーが適用され、IPv6 トラフィックをリダイレクトするために IPv6 ITD ポリシーが適用されます。

（注） 同じ入力インターフェイスが複数の IPv4 ITD サービスまたは複数の IPv6 ITD サービスで参照されていないことを確認してください。システムはそれを自動的に適用せず、サポートされていません。

（注） ITD IPv4 サービスは、IPv4 PBR ポリシーがすでに適用されている入力インターフェイスでは有効にできません。ITD IPv6 サービスは、IPv6 PBR ポリシーがすでに適用されている入力インターフェイスでは有効にできません。

システム ヘルスモニタリング

ITDは、ノードとそれらのノードで実行されているアプリケーションの状態を定期的に監視して、障害を検出し、障害シナリオを処理します。

ICMP、TCP、UDP、DNS、および HTTP プローブがサポートされています。

ノードに接続されたインターフェイスの正常性

Cisco NX-OS リリース 7.0(3)I3(1) 以降、ITD ITD は IP サービスレベル アグリーメント（IP SLA）機能を利用して、各ノードを定期的にプローブします。以前のリリースでは、ITD は Internet Control Message Protocol（ICMP）を使用して、各ノードを定期的にプローブします。プローブはデフォルトで10秒の頻度で送信され、1秒まで設定できます。それらはすべてのノードに同時に送信されます。プール グループ構成の一部としてプローブを構成できます。

プローブは、デフォルトで3回再試行した後に障害が発生したと宣言されます。この時点で、ノードの状態は「機能不全」、ステータスは「PROBE_FAILED」になります。

ノード障害の処理

ノードがダウン状態としてマークされると、ITDはトラフィックの中断を最小限に抑えて、トラフィックを残りの運用可能なノードに再配布するために自動的に次のタスクを行います。

- 障害が発生したノードを引き継ぐようにスタンバイ ノードが構成されているかどうかを判別します。
- スタンバイ ノードが運用可能な場合、トラフィックを処理するノードの候補としてそのノードを識別します。
- 運用可能なスタンバイ ノードを使用できる場合、トラフィックを処理するアクティブ ノードとしてそのスタンバイ ノードを再定義します。
- 障害が発生したノードから新しくアクティブにされたスタンバイ ノードにトラフィックを再割り当てするように自動的にプログラムします。

プローブのユーザー定義トラック ID

ユーザーは独自のトラックを定義し、それらを各ノードに関連付けることができます。ノードにユーザー定義のトラックが割り当てられている場合、対応する **ip sla** 構成は、トラックを操作するユーザーによって構成される必要があります。ITD は、ノードに新しいトラックと **ip sla** ID を割り当てません。ユーザー定義のトラックは、プライマリ、スタンバイ、およびホット スタンバイ ノードに割り当てることができます。ユーザーは、ITD セッションによって追加された新しいノードにユーザー定義のトラックを割り当てることができます。ITDによって生成されたトラックは、ユーザー定義のトラックとして使用できません。

ユーザー定義のトラックを使用して新しいノードを追加する例：

```
itd device-group dg1
  node ip 1.1.1.2
    probe track 30
  node ip 1.1.1.3
    probe track 40
```

```
  node ip 1.1.1.4
    mode hot-standby
    probe track 50

itd device-group dg2
  node ip 1.1.1.6
    probe track 70
    standby ip 1.1.1.5
      probe track 60
```

ノードにユーザー定義のトラックがない場合、サービスが有効になったときに、ITDサービスは **track id** および **ip sla** ID を割り当てます。

ピア同期

ピア同期機能は、サンドイッチ モードで 2 つの ITD ピア サービス間でノードのヘルス ステータスを同期します。いずれかの ITD ピア サービスのリンクがダウンした場合のトラフィック損失を防ぐのに役立ちます。

各 ITD サービスは、ピア サービスを定期的にプローブして、障害を検出します。ping は毎秒 ITD ピア サービスに送信されます。応答が受信されない場合は、3 回再試行されます。頻度と再試行回数は構成できません。

（注） ピア サービス機能では、サービス間でノードの同期フェールオーバーを可能にするために、fail-action 最小バケットまたはバケットごとの fail-action ノードを構成する必要があります。さらに、いずれかのサービスがホット スタンバイ ノードまたはノード レベルのスタンバイを使用している場合、同期フェールオーバーはサポートされません。

Failaction 再割り当て

ITD の Failaction により、障害が発生したノードへのトラフィックを 1 つ以上のアクティブ ノードに再割り当てできます。障害が発生したノードが再びアクティブになると、接続の処理が再開されます。すべてのノードがダウンした場合、パケットは自動的にルーティングされます。すべての Failaction メカニズムは、IPv4 サービスと IPv6 サービスの両方でサポートされます。

（注） Failaction 機能をイネーブルにする前に、ITD デバイス グループにプローブを設定する必要があります。

Failaction ノードの再割り当て

ノードがダウンすると、そのノードに関連付けられたトラフィック バケットは、構成されている一連のノードで最初に検出されたアクティブ ノードに再割り当てされます。新しく再割り当てされたノードでも障害が発生すると、トラフィックは次に使用可能なアクティブ ノードに再割り当てされます。

ノードが回復し、それ以上の障害イベントがない場合は、障害が発生する前にノードに最初に割り当てられていたトラフィック バケットがそのノードに再割り当てされます。

Failaction ノードの最小バケット（Failaction Node Least-Bucket）

ノードがダウンすると、そのノードに関連付けられたトラフィック バケットは、現在最小数のトラフィック バケットからトラフィックを受信しているアクティブ ノードに再割り当てされます。後続のノード障害ごとに、トラフィック バケットが最も少ないアクティブ ノードが再計算され、障害が発生したノードに向けられたすべてのバケットがこのノードにリダイレクトされるため、再割り当てされたバケットを複数のアクティブ ノードに分散できます。

ノードが回復し、それ以上の障害イベントがない場合は、障害が発生する前にノードに最初に割り当てられていたトラフィック バケットがそのノードに再割り当てされます。

Failaction バケット分配（Failaction Bucket Distribute）

サービスが有効な場合、ITDは内部アルゴリズムを使用して、プライマリ ノードのさまざまなシーケンスを、プライマリ ノードごとに異なる優先順位を持つ代替バックアップ パスとして事前に選択します。ノードがダウンすると、そのノードへのトラフィックは、優先度が最も高い最初のアクティブ バックアップ ノードにリダイレクトされ、その後の障害についても同様にリダイレクトされ、それによってコンバージェンスの遅延が最小限に抑えられます。

ノードが回復すると、最初にプライマリとしてこのノードに割り当てられていたトラフィック バケットがそのノードに再割り当てされます。プライマリ ノードがまだ障害状態であり、新しく回復したノードが最も優先順位の高いアクティブ バックアップとして動作するトラフィック バケットも、そのトラフィック バケットに再割り当てされます。

Cisco NX-OS リリース 9.3(2) 以降では、すべてのデバイス グループののプライマリ ノード、またはデバイス グループの最大 32 のプライマリ ノード（いずれか少ない方）が、ノードごとに異なる優先順位で事前に選択されます。

（注） このアルゴリズムは、比較的均等なトラフィック分散を目的としていますが、ノード障害が発生した場合の均等な分散を保証するものではありません。

Failaction Node-Per-Bucket

特定のノードに障害が発生すると、バケットの数が最も少ないノードが識別され、バケットは、バケットの数が最も少ないノードから開始して、他のアクティブ ノードに分散されます。

ITDは、現在最も少ないバケット ノードを繰り返し識別し、すべてのバケットが再割り当てされるまで、そのノードに1つのバケットを割り当てます。したがって、すべてのバケットは、残りのすべてのアクティブ ノード間で均等に分散されます。

（注） Cisco Nexus NX-OS リリース 9.3(5) 以降、ITD ITD は、ノードの重みに基づいて、フェールオーバーするノードを識別します。ノードに重みが設定されていない場合、デフォルトの重み 1 が使用されます。

（注） failaction node-per-bucket とピア同期しているノードのノードの重みはサポートされていません。

ノード障害で ITD Fail-Action のドロップ

ノード障害時の ITD Fail-Action Drop は、パケットをルーティングする代わりにドロップできるようにする failaction オプションです。構成時に、次の条件がすべて満たされる場合、プライマリ ノード N に割り当てられたパケットはドロップされます。

- プライマリ ノード N がダウンしています。
- プライマリ ノード N に構成されているスタンバイ ノードまたはホット スタンバイ ノードがダウンしています。
- 再割り当てに使用できる他のアクティブ ノードはありません。

Cisco NX-OS リリース 10.1(1) 以降、このオプションを次の failaction メソッドと一緒に使用できます。**drop-on-fail**

- Failaction ノードの再割り当て（Failaction Node Reassign）
- Failaction ノードの最小バケット（Failaction Node Least-Bucket）
- Failaction バケット分配（Failaction Bucket Distribute）
- バケットごとのノードの Failaction 再割り当て（Failaction Reassign Node-Per-Bucket）

バケットのネクストホップが再びアクティブになるか、ITD がアクティブ ノードを検出してルートマップを再プログラムするまで、パケットはドロップされたままになります。その後、パケットは再びリダイレクトされます。

Cisco NX-OS リリース 10.2(2)F 以降、ITD デバイス グループの一部として、ノード IP アドレスの下にノード レベルのスタンバイ IP を設定できます。Failaction Bucket Distribute でスタンバイ IP を設定できます。

Failaction 最適化

Cisco NX-OS リリース 9.2(2) より前では、ノードがダウンすると、そのノードに関連付けられたバケットは、fail-action アルゴリズムの決定に従ってアクティブ ノードに再割り当てされます。ただし、新しく再割り当てされたノードにも同時に障害が発生した場合、障害アクションの計算を再実行した後、元の障害ノードのトラフィック バケットを別のアクティブ ノードに

再割り当てする必要があります。障害が発生したノード バケットをアクティブ ノードに再割り当てする際の遅延は、ネットワーク パフォーマンスに影響します。

fail-action の最適化では、ノードがダウンすると、利用可能なすべてのノードのステータスが最初に事前に取得されます。障害として検出されたすべてのノードの再割り当ては、失敗アクション メカニズムに基づいて実行されるため、再割り当ての繰り返しによる遅延が回避されます。

Cisco NX-OS リリース 9.3(3) 以降、この最適化は、ピア同期が設定されている場合を除き、すべてのサービスに対してデフォルトで有効になっています。

vPC のバケット配布を使用した ITD NAT

Cisco NX-OS リリース 10.2(2)F 以降、vPC ノードの Fail-Action バケット配布で ITD NAT を使用できます。この fail-action オプションにより、バケットは事前定義されたバケットをノードマッピングに配布できます。

ノードが vPCペア全体でダウンすると、バケット分散ロジックにより、再割り当てされたノードが vPC 全体で同じになるようにします。VPC の ITD NAT で fail-action バケット配布を使用することをお勧めします。

Failaction 再割り当てを使用しない場合

Failaction によるノードの再割り当てを設定しない場合は、次の 2 つのシナリオが考えられます。

プローブを構成して Failaction 再割り当てをしない

ITDプローブでは、ノードの障害やサービス到達可能性の消失を検出できます。ノードに障害が発生した場合、failactionが設定されていないため、トラフィックはルーティングされ、再割り当てされません。ノードが回復すると、その回復したノードがトラフィックの処理を開始します。

プローブの構成なしで Failaction 再割り当てをしない

プローブが構成されていないと、ITDはノードの障害を検出できません。ノードがダウンしても、ITD はアクティブ ノードへのトラフィックの再割り当てまたはリダイレクトを行いません。

ITD ノードのメンテナンス モード

ITDサービスの接続先ノードは、メンテナンスまたはアップグレード手順のために使用しないようにする必要がある場合があります。この間、これらのノードはネットワーク内で到達可能ですが、トラフィックの受信や処理には使用されません。

バージョン10.1(2)以降、関連するデバイス グループ内のそのようなITDノードを管理上シャットダウンすることにより、ノードをメンテナンス モードに移行できます。ノードがシャットダ

ウンすると、ノードは引き続きデバイス グループ内の有効なエンドポイントとして保持されますが、ITD サービスはそのノードへのトラフィック フローの送信を停止し、他の運用上アクティブなノードに切り替えます。

ノードの管理シャットダウン状態を解除することで、ノードのメンテナンス モードを解除できます。これにより、ITD サービスはノードへのロード バランシング トラフィック フローを再開できます。

プライマリ、ホット スタンバイ、およびノード レベルのスタンバイ ノードは、メンテナンス モードにすることができます。デバイス グループがアクティブなサービスによって使用されていない場合でも、ノードはデバイス グループ内で管理上シャットダウンまたは非シャットダウンになる場合があります。

障害時の ITD ノード ホールドダウン

ノードが障害から回復した後、ITDは、ノードからバケットへの割り当てに基づいて、運用上アクティブなノードから回復したノードにトラフィック フローをリダイレクトします。ITD ノード間で状態の同期が有効になっていない場合、アクティブなITD ノード間でトラフィック フローが切り替わるたびに、ユーザー接続がリセットされる可能性があります。また、到達可能性を頻繁に変更するノードへのトラフィックのリダイレクトを再開することは望ましくない場合があります。

バージョン 10.1(2) 以降では、ノードの回復後であっても、ITD がトラフィック フローをリダイレクトするのを防ぐために、特定の数の障害が発生した後にノードを動作的に停止させることができます。これは、ノード（プライマリまたはホット スタンバイまたはノード レベル スタンバイ）またはデバイス グループのホールドダウンしきい値障害カウントとタイマーを定義することによって実現されます。

- ホールドダウン障害のしきい値カウントが 1 に指定されている場合、ITD は、1 回の障害の後、ノードの回復後にトラフィックがリダイレクトされることを許可しません。
- ホールドダウン障害のしきい値カウントが 1 より大きくなるように指定されている場合、ITDは、設定されたホールドダウンしきい値タイマーに関連するスライディングウィンドウを使用します。これは、ノードのホールドダウンの前に、指定されたホールドダウンの失敗のカウントに達したかどうかを識別します。

その後、ノードは、デバイス グループ内のノードで管理上の shut および no-shut を介して、メンテナンス ウィンドウ中に到達可能であれば、動作上アクティブな状態に戻すことができます（ITD ノードのメンテナンス モード （29 ページ）を参照してください）。

または、関連するデバイス グループを使用してすべてのサービスを管理上無効にすると、ノードが到達可能であれば、その後サービスを有効にした後にノードを使用できるようになります。

ITD サブセカンド コンバージェンス

ITD は、IP-SLA プローブを介してエンドポイントのヘルスモニタリングを提供し、障害が発生したエンドポイントからアクティブなエンドポイントにトラフィックをリダイレクトする追

跡および失敗アクション メカニズムを提供します。ITD はトラフィック フローをライン レートで負荷分散およびリダイレクトするため、すべてのITDバケットを切り替えて別のアクティブなエンドポイントにリダイレクトすることにより、エンドポイント障害時のトラフィック損失を最小限に抑えることが不可欠です。このコンバージェンス時間は、プローブ タイマー、追跡再試行タイマー、およびハードウェア構成の更新にかかる時間によって異なります。

Cisco NX-OS リリース 10.1(1) 以降では、次の設定、トポロジ、プラットフォーム、およびスケールの推奨事項を使用して、ITD ノード障害イベントの 1 秒未満のコンバージェンスを実現できます。

- スイッチで PBR 高速コンバージェンス機能を有効にします。詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide、リリース 10.1(x)』の「ポリシーベースのルーティングの構成」の章を参照してください。
- バケット配布の失敗アクション メカニズムを使用して ITD サービスを設定します。
- または、障害アクション メカニズムのないサービスを備えたノード レベルまたはホット スタンバイ ノードで ITD デバイス グループを使用します。

（注） アクティブ ノードとそれに該当するスタンバイ ノードに障害が発生した場合、failaction が設定されていない場合、トラフィックの損失が観察されます。

- ハードウェア アトミック アップデートが有効になっていることを確認します。
- エンドポイントまたはITD ノードが直接接続されており、以下を介して到達可能であることを確認してください。
  - レイヤ 3 物理インターフェイス
  - レイヤ 3 ポート チャネル
  - サブインターフェイス
  - 単一の物理インターフェイスまたは単一のレイヤ2ポートチャネルのメンバーシップを持つ SVI。
  - VPC ピアで ITD が設定されている場合の SVI 経由の一意の VPC（Cisco Nexus C9316D-GX、C93600CD-GX、C9364C-GX でのみサポート）。トラフィック コンバージェンスを向上させるには、両方の VPC ピアで、VPC のメンバーであるすべてのインターフェイスで光ファイバトランシーバを使用します。
- Cisco NX-OS リリース 10.1(1) 以降、ITD サブセカンド コンバージェンスは Cisco Nexus C93180YC-FX、C93108TC-FX、C9336C-FX2、C93240YC-FX2、C93360YC-FX2、C93216TC-FX2、C9336C-FX2-E、C9316D-GX、C93600CD-GX、C9364C-GX でのみサポートされています。

（注） 各スイッチのモデル番号は、スイッチの基本製品 ID（PID）を表します。スイッチに基づく製品バンドルと構成を表す拡張 PID は表示されません。一般に、スイッチがサポートされている場合、これらの拡張 PID もサポートされます。

ITD サブセカンドコンバージェンスは、次の構成プロファイルまたは同等のものでサポートされています。

ITD サービスあたりのバケット数	ITD サービスごとのインクルード ACL の数	ITD サービスあたりの VIP の数	ITD サービスあたりの ACE の数	障害により影響を受けるサービスの数
64	8	N/A	512（64 × 8）	2（I IPv4、1 IPv6 サービス）
64	該当なし	8	512（64 × 8）	2（I IPv4、1 IPv6 サービス）
256	IPv4 の 3 つの ACL、IPv6 の 1 つの ACL	該当なし	1024（256 × 3 + 256）	2（I IPv4、1 IPv6 サービス）
256	該当なし	3 IPv4 の VIP、IPv6 の VIP	1024（256 × 3 + 256）	2（I IPv4、1 IPv6 サービス）
256（VPC 上の ITD の場合）	1 つのキャッチオール ACL	該当なし	256	1 IPv4 サービス
256（VPC 上の ITD の場合）	該当なし	1 キャッチオール VIP	256	1 IPv4 サービス

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS* ライセンス ガイド』および『*Cisco NX-OS* ライセンス オプション ガイド』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降、「Nexus スイッチ プラットフォーム サポート マトリクス」を使用して、選択した機能をサポートするさまざまな Cisco Nexus 9000 および 3000 スイッチのリリース元である Cisco NX-OS を知ることができます。

ITD の注意事項と制約事項

ITD に関する注意事項と制約事項は次のとおりです。

- ITD は、次のプラットフォームでサポートされています。

ITDv4 のサポート

- Cisco Nexus NX-OS リリース 10.1(1) 以降、Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ラインカードがサポートされています。
- Cisco Nexus NX-OS リリース 9.3(1) 以降、Cisco Nexus X9788TC-FX、X97160YC-EX、および X9732C-EX ラインカードを備えた Cisco Nexus 9500 シリーズ スイッチ。
- Cisco Nexus NX-OS リリース 9.2 (1) 以降、Cisco Nexus C9364C、C9336C-FX2、C93240YC-FX2 スイッチがサポートされています。
- Cisco Nexus 93180YC-EX、93108TC-EX、C93180YC-FX、および C93108TC-FX スイッチがサポートされています。
- Cisco NX-OS リリース 10.4(1)F 以降、ITD は、トラフィックのロードバランシングとリダイレクションのために、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチ上のサービスの入力インターフェイスとして、GRE および IP-IP トンネル インターフェイスをサポートします。

（注） NAT 宛先機能が有効になっている ITD サービスは、IP-IP および GRE トンネル インターフェイスを入力インターフェイスとしてサポートしません。

ITDv6 のサポート

- Cisco Nexus 93180YC-EX、93108TC-EX、C93180YC-FX、および C93108TC-FX スイッチがサポートされています。
- Cisco NX-OS リリース 9.2 (1) 以降、Cisco Nexus C9364C、C9336C-FX2、C93240YC-FX2 スイッチがサポートされています。
- Cisco NX-OS リリース 9.3 (5) 以降、Cisco Nexus X9732C-FX および X97160YC-EX ラインカードと Sup B+ を備えた Cisco Nexus 9500 シリーズ スイッチがサポートされています。
- Cisco NX-OS リリース 9.3 (5) 以降、Cisco Nexus C9316D-GX、C93600CD-GX、C9364C-GX、および C93180YC-FX3S スイッチがサポートされています。
- Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ラインカードがサポートされています。

- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、IPv6 サービスのロード バランシング レイヤ 4 ポート範囲オプションをサポートしていません。
- Cisco NX-OS リリース 10.4(1)F 以降、ITD はトラフィックのロードバランシングとリダイレクションのために、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチ上の IPv6 サービスの入力インターフェイスとして、GRE トンネル インターフェイスをサポートします。

- Cisco NX-OS リリース 10.1(2) 以降、IPv4 および IPv6 を使用した PBR は N9K-C93108TC-FX3P スイッチでサポートされます。
- ITD は、ネクストホップ IP アドレスへの入力または出力に FEX ポートを使用することをサポートしていません。
- 構成のロールバックおよび構成の置換は、ターゲット構成とソース構成の両方でITDサービスがシャット モードの場合にのみサポートされます。
- 宛先 NAT は、IPv4 でのみサポートされます。
- シームレスなスイッチオーバーは、L3 ITD サービスでサポートされています。
- SNMP は ITD ではサポートされていません。
- 設定置換機能を使用してITDを変更する前に、ITD サービスをシャットダウンする必要があります（**shutdown**）。
- Cisco NX-OS リリース 9.3(2) 以降、IPv6 はノード レベルのプローブとデバイス グループ レベルのプローブをサポートします。
- ノード レベルの IPv6 TCP、ICMP プローブがサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降、ITD は重み付きの **fail-action node-per-bucket** をサポートします。
- オプションは、IPv4 および IPv6 で使用できます。 **bucket distribution**

（注） ホット スタンバイ ノードを使用するサービスでは、フェイル アクション バケット配布は推奨されません。

- Cisco NX-OS リリース 10.1(2) 以降、レイヤ 3 ポートチャネル入力サブインターフェイスを使用したポリシーベース ルーティングは、Cisco Nexus 9300-X、FX2、FX3、GX TOR および FX、GX EOR スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、ITD は、すべての failaction メソッドで使用できるノード障害オプションとして **drop-on-fail** オプションをサポートしています。このオプションは ITD IPv4 および IPv6 サービスをサポートしますが、ITD L2 サービス、ITD L3 NAT サービス、またはピア サービスを使用した ITD L3 サービスはサポートしません。

Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、**drop-on-fail** オプションをサポートしていません。

- **ITD クラスタリング機能には、次のガイドラインと制限事項が適用されます。**
  - Cisco NX-OS リリース 10.1(1) 以降、ITD クラスタリングは Cisco Nexus C93240YC-FX2、C93108TC-FX、C9316D-GX、C9364C-GX でサポートされています。
  - ITD は、ノード レベルのスタンバイ ノードまたはホット スタンバイ ノードを持つデバイス グループ内のノードのクラスタリングをサポートしていません。
  - ITD クラスタリングは、**fail-action bucket distribute** fail-action オプションでのみサポートされます。
  - ピア同期が有効になっているサービスでは、ITD クラスタリングはサポートされていません。
  - ノードがデバイス グループの重みで構成されている場合、ITD クラスタリングはサポートされません。
- **ITD サブセカンド コンバージェンス機能には、次のガイドラインと制限事項が適用されます。**
  - Cisco NX-OS リリース 10.1(1) 以降、ITD サブセカンド コンバージェンスがサポートされるのは次のスイッチです。Cisco Nexus C93180YC-FX、C93108TC-FX、C9336C-FX2、C93240YC-FX2、C93360YC-FX2、C93216TC-FX2、C9336C-FX2-E、C9316D-GX、C93600CD-GX、C9364C-GX
  - ITD サブセカンド コンバージェンスは、ITD over VXLAN、レイヤ 2 ITD、および NAT 対応の ITD サービスではサポートされていません。
  - ITD サブセカンド コンバージェンスは、単一エンドポイントの障害にのみ適用されます。複数の同時エンドポイント障害には適用されません。
  - PBR 高速コンバージェンスは主に、ITD エンドポイントに到達可能なリンクが障害として検出されたイベントでサポートされます。
  - PBR 高速コンバージェンスは、ミリ秒の SLA またはトラックと一緒に使用して、ITD のミリ秒のコンバージェンスを実現することはできません。
- 次の注意事項および制約事項を除外 ACL 機能に適用します。
  - 除外 ACL は、許可アクセス制御エントリ（ACE）のみをサポートします。ACE 拒否はサポートされていません。
  - 除外 ACL の許可 ACE と一致するトラフィックは、ITD をバイパスします。
  - Cisco NX-OS リリース 10.1(1) 以降、ノードの無停止の追加および削除は、除外 ACL を使用した IPv4 および IPv6 サービスの両方でサポートされています。
- 次の注意事項および制約事項をインクルード ACL 機能に適用します。

- ASIC の 1 枚で固有の 62 個の ACL のみが設定できます。各 ACL は、1 つのラベルを持ちます。同じ ACL が複数のインターフェイスで設定される場合、同じラベルが共有されます。ただし、各 ACL が一意のエントリを持つ場合、ACL のラベルは共有されず、そのラベルの上限は 62 です。一枚あたり 62 個の ACL の制限付きでスイッチあたり 150 ITD サービスを実現するには、入力インターフェイスを ASIC の複数枚に分散させる必要があります。詳細については、IP ACL の構成 を参照してください。
- 送信元パラメータまたは宛先パラメータのいずれかでアドレス グループまたはポート グループとして指定されたオブジェクト グループを持つACEはサポートされません。
- IPv6 ACL は、ITD サービスのトラフィック選択のためのインクルード アクセス リストとして設定できます。
- 入力 ACL は、ユーザー定義 ACL のレイヤ 4 ポート範囲をサポートしていません。
- **permit** メソッドを持つ ACE のみが ACL でサポートされます。他の方法（**deny** または **remark** など）の ACE は無視されます。
- 1 つの ACL で最大 256 の許可 ACE がサポートされます。
- Failaction はノード間でサポートされています。
- ITD は、インクルード ACL 機能または仮想 IP アドレス（VIP）機能のいずれかをサポートしますが、両方はサポートしません。
- インクルード ACL を使用して ITD を設定し、送信元 IP ベースのロード バランシングを使用している場合、ACE の送信元 IPv4 のサブネット マスクを /32 にすることはできません。または、ACE の送信元 IPv6 アドレスのサブネット マスクを /128 にすることはできません。また送信元アドレスのサブネットマスクは、構成されたバケットと互換性がある必要があります。インクルード ACL を使用して ITD を設定し、宛先 IP ベースのロード バランシングを使用している場合、ACE の宛先 IPv4 アドレスのサブネット マスクを /32 にすることはできません。または、ACE の宛先 IPv6 アドレスのサブネット マスクを /128 にすることはできません。また宛先アドレスのサブネット マスクは、構成されたバケットと互換性がある必要があります。
- Cisco Nexus NX-OS リリース 9.3(5) 以降、インクルード ACL を使用してトラフィックをフィルタリングするサービスに対してマスク位置がサポートされています。
- Cisco Nexus NX-OS リリース 9.3(5) 以降、インクルード ACL 機能で最小ビット ロード バランシングがサポートされています。
- Cisco NX-OS リリース 10.1(1) 以降、マルチ インクルード ACL を使用した IPv4 および IPv6 サービスの無停止でのノードの追加および削除がサポートされています。
- Cisco NX-OS リリース 10.4(1)F 以降では、include ACL ルールのレイヤ 4 ポート範囲とその他のポート操作（「等しくない」、「より大きい」、「より小さい」など）が適用されます。 ITD サービス用に生成されたバケット アクセス リスト内のトラフィックのフィルタリングに使用されます。
- アクセスリストでレイヤ 4 ポートオペレータを使用しながら、TCAM ACE の使用率を最適化するには、この構成 **hardware access-list lou resource threshold**を使用する必

要があります。このコマンドの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド』の「**IP ACL の構成**」のセクションを参照してください。

- Cisco NX-OS リリース 10.4(1)F 以降、ITD は、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチの GRE および IP-IP トンネル インターフェイスを介して到達可能なレイヤ 3 ノードへのリダイレクションまたはロードバランシングをサポートします。

（注） NAT 宛先機能が有効になっている ITD サービスは、トンネル インターフェイスを介して到達可能なレイヤ 3 ノードへのリダイレクションまたはロードバランシングをサポートしていません。

- プローブ トラフィックを別の CoPP クラスに分類することをお勧めします。そうしないと、プローブ トラフィックはデフォルトでデフォルトの CoPP クラスになり、ドロップされる可能性があり、プローブ トラフィックの IP SLA バウンスが発生します。構成情報については、IP SLA パケットの CoPP の構成 を参照してください。
- ITD セッションは、次ではサポートされていません。
  - ノード レベルのプローブ。

（注） ユーザー定義のトラックを使用するノード レベルのプローブがサポートされています。

  - ホットスタンバイまたはノードレベルのスタンバイノードを持つデバイスグループ。
  - ピア同期が有効になっているサービスによって使用されているデバイス グループ。
  - レイヤ 4 ロードバランス オプションが構成されたサービス。
  - 異なるデバイス グループを使用する複数の仮想 IP を持つサービス。
- アトミック アップデートを無効にすると、より多くの TCAM リソースを ITD ポリシーで使用できるようになりますが、ポリシーの変更中にトラフィックが中断する可能性があります。詳細については、セキュリティ構成ガイド 10.1(x) を参照してください。
- ITD-L2 および ITD レイヤ 3 には、個別のインターフェイスが必要です。
- ITDのチェックポイントと構成のロールバック機能は、サービスがダウンしている場合にのみサポートされます。
- **接続先 NAT 機能には、次のガイドラインと制限事項が適用されます。**
  - Cisco NX-OS リリース 10.2(1)F 以降、ITD は NAT 統計をサポートします。
  - Cisco NX-OS リリース 10.2(2)F 以降、ITD はレイヤ 3/レイヤ 4 ロード バランシングとライン レート ロード バランシング + NAT を提供します。

- クライアントからの実サーバー IP からサーバー IP とネットワークを保護します。
- NAT は、VIP および/またはプロトコル/ポートでサポートされています。VIP なしではサポートされません。
- 同じサーバーセットを使用してロードバランサを行う場合、仮想IP（VIP）には一意の L4 ポート番号が必要です。
- ポート番号が複数のサービスで同じ場合、NAT は同じデバイス グループとノードを再利用できません。
- アトミック更新が無効な場合は最大1024、アトミック更新が有効な場合は672のNATエントリの制限。
- Cisco NX-OS リリース 10.3(1)F 以降、N9K-C9364C-GX および N9K-C93600CD-GX の制限は、アトミック更新が無効になっている場合は 1920 NAT エントリ、有効になっている場合は 1344 です。
- Cisco NX-OS リリース 10.3(1)F 以降、ITD NAT はデフォルトおよびデフォルト以外の VRF でサービスとデバイス グループをサポートします。

（注） 入力インターフェイスと関連するデバイス グループ ノードが、すべて NAT 宛先が有効になっているサービスのデフォルト以外の同じ VRF で到達可能である場合は、ITD サービスと ITD デバイスグループの両方でVRFを明示的に構成する必要があります。

（注） ITD NAT VRF 構成については、『**Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド**』の「*[IP ACL* の構成」セクションを参照してください。

- NAT IPv6 はサポートされていません。IPv4 のみがサポートされています。
- **least-bucket** および **node per bucket** および **bucket distribute** fail アクションのみがサポートされています。

（注） ITD NAT は **fail-action node reassign** でサポートされていません。

- ITD NAT は Nexus 9300 でのみサポートされています。
- ITD ピア同期は ITD NAT ではサポートされていません。
- ITD セッションは NAT をサポートしていません。
- ホットスタンバイ、デバイス グループ、およびノード レベルのスタンバイはITD NATではサポートされません。

- アドバタイズ可能オプションは、ITD NAT 可能なサービスでのすべての VIP にとって必須です。
- NAT は VXLAN 上の ITD ではサポートされていません。
- NAT は、DST ベースのロードバランシングではサポートされていません。
- Cisco NX-OS リリース 10.3(1)F 以降、ITD NAT は Exclude ACL でサポートされます。
- Cisco NX-OS リリース 10.3(1)F 以降、ITD NAT はレイヤ 4 送信元ベースのロード バランシング オプションをサポートします。
- アトミック アップデートが有効になっている場合、TCAM エントリの数は TCAM カービングよりも少なくする必要があります。
- ITD セッションとノードの無停止の追加または削除はサポートされていません。
- ITD NAT ではシームレス スイッチオーバーはサポートされていません。
- Cisco NX-OS リリース 10.2(1q)F 以降、ITD NAT は N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは ITD NAT をサポートしていません。

（注） Cisco NX-OS リリース 9.3(1) から以前のリリースへの ISSD を実行する前に、サービスから NAT 接続先構成を削除し、ダウングレードを続行します。

- Cisco NX-OS リリース 10.3(1)F 以降、ドロップ ACL は ITD NAT サービスでのみサポートされます。
- 次の注意事項および制約事項を VXLAN 上での ITD 機能に適用します。

  次の機能はサポートされていません。

  - Fail アクション メソッド。
  - プローブ。
  - ITD セッション。
  - デバイス グループ内の IPv6 ノード。
  - VPC
  - ピア同期。
  - ノードレベルのスタンバイ。
  - レガシー ITD および ITD over VXLAN サービスは、ノード上の同じデバイス グループを共有できません。

- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、VXLAN 上での ITD をサポートしていません。

- 以前のリリースから ISSU を使用する前に、 **feature PLB** を非アクティブ化する必要があります。
- VIP とホットスタンバイは、ITD over VXLAN を有効にするための必須の構成です。
- 構成の適用方法（CLI または DME を使用）に関係なく、デバイス グループの順序のノードはすべてのリーフ ノードで同じである必要があります。
- Cisco NX-OS リリース 10.2(1q)F 以降、VXLAN 上での ITD は N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(3)F 以降では、新しい L3VNI インターフェイス タイプを IPv4 サービスと IPv6 サービスの両方の入力インターフェイスとして構成できます。適用される注意事項と制限事項は次のとおりです。
  - マルチ ACL とマルチ VIP サービスの両方がサポートされ、基本的な ITD サービスもサポートされます。
  - この機能は N9K-X9716D-GX ライン カードおよび Cisco N9K-C93180YC-FX3 プラットフォーム スイッチを搭載した Cisco Nexus 9504 および 9508 スイッチでサポートされます。

ITD PAT に関する注意事項と制約事項は次のとおりです。

- デバイス グループで複数の VIP を PAT で使用する場合は、VIP ごとに一意のデバイス グループを関連付ける必要があります。
- PAT を使用する場合は、VIP とともにポート番号が必須です。
- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは ITD PAT をサポートしていません。

ITD-L2 ロード バランシングには、次の構成に関する注意事項と制限事項があります。

- Cisco Nexus 93108TC-EX および Cisco Nexus 9516 スイッチは、レイヤ 2 ロード バランシング サービスをサポートします。Cisco Nexus NX-OS リリース 9.3(5) 以降、C93180YC-FX および C93240YC-FX2 がサポートされています。

（注） レイヤ 2 ロード バランシング機能は、Cisco 9500 EX/FX/R ライン カードではサポートされていません。

レイヤ 2 ロード バランシングは、vPC、ポート チャネル、および L3 インターフェイスをサポートしていません。

- トランク内のポート グループ インターフェイスのみがサポートされます。

- ITD-L2 ポート グループを 3 つ以上のサービスで共有しないでください。
- TCAM サイズが、サービスの数に加えてバケットの数の合計と等しいことを確認します。
- ITD では、150 のサービスを構成できます。ただし、ITD-L2 の場合、4 つ以上のサービスを構成することはできません。
- 以前のリリースから ISSU を使用する前に、**feature smart-channel** を非アクティブ化する必要があります。レイヤ 2 ITD サービスは、スマート チャネルの代わりにレイヤ 2 ロード バランシング用に設定する必要があります。
- L4 ポートベースのロードバランシングがサポートされています。
- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、ITD-L2 ロード バランシングをサポートしていません。
- 次の制限は ITD-L2 機能に適用され、サポートされていません。
  - Fail アクション メソッド。
  - プローブ。
  - ITD セッション。
  - デバイス グループ内の IPv6 ノード。
  - VPC
  - ピア同期。
  - ノードレベルのスタンバイ。
- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、次の機能をサポートしていません。
  - ピア サービス
  - ピア同期
  - プローブの ITD ユーザー定義トラック ID
  - 重みの変更またはセッションを介した重みを持つノードの追加
  - ノードのクラスタへのマッピング
  - 統計

（注） ITD ノード上のトラフィック フローのロードバランスを特定するには、インターフェイスの統計情報を表示します。

- Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カードは、現在、ICMP、TCP、および UDP プローブのみをサポートしています。

次の注意事項と制限事項は、ITD ノード メンテナンス モードとノード保留機能に適用されます。

- 使用される保留タイマーは、使用中のプローブ（トラックおよびIPSLA）の頻度およびタイムアウトと互換性がある必要があります。これにより、障害を時間内に検出できます。
- ノードの到達可能性に関連する構成は、特にしきい値カウント 1 が使用されている場合に、ノードが障害として検出されるのを避けるために、最初のサービスの起動またはセッションのかなり前に完了する必要があります。
- ノードは、保持されているノードを管理的に回復（シャットダウンおよび非シャットダウン）する前に、到達可能であると識別される必要があります。ノードの到達可能性は、トラックの状態を観察することで識別できます。
- ノードが管理上シャットダウンされている場合、またはデバイス グループ内またはノードに対して保留しきい値設定が使用されている場合、サービスはピア同期機能を使用しないことがあります。
- すべてのノードには、ノード レベルまたはデバイス グループ レベルのいずれかで、プロトコルまたはユーザー定義のプローブが必要です。
- 使用可能なスタンバイ ノードがない場合、サービスは fail-action メカニズムで構成する必要があります。
- ユーザー定義のトラックが ITD プロトコル プローブ メカニズムではなくデバイス グループで使用されている場合、ITD ノード メンテナンス モードまたはノード保留機能を使用できるように、ノード間またはデバイス グループ間でトラック識別子を共有しないことをお勧めします。
- Cisco NX-OS リリース 10.1(2) 以降、CoPP は N9K-C9364D-GX2A および N9K C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降、RACL は N9K-C9364D-GX2A および N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。

ITD サポート サマリー

ITD サポート レベルのリストについては、次の表を参照してください。

表 *1* : *ITD* サポート レベル

機能	ITDv4	ITDv6	説明
デバイス グループ レベル	• TCP • ICMP • HTTP • UDP • DNS	• TCPv6 • ICMPv3	Cisco NX-OS リリース 7.0(3)I7(3) で導入された ITDv6 Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX は、ICMP、TCP、および UDP プローブのみサポートします。
ノードごとのプローブ レベル	はい	○	
Hot-Standby	はい	○	Cisco NX-OS リリース 7.0(3)I7(3) で導入済み
重量	はい	○	
クラスタ	はい	○	Cisco NX-OS リリース 10.1(1) で導入済み
中断のない運用			
ACL リフレッシュ	はい	○	
プライマリ ノード	はい	○	
重みのあるプライマリ ノード	はい	○	Cisco NX-OS リリース 10.1(1) で導入済み
ホット スタンバイ ノード	いいえ	いいえ	
サービス レベル			
インクルード ACL	はい	○	

機能	ITDv4	ITDv6	説明
Failaction メソッド	• **reassign** • **least-bucket** • **node-per-bucket** • **bucket distribute**	• **reassign** • **least-bucket** • **node-per-bucket** • **bucket distribute**	Cisco NX-OS リリース 10.1(1) で導入された **drop-on-fail** オプションは、すべての failaction メソッドで使用できます。
除外-ACL	はい	○	拒否 ACE はサポートされていません。
サポートされるプラットフォーム	EX/FX ラインカードを搭載した Cisco Nexus 9500 スイッチ: X9788TC-FX、X97160YC-EX、および X9732C-EX。 Cisco Nexus 9236C、92304QC スイッチ、および 9300-EX シリーズ スイッチ Cisco Nexus C9336C-FX2-E および C93180YC-FX3 スイッチと Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カード。	Cisco Nexus 93180YC-EX、93108TC-EX、C93180YC-FX および C93108TC-FX スイッチ。 Cisco Nexus C9364C、C9336C-FX2、C93240YC-FX2 スイッチ。 Cisco Nexus C9336C-FX2-E および C93180YC-FX3 スイッチと Cisco Nexus X96136YC-R、X9636Q-R、X9636C-R、および X9636C-RX ライン カード。	

機能	ITDv4	ITDv6	説明
宛先 NAT	Cisco Nexus 93180YC-EX、93108TC-EX、C93180YC-FX、C93180YC-FX3S、C93108TC-FX3P、93108TC-FX、93240YC-FX2、C9336C-FX2、9300-GX、C9364D-GX2A、および C9332D-GX2B プラットフォームスイッチがサポートされています。	いいえ	
ITD over VXLAN	はい	いいえ	

ITD のデフォルト設定

次の表に、ITD パラメータのデフォルト設定を示します。

表 *2:* デフォルトの *ITD* パラメータ

パラメータ	デフォルト
プローブの頻度	10 秒
プローブの再試行ダウン カウント	3
プローブの再試行アップ カウント	3
プローブ タイムアウト	5 秒

ITD の構成

ITD のイネーブル化

ITD コマンドにアクセスする前に、ITD 機能を有効にする必要があります。

始める前に

ネットワーク サービス ライセンスがインストールされていることを確認してください。

ポリシーベース ルーティング（PBR）が有効になっていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **feature itd**
3. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature itd** 例： `switch(config)# feature itd`	ITD 機能をイネーブルにします。デフォルトでは、ITD は無効になっています。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デバイス グループの構成

ITD デバイス グループを作成してから、グループのノードとプローブを指定できます。Cisco NX-OS リリース 7.0(3)I3(1) 以降では、複数のデバイス グループを構成できます。

Cisco NX-OS リリース 10.1(1) 以降では、デバイス グループ内のノードをクラスタに追加できます。この場合、デバイス グループにはノード レベルのスタンバイ ノードまたはホット スタンバイ ノードがなく、failaction オプションが設定されています。 **fail-action bucket-distribute**

始める前に

ITD 機能がイネーブルであることを確認します。

デバイスが Cisco NX-OS リリース 7.0(3)I3(1) 以降を実行している場合は、次のコマンドが設定されていることを確認します。 **feature sla senderfeature sla responder**

手順の概要

1. **configure terminal**
2. [**no**] **itd device-group** *name*

3. **vrf** *vrf-name*
4. [**no**] **node {ip | ipv6} {***ipv4-address* | *ipv6-address***}**
5. [**no**] **probe** *track id*
6. [**no**] **weight** *weight*
7. [**no**] **cluster** *ID* **description** *description-string*
8. [**no**] **port** *port value*
9. [**no**] **mode hot-standby**
10. [**no**] **shutdown**
11. **exit**
12. ノードごとに手順 3 ～ 5 を繰り返します。
13. [**no**] **probe** {**icmp** | **http** | **tcp port** *port-number* | **udp port** *port-number* | **dns** [**frequency** *seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout** *seconds*]
14. [**no**] **hold-down threshold count <count> [time <time>]**
15. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **itd device-group** *name*
	例：
	`switch(config)# itd device-group dg1`
	`switch(config-device-group)#`
		ITD デバイス グループを作成し、デバイス グループ コンフィギュレーション モードを開始します。最大 32 文字の英数字を入力できます。

ステップ 3	**vrf** *vrf-name*
	例：
	`switch(config-device-group)# vrf vrf1`
	`switch(config-device-group)#`
		デバイス グループの VRF を構成します。詳細については、VRF のサポート （21 ページ）のセクションを参照してください。

ステップ 4	[**no**] **node {ip	ipv6} {***ipv4-address*	*ipv6-address***}**
			例：
			`switch(config-device-group)# node ip 20.20.20.3`
			`switch(config-dg-node)#`
			例：
			`switch(config-device-group)# node ipv6 2001::198:1:1:11`
			`switch(config-dg-node)#`
				ITD のノードを指定します。

ステップ 5	[**no**] **probe** *track id*
	例：
	`switch (config-device-group)# probe track 30`
	`switch(config-device-group-node)#`
		プローブのユーザー定義トラック ID を構成します。

	コマンドまたはアクション	目的
ステップ 6	[**no**] **weight** *weight* 例： `switch(config-dg-node)# weight 6`	ITD のノードの重みを指定します。有効な範囲は 1 ～ 256 です。

ステップ 7	[**no**] **cluster** *ID* **description** *description-string*
	例：
	`switch(config) # itd device-group dg1`
	`switch(config-device-group) # node ip 20.20.20.3`
	`switch(config-dg-node) # cluster 2 description C1`
	例：
	`switch(config)# itd device-group dg1`
	`switch(config-device-group) # node ipv6 2001::198:1:1:11`
	`switch(config-dg-node) # cluster 3 description C3`
		指定されたクラスタにノードを追加します。

ステップ 8	[**no**] **port** *port value*
	例：
	`switch(config-dg-node)# node ip 10.10.10.10`
	`port 1000`
		機能ポート アドレス変換のポート番号を指定します。値の範囲は 1 ～ 65535 です。

ステップ 9	[**no**] **mode hot-standby**
	例：
	`switch (config-device-group)# node ipv6 50::1`
	`switch(config-device-group-node)# mode hot-standby`
		ノードをデバイス グループのホット スタンバイ ノードとして構成します。

ステップ 10	[**no**] **shutdown**
	例：
	`switch(config-dg-node)# node ip 2.1.1.1`
	`switch(config-dg-node)# shutdown`
	`switch(config-dg-node)# no shutdown`
	`switch(config-dg-node)#`
		ノードをメンテナンス モードに移動または終了します。

ステップ 11	**exit**
	例：
	`switch(config-dg-node)# exit`
	`switch(config-device-group)#`
		デバイス グループ ノード コンフィグレーション モードを終了します。

ステップ 12	ノードごとに手順 3 ～ 5 を繰り返します。	
ステップ 13	[**no**] **probe** {**icmp** | **http** | **tcp port** *port-number* | **udp port** *port-number* | **dns** [**frequency** *seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout** *seconds*]	クラスタ グループのサービス プローブを構成します。

	コマンドまたはアクション	目的
	例： `switch(config-device-group)# probe icmp frequency 100`	Cisco NX-OS リリース 7.0(3)I3(1) 以降、ITD サービスのプローブとして次のプロトコルを指定できます。 • ICMP • [TCP] • [UDP] • HTTP • DNS 以前のリリースでは、ITDサービスのプローブとして ICMP が使用されていました。 オプションは次のとおりです。 • **frequency**：プローブの頻度を秒単位で指定します。値の範囲は 1 ～ 604800 です。 • **retry-down-count**：ノードがダウンしたときにプローブによって実行される再カウントの数を指定します。指定できる範囲は 1 ～ 5 です。 • **retry-up-count**：ノードが復帰したときにプローブが実行する再カウントの数を指定します。指定できる範囲は 1 ～ 5 です。 • **timeout**：タイムアウト期間を秒単位で指定します。値の範囲は 1 ～ 604800 です。

ステップ 14	**[no] hold-down threshold count <count> [time <time>]**
	例：
	`switch(config-itd)# itd device-group dg`
	`switch(config-device-group)# hold-down threshold count 1`
	`switch(config-device-group)# node ip 1.1.1.1`
	`switch(config-dg-node)# hold-down threshold count 3 time 200`
		ノードまたはデバイス グループの保留しきい値障害カウントとしきい値タイマーを指定します。

ステップ 15	（任意） **copy running-config startup-config** 例： `switch(config-device-group)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ITD サービスの構成

始める前に

ITD 機能がイネーブルであることを確認します。

ITD サービスに追加されるデバイス グループが構成されたことを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **itd** *service-name*
3. [**no**] **device-group** *device-group-name*
4. [**no**] **ingress interface** *interface*
5. [**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number* | **mask-position** *mask-position* | **least-bit**}
6. **[no] virtual [ip | ipv6] {** *ipv4-address ipv4-network-mask* **|** *ipv6-address ipv6-network-mask* **}**[{ **proto** {*port_num* | *port_any*}}] [{**advertise**} {**enable** | **disable**}] [device-group *dgrp_name*]
7. 次のいずれかのコマンドを入力して、ノード障害後にトラフィックを再割り当てする方法を決定します。
   - [**no**] **failaction node reassign** [**drop-on-fail**]
   - [**no**] **failaction node least-bucket** [**drop-on-fail**]
   - [**no**] **failaction bucket distribute** [**drop-on-fail**]
   - [**no**] **failaction node per-bucket** [**drop-on-fail**]
8. [**no**] **vrf** *vrf-name*
9. [**no**] **exclude access-list** *acl-name*
10. [**no**] **drop access-list** *acl-name*
11. （任意） [**no**] **peer local service** *peer-service-name*
12. **no shutdown**
13. （任意） **show itd** [*itd-name*]
14. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] **itd** *service-name*
	例：
	`switch(config)# itd service1`
	`switch(config-itd)#`
		ITD サービスを設定し、ITD 構成モードを開始します。最大 32 文字の英数字を入力できます。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **device-group** *device-group-name* 例： `switch(config-itd)# device-group dg1`	ITD サービスに既存のデバイス グループを追加します。*device-group-name* は、デバイス グループの名前を指定します。最大 32 文字の英数字を入力できます。 （注） Cisco NX-OS リリース 7.0(3)I3(1) 以降では、複数のデバイス グループを ITD サービスに追加できます。

ステップ 4	[**no**] **ingress interface** *interface*
	例：
	`switch(config-itd)# ingress interface ethernet 4/1-10`
	`switch(config-itd)# ingress interface Vni500001`
		ITDサービスに1つ以上のインターフェイスを追加します。
		複数のインターフェイスは、カンマを（「,」）を使用して区切ります。インターフェイスの範囲は、ハイフン（「-」）を使用して指定します。
		インターフェイスをサービスに関連付ける前に、必要なVRFおよびインターフェイス モードを設定します。

ステップ 5	[**no**] **load-balance** {**method** {**src** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*} | **dst** {**ip** | **ip-l4port** [**tcp** | **udp**] **range** *x y*}} | **buckets** *bucket-number* | **mask-position** *mask-position* | **least-bit**} 例： `switch(config-itd)# load-balance method src ip buckets 16`	ITD サービスのロード バランシング オプションを設定します。 オプションは次のとおりです。 • **method** ：送信先または接続先の IP アドレス ベースの負荷またはトラフィック分散を指定します。 • **buckets** ：作成するバケットの数を指定します。1 つ以上のバケットが 1 つのノードにマップされています。バケットは2のべき乗数で設定する必要があります。範囲は2～256です。 （注） 設定するバケットの数がノードの数より多い場合、バケットはすべてのノードにラウンドロビン方式で適用されます。 • **mask-position** ：ロードバランスのマスク位置を指定します。 • **least-bit**：最小ビットのロードバランス スキームを可能にします。このスキームにより、バケット生成メカニズムが連続する少数のクライアント IP プレフィクスを同じバケットに分配できるようにします。

	コマンドまたはアクション	目的
		• include-acl を使用するサービスの場合、最小ビット（マスク位置の有無にかかわらず）を使用して、同じバケットに分散する連続する IP ホストを減らします。 （注） マスク位置がバケット数と負荷分散モードに基づいて使用可能なビットを超えると、バケットの生成中に内部的にデフォルトで 0 になります。

ステップ 6	**[no] virtual [ip | ipv6] {** *ipv4-address ipv4-network-mask* **|** *ipv6-address ipv6-network-mask* **}**[{ **proto** {*port_num* | *port_any*} }] [{**advertise**} {**enable** | **disable**}] [device-group *dgrp_name*]
	例：
	`switch(config-itd)# virtual ip 100.100.100.100 255.255.255.255 udp 443 advertise enable active`
	例：
	`switch(config-itd)# virtual ipv6 100::100 128 udp 443`
		ITD サービスの仮想 IPv4 または IPv6 アドレスを設定します。
		proto オプション（TCP または UDP）は、仮想 IP アドレスが指定されたプロトコルからのフローを受け入れることを指定します。ポート範囲は 0 ～ 65535 です。
		[**advertise** {**enable** | **disable**}] オプションは、仮想 IP ルートを隣接デバイスにアドバタイズするかどうかを指定します。VIP アドバタイズ オプションが有効になっている場合、1つ以上のプライマリ ノードまたはホットスタンバイ ノードが仮想 IP またはサービスの下のデフォルトのデバイスグループに関連付けられたデバイスグループでアクティブになっている場合、ITD はルートを仮想 IP アドレスにアドバタイズします（該当する場合）。VIP アドバタイズ オプションを有効にするには、すべてのプライマリ ノードとホット スタンバイ ノードを、デバイス グループまたはノード レベルでプローブを介して追跡できる必要があります。
		（注） Cisco NX-OS リリース 9.3(2) 以降、**advertise** {**enable** | **disable**} [**active**] オプションは Warning（注意）を発行して [**advertise** {**enable** | **disable**}] オプションを使用します。

	コマンドまたはアクション	目的
		（注） Cisco NX-OS リリース 9.3(3) 以降、IPv6 ITD では、 **advertise enable** および **advertise enable active** オプションがサポートされています。 仮想 IP の複数のインスタンスは、同じ IP アドレスを持つサービスの下で構成できますが、ネットマスク（またはプレフィックス長）、プロトコル、またはポートが異なります。ユーザーは、トラフィック フローが意図したとおりに負荷分散できるように、仮想 IP、マスク プロトコル、およびポートの一致が一意であることを確認する必要があります。

ステップ 7	次のいずれかのコマンドを入力して、ノード障害後にトラフィックを再割り当てする方法を決定します。
	• [**no**] **failaction node reassign** [**drop-on-fail**]
	• [**no**] **failaction node least-bucket** [**drop-on-fail**]
	• [**no**] **failaction bucket distribute** [**drop-on-fail**]
	• [**no**] **failaction node per-bucket** [**drop-on-fail**]
	例：
	`switch(config-itd)# failaction node reassign`
	例：
	`switch(config-itd)# failaction node least-bucket`
	例：
	`switch(config-itd)# failaction bucket distribute`
	例：
	`switch (config-itd)# failaction node per-bucket [drop-on-fail]`
		サービスが使用する fail-action メカニズムを構成します。
		（注） このアルゴリズムは、比較的均等なトラフィック分散を目的としていますが、均等な分散を保証するものではありません。
		（注） **failaction bucket distribute** コマンドは、IPv4 と IPv6 の両方でサポートされています。
		（注） **drop-on-fail** オプションは、IPv4 と IPv6 の両方でサポートされています。

ステップ 8	[**no**] **vrf** *vrf-name* 例： `switch(config-itd)# vrf RED`	ITD サービスの VRF を指定します。
ステップ 9	[**no**] **exclude access-list** *acl-name* 例： `switch(config-itd)# exclude access-list acl1`	ITD が ITD ロードバランサから除外するトラフィックを指定します。

	コマンドまたはアクション	目的
ステップ 10	[**no**] **drop access-list** *acl-name* 例： `switch(config-itd)# drop access-list acl4`	ACL に一致するトラフィックをドロップします。
ステップ 11	（任意） [**no**] **peer local service** *peer-service-name* 例： `switch(config-itd)# peer local service service-A`	同じ（ローカル）スイッチ上にあるサンドイッチ モードの 2 つの ITD ピア サービスの 1 つを指定します。別の ITD サービスを作成し、このコマンドを使用して 2 番目の ITD ピア サービスを指定する必要があります。両方のサービスでこのコマンドを実行すると、ノードのヘルス ステータスが 2 つのサービス間で同期されます。 （注） 2 つのデバイス グループのノードは、同じ順序である必要があります。具体的には、順序が保持されるように、両方のデバイス グループの最初のエントリは同じサンドイッチ モード用である必要があります。
ステップ 12	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。
ステップ 13	（任意） **show itd** [*itd-name*] 例： `switch(config-itd)# show itd`	特定の ITD インスタンスのステータスおよび構成を表示します。
ステップ 14	（任意） **copy running-config startup-config** 例： `switch(config-itd)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ITD の構成例

以下に、ITD デバイス グループを設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# node ip 210.10.10.11
switch(config-dg-node)# weight 6
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.12
switch(config-dg-node)# weight 6
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.13
switch(config-dg-node)# weight 2
```

```
switch(config-dg-node)# exit
switch(config-device-group)# node ip 210.10.10.14
switch(config-dg-node)# weight 2
switch(config-dg-node)# exit
switch(config-device-group)# probe icmp
```

この例は、複数の ITD デバイス グループ（http_servers および telnet_servers）を構成する方法を示しています。仮想 IP アドレスはデバイス グループごとに構成され、負荷分散バケットは仮想 IP アドレスごとにあります。

```
switch(config)# itd device-group http_servers
  probe icmp
  node ip 10.10.10.9
  node ip 10.10.10.10

switch(config)# itd device-group telnet_servers
  probe icmp
  node ip 1.1.1.1
  node ip 1.1.1.2

switch(config)# itd test
virtual ip 40.1.1.100 255.255.255.255 tcp 23 device-group telnet_servers
virtual ip 30.1.1.100 255.255.255.255 tcp 80 device-group http_servers
  ingress interface Eth3/1
  no shut
```

この例は、入力ポート チャネル サブインターフェイスによるポリシーベース ルーティングの ITD サポートを示しています。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1.1
switch(config-itd)# device-group DG
switch(config-itd)# virtual ip 172.16.1.1 255.255.255.255
switch(config-itd)# no shutdown
```

この例は、（デバイス グループ レベルのプローブではなく）ノード レベルのプローブを構成する方法を示しています。ノードレベルのプローブを行う場合、それぞれのノードは自身のプローブで構成可能なため、ノードごとにさらにカスタマイズすることができます。

```
switch(config)# feature itd
switch(config)# itd device-group Servers
switch(config-device-group)# node ip 192.168.1.10
switch(config-dg-node)# probe icmp frequency 10 retry-down-count 5
switch(config-device-group)# node ip 192.168.1.20
switch(config-dg-node)# probe icmp frequency 5 retry-down-count 5
switch(config-device-group)# node ip 192.168.1.30
switch(config-dg-node)# probe icmp frequency 20 retry-down-count 3
```

この例は、接続先 NAT を構成する方法を示しています

```
Itd device-group <dg1>
probe icmp
node ip 1.1.1.1
node ip 2.2.2.2

Itd device-group <dg2>
probe icmp
node ip 3.3.3.3
node ip 4.4.4.4
```

```
Itd test1
device-group <dg1>
virtual ip 10.10.10.10 255.255.255.255 tcp 80
nat destination

Itd test2
device-group <dg2>
virtual ip 30.30.30.30 255.255.255.255 tcp 80
nat destination
switch(config)# sh nat itd
        ACL (Bucket_List)           Global_IP(Node_IP):Port    Local_IP(Virtual_IP):Port
    Protocol
-------------------------------+-------------------------+-------------------------+----------
ser1_itd_vip_1_bucket_1                    8.8.1.2:0                   6.6.1.1:101
         TCP
ser1_itd_vip_1_bucket_21                   8.8.1.2:0                   6.6.1.1:101
         TCP
ser1_itd_vip_1_bucket_2                    8.8.1.3:0                   6.6.1.1:101
         TCP
ser1_itd_vip_1_bucket_22                   8.8.1.3:0                   6.6.1.1:101
         TCP
```

ITD NAT および PAT の構成

```
feature itd


itd device-group dg1
  probe icmp
  node ip 10.10.10.10
    port 1000
  node ip 20.20.20.20
    port 2000
  node ip 30.30.30.30
    port 3000
  node ip 40.40.40.40
    port 4000


itd device-group dg2
  probe icmp
  node ip 10.10.10.11
  node ip 20.20.20.21
    port 2000
  node ip 30.30.30.31
    port 3000
  node ip 40.40.40.41
    port 4000


itd ser1
  virtual ip 6.6.6.1 255.255.255.255 tcp 80 advertise enable device-group dg1
  virtual ip 6.6.6.11 255.255.255.255 tcp 81 advertise enable device-group dg2
  ingress interface Eth1/1
  nat destination
  failaction node per-bucket
  load-balance method src ip buckets 64
  no shut
```

以下に、仮想 IPv4 アドレスを構成する例を示します。

```
switch(config)# feature itd
switch(config)# itd s4-101
switch(config-itd)# device-group dg_v4
switch(config-device-group)# ingress interface Vlan913
```

```
switch(config-device-group)# virtual ip 100.100.100.100 255.255.255.255 udp 443 advertise
 enable active
```

以下に、仮想 IPv6 アドレスを構成する例を示します。

この例は、トラフィックを比例的に分散するように加重ロードバランシングを構成する方法を示しています。この例では、ノード 1 と 2 は、ノード 3 と 4 の 3 倍のトラフィックを受け取ります。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# probe icmp
switch(config-device-group)# node ip 210.10.10.11
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 210.10.10.12
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
```

この例は、除外 ACL を構成して、ITD が ITD ロードバランサから除外するトラフィックを指定する方法を示しています。たとえば、ファイアウォールインスペクションを必要としない開発者 VLAN およびテスト ベッド VLAN は、ITD をバイパスできます。

```
switch(config)# feature itd
switch(config)# itd Service_Test
switch(config-itd)# device-group test-group
switch(config-itd)# ingress interface vlan10
switch(config-itd)# exclude access-list ITDExclude
switch(config-itd)# no shutdown

switch(config)# ip access-list ITDExclude
switch(config-acl)# 10 permit ip 5.5.5.0/24 any
switch(config-acl)# 20 permit ip 192.168.100.0/24 192.168.200.0/24
```

この例は、acl1 を作成して ITD サービスに割り当てる方法を示しています。**show** コマンドは、生成された IP アクセス リストとルートマップを表示します。

```
  switch(config)# ip access-list acl1
switch(config-acl)# 2460 permit tcp 100.1.1.0/24 any
switch(config-acl)# exit

switch(config)# itd test
switch(config-itd)# device-group dg1
switch(config-itd)# ingress interface Eth3/1
switch(config-itd)# load-balance method src ip
switch(config-itd)# access-list acl1
switch(config-itd)# show itd test
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   4

Exclude ACL
-------------------------------


Device Group                                        Probe  Port
```

```
------------------------------------------------ ----- ------
dg1                                               ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth3/1       UP       1

ACL Name/SeqNo                   IP/Netmask/Prefix            Protocol Port
-------------------------------- ---------------------------- -------- ----
acl1/2460                          100.1.1.0/24                 TCP      0

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- -------------- --- ---  -------
  1     1.1.1.1       Active   1  ICMP                      OK   2   10002
Bucket List
--------------------------------------------------------------------------
test_itd_ace_1_bucket_1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- -------------- --- --- -------
  2     1.1.1.2       Active   1  ICMP                      OK   3   10003

Bucket List
--------------------------------------------------------------------------
test_itd_ace_1_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- -------------- --- --- -------
  3     10.10.10.9    Active   1  ICMP                      OK   4   10004

Bucket List
--------------------------------------------------------------------------
test_itd_ace_1_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- -------------- --- --- -------
  4     10.10.10.10   Active   1  ICMP                      OK   5   10005

Bucket List
--------------------------------------------------------------------------
test_itd_ace_1_bucket_4
```

Cisco NX-OS リリース 7.0(3)I7(3) 以降、ITD は IPv6 をサポートします。この例は、acl を作成し、ITDv4 および ITDv6 サービスに割り当てる方法を示しています。**show** コマンドは、生成された IP アクセス リストとルートマップを表示します。

```
switch(config)# IPv6 access list acl6-101
switch(config-acl)# 10 permit udp 2405:200:1412:2000::/96 any
switch(config-acl)# exit
switch(config)# IP access list acl4-101
switch(config)# 10 permit tcp 10.0.0.0/10 any
switch(config-acl)# exit

switch(config-itd)# device-group dg6-101
switch(config-itd)# ingress interface Vlan913
switch(config-itd)# failaction node reassign
switch(config-itd)# load-balance method src ip
switch(config-itd)#  access-list ipv6 acl6-101
switch(config-itd)# no shut


switch(config-itd)# device-group dg4-101
switch(config-itd)#  ingress interface Vlan913
```

```
switch(config-itd)# failaction node reassign
switch(config-itd)# load-balance method src ip
switch(config-itd)#  access-list acl4-101
switch(config-itd)# no shut
```

この例では、ノード障害後に、障害が発生したノードバケットを、バケットの数が最も少ないアクティブ ノードに割り当てるように ITD サービスを構成する方法を示します。

```
switch(config-itd)# show run services

!Command: show running-config services
!Time: Thu Sep 22 22:22:01 2016

version 7.0(3)I5(1)
feature itd


itd session device-group dg


itd device-group dg
  probe icmp
  node ip 1.1.1.1
  node ip 2.2.2.2
  node ip 3.3.3.3


itd test
  device-group dg
  ingress interface Eth1/1
  failaction node least-bucket
  no shut



switch(config-itd)#

switch(config-itd)# show itd

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   4

Exclude ACL
--------------------------------


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
dg                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/1       UP       1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                      OK   2   10002
```

```
      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_1, 4

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ----- ----- --------------- -- --- -------
  2           2.2.2.2  Active   1 ICMP                       OK   3   10003

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ----- ----- --------------- -- --- -------
  3           3.3.3.3  Active   1 ICMP                       OK   4   10004

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_3


switch(config-itd)#


# Brought down Node 3, and the failed node buckets are send to Node 2.

switch# show itd

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   4

Exclude ACL
-------------------------------


Device Group                                        Probe  Port
-------------------------------------------------- ----- ------
dg                                                  ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/1       UP       1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ----- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                       OK   2   10002

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_1, 4

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ----- ----- --------------- -- --- -------
  2           2.2.2.2  Active   1 ICMP                       OK   3   10003

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
```

```
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.3.3.3  Active   1 ICMP                       PF   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3


switch#
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# end

switch#
```

この例では、ノード障害後に（1つのアクティブ ノードだけにではなく）使用可能なすべてのノードにトラフィックを均等に分散するようにITDサービスを構成する方法を示しています。

```
switch# show run services

!Command: show running-config services
!Time: Thu Sep 22 22:30:21 2016

version 7.0(3)I5(1)
feature itd


itd session device-group dg


itd device-group dg
  probe icmp
  node ip 1.1.1.1
  node ip 2.2.2.2
  node ip 3.3.3.3


itd test
  device-group dg
  ingress interface Eth1/1
failaction bucket distribute
  no shut



switch#

switch# show itd
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   4

Exclude ACL
--------------------------------


Device Group                                          Probe  Port
----------------------------------------------------- ----- ------
dg                                                     ICMP

Pool                           Interface    Status Track_id
```

```
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/1       UP       1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                      OK   2   10002

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1, 4

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2           2.2.2.2  Active   1 ICMP                      OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.3.3.3  Active   1 ICMP                      PF   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3
switch#
```

次の例は、ITD セッションを作成して、dg1 デバイス グループにノードを無停止で追加する方法を示しています。

```
switch(config)# feature itd
switch(config)# itd device-group dg1
switch(config-device-group)#   probe icmp
switch(config-device-group)#   node ip 1.1.1.1
switch(config-dg-node)#   node ip 2.1.1.1
switch(config-dg-node)#   node ip 3.1.1.1
switch(config-dg-node)#
switch(config-dg-node)# itd test
switch(config-itd)#   device-group dg1
switch(config-itd)#   ingress interface Eth1/11
switch(config-itd)#   load-balance method dst ip
Note: Configure buckets equal or more than the total number of nodes.

switch(config-itd)#   access-list acl1
switch(config-itd)#   no shut
switch(config-itd)# show itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
-------------------------------


Device Group                                        Probe  Port
-------------------------------------------------- ----- ------
dg1                                                 ICMP
```

```
Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/11      UP       2

ACL Name
--------------------------------
acl1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                       OK   3   10003
Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1, 4

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                       OK   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.1.1.1  Active   1 ICMP                       OK   5   10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3

switch(config-itd)# show run service
!Command: show running-config services
!Time: Tue Sep 20 20:36:04 2016
version 7.0(3)I5(1)
feature itd


itd device-group dg1
  probe icmp
  node ip 1.1.1.1
  node ip 2.1.1.1
  node ip 3.1.1.1
itd test
  device-group dg1
  ingress interface Eth1/11
  load-balance method dst ip
  access-list acl1
  no shut

switch(config-itd)# itd session device-group dg1
switch(config-session-device-group)# node ip 4.1.1.1
switch(config-session-dg-node)# commit
switch(config)# show itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
```

```
------------------------------
Device Group                                        Probe  Port
-------------------------------------------------- ----- ------
dg1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/11      UP       2

ACL Name
------------------------------
acl1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                       OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1
Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                       OK   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.1.1.1  Active   1 ICMP                       OK   5   10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  4           4.1.1.1  Active   1 ICMP                       OK   6   10006

      Bucket List
      ----------------------------------------------------------------------------
test_itd_bucket_4


switch(config)# show run service

!Command: show running-config services
!Time: Tue Sep 20 20:37:14 2016

version 7.0(3)I5(1)
feature itd


itd device-group dg1
  probe icmp
  node ip 1.1.1.1
node ip 2.1.1.1
  node ip 3.1.1.1
  node ip 4.1.1.1


itd test
```

```
  device-group dg1
  ingress interface Eth1/11
  load-balance method dst ip
  access-list acl1
  no shut
```

次の例は、ITD セッションを作成して、dg1 デバイス グループにノードを無停止で削除する方法を示しています。

```
switch(config)# feature itd
switch(config)#
switch(config)# itd device-group dg1
switch(config-device-group)#   probe icmp
switch(config-device-group)#   node ip 1.1.1.1
switch(config-dg-node)#   node ip 2.1.1.1
switch(config-dg-node)#   node ip 3.1.1.1
switch(config-dg-node)#   node ip 4.1.1.1
switch(config-dg-node)#
switch(config-dg-node)# itd test
switch(config-itd)#   device-group dg1
switch(config-itd)#   ingress interface Eth1/11
switch(config-itd)#   load-balance method dst ip
Note: Configure buckets equal or more than the total number of nodes.

switch(config-itd)#   access-list acl1
switch(config-itd)#   no shut

switch(config-itd)# show itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive
Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
--------------------------------


Device Group                                        Probe  Port
-------------------------------------------------- ----- ------
dg1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/11      UP       2

ACL Name
------------------------------
acl1
Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                      OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                      OK   4   10004

      Bucket List
```

```
      --------------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.1.1.1  Active   1 ICMP                       OK   5   10005

      Bucket List
      --------------------------------------------------------------------------------
test_itd_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  4           4.1.1.1  Active   1 ICMP                       OK   6   10006

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_bucket_4

switch(config-itd)# sh run service

!Command: show running-config services
!Time: Tue Sep 20 20:39:55 2016
version 7.0(3)I5(1)
feature itd


itd device-group dg1
  probe icmp
  node ip 1.1.1.1
  node ip 2.1.1.1
  node ip 3.1.1.1
  node ip 4.1.1.1


itd test
  device-group dg1
  ingress interface Eth1/11
  load-balance method dst ip
  access-list acl1
  no shut

switch(config-itd)# itd session device-group dg1
switch(config-session-device-group)# no node ip 4.1.1.1
switch(config-session-device-group)# commit
switch(config)# show itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
--------------------------------


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
dg1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
```

```
test_itd_pool                  Eth1/11      UP       2

ACL Name
------------------------------
acl1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                       OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                       OK   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
3           3.1.1.1  Active   1 ICMP                      OK   5   10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3, 4


switch(config)# show run service

!Command: show running-config services
!Time: Tue Sep 20 20:41:07 2016

version 7.0(3)I5(1)
feature itd
itd device-group dg1
  probe icmp
  node ip 1.1.1.1
  node ip 2.1.1.1
  node ip 3.1.1.1


itd test
  device-group dg1
  ingress interface Eth1/11
  load-balance method dst ip
  access-list acl1
  no shut
```

次の例は、ITDセッションを作成して、重みを持つノードを無停止で追加し、既存のノードの重みを変更し、dg1 デバイス グループからノードを削除する方法を示しています。

```
switch(config)# sh itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
```

```
test           src-ip     ACTIVE   n/a

Source Interface
----------------

Device Group                                          Probe  Port
------------------------------------------------- ----- ------

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
                               Eth1/3       UP       1

ACL Name                           Buckets
--------------------------------------------------------------------------------
APP1                             8

  Device Group
  ------------------------------------------------------------------------------
  dg1


  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  1                1.1.1.3             Active   1 ICMP                       OK   3
10003

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_2, 1

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  2                1.1.1.4             Active   1 ICMP                       OK   4
10004

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_3, 6

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                1.1.1.5             Active   1 ICMP                       OK   5
10005

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_4, 5

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                1.1.1.2             Active   1 ICMP                       OK   2
10010

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_8, 7
```

```
ACL Name                            Buckets
--------------------------------------------------------------------------------
APP2                               8

  Device Group
  --------------------------------------------------------------------------------
  dg2


  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  1                2.1.1.1             Active   1 ICMP                       OK   6
10006

      Bucket List
      --------------------------------------------------------------------------
      test_itd_acl_1_bucket_1, 6

  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  2                2.1.1.2             Active   1 ICMP                       OK   7
10007

      Bucket List
      --------------------------------------------------------------------------
      test_itd_acl_1_bucket_2, 7

  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                2.1.1.3             Active   1 ICMP                       OK   8
10008

      Bucket List
      --------------------------------------------------------------------------
      test_itd_acl_1_bucket_3, 8

  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                2.1.1.4             Active   1 ICMP                       OK   9
10009

      Bucket List
      --------------------------------------------------------------------------
      test_itd_acl_1_bucket_4, 5

switch(config)# show run services

!Command: show running-config services
!Running configuration last done at: Sun Nov 15 12:09:30 2020
!Time: Sun Nov 15 12:15:10 2020

version 9.4(1) Bios:version N/A
feature itd

itd device-group dg1
  probe icmp frequency 1 timeout 1
```

```
  node ip 1.1.1.3
  node ip 1.1.1.4
  node ip 1.1.1.5
  node ip 1.1.1.2

itd device-group dg2
  probe icmp frequency 1 timeout 1
  node ip 2.1.1.1
  node ip 2.1.1.2
  node ip 2.1.1.3
  node ip 2.1.1.4

itd test
  ingress interface Eth1/3
  failaction node least-bucket
  load-balance method src ip
  access-list APP1 device-group dg1
  access-list APP2 device-group dg2
  no shut

switch(config)# itd session device-group dg1
switch(config-session-device-group)# node ip 1.1.1.5
switch(config-session-dg-node)# weight 2
switch(config-session-dg-node)# node ip 1.1.1.4
switch(config-session-dg-node)# weight 3
switch(config-session-dg-node)# node ip 1.1.1.6
switch(config-session-dg-node)# weight 2
switch(config-session-dg-node)# no node ip 1.1.1.2
switch(config-session-device-group)# commit
switch(config)# sh itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   n/a

Source Interface
----------------


Device Group                                        Probe  Port
-------------------------------------------------- ----- ------


Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
                               Eth1/3       UP       1

ACL Name                          Buckets
--------------------------------------------------------------------------------
APP1                               8

  Device Group
  ------------------------------------------------------------------------------
  dg1


  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  1                1.1.1.3             Active   1 ICMP                       OK   3
```

```
10003

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ----------------------- ---------- ------- --- ----- ------ --------------- -- ---
-------
  2                1.1.1.4             Active   3 ICMP                       OK   4
10004

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_3, 6, 7

  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ----------------------- ---------- ------- --- ----- ------ --------------- -- ---
-------
  3                1.1.1.5             Active   2 ICMP                       OK   5
10005

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_4, 5

  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ----------------------- ---------- ------- --- ----- ------ --------------- -- ---
-------
  4                1.1.1.6             Active   2 ICMP                       PF  10
10011

      Bucket List
      ------------------------------------------------------------------------
      test_itd_bucket_8, 1
ACL Name                          Buckets
--------------------------------------------------------------------------------
APP2                             8

  Device Group
  ------------------------------------------------------------------------------
  dg2


  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ----------------------- ---------- ------- --- ----- ------ --------------- -- ---
-------
  1                2.1.1.1             Active   1 ICMP                       OK   6
10006

      Bucket List
      ------------------------------------------------------------------------
      test_itd_acl_1_bucket_1, 6

  Node  IP                Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ----------------------- ---------- ------- --- ----- ------ --------------- -- ---
-------
  2                2.1.1.2             Active   1 ICMP                       OK   7
10007
```

```
      Bucket List
      --------------------------------------------------------------------------------
      test_itd_acl_1_bucket_2, 7

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                 2.1.1.3             Active   1 ICMP                       OK   8
10008

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_acl_1_bucket_3, 8

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                 2.1.1.4             Active   1 ICMP                       OK   9
10009

      Bucket List
      --------------------------------------------------------------------------------
      test_itd_acl_1_bucket_4, 5

switch(config)# sh run services

!Command: show running-config services
!Running configuration last done at: Sun Nov 15 12:17:19 2020
!Time: Sun Nov 15 12:18:16 2020

version 9.4(1) Bios:version N/A
feature itd

itd device-group dg1
  probe icmp frequency 1 timeout 1
  node ip 1.1.1.3
    weight 1
  node ip 1.1.1.4
    weight 3
  node ip 1.1.1.5
    weight 2
  node ip 1.1.1.6
    weight 2

itd device-group dg2
  probe icmp frequency 1 timeout 1
  node ip 2.1.1.1
  node ip 2.1.1.2
  node ip 2.1.1.3
  node ip 2.1.1.4

itd test
  ingress interface Eth1/3
  failaction node least-bucket
  load-balance method src ip
  access-list APP1 device-group dg1
  access-list APP2 device-group dg2
  no shut
```

この例は、ITD セッションを介してマルチ インクルード ACL を使用してノードをサービスに無停止で追加する方法を示しています。この例では、デバイス グループとマルチ インクルード ACL がすでに構成されています。

```
switch(config)# sh run services

!Command: show running-config services
!Running configuration last done at: Sun Nov 15 12:05:44 2020
!Time: Sun Nov 15 12:07:42 2020

version 9.4(1) Bios:version N/A
feature itd

itd device-group dg1
  probe icmp frequency 1 timeout 1
  node ip 1.1.1.3
  node ip 1.1.1.4
  node ip 1.1.1.5

itd device-group dg2
  probe icmp frequency 1 timeout 1
  node ip 2.1.1.1
  node ip 2.1.1.2
  node ip 2.1.1.3
  node ip 2.1.1.4

itd test
  ingress interface Eth1/3
  failaction node least-bucket
  load-balance method src ip
  access-list APP1 device-group dg1
  access-list APP2 device-group dg2
  no shut

switch(config)# sh itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   n/a

Source Interface
-----------------

Device Group                                        Probe  Port
-------------------------------------------------- ----- ------

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
                               Eth1/3       UP       1

ACL Name                           Buckets
--------------------------------------------------------------------------------
APP1                                 8

  Device Group
  --------------------------------------------------------------------------------
  dg1


  Node  IP                 Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
```

```
Sla_id
  ------------------------- ----------- -------- --- ---- ----- ---------------- -- ---
-------
  1                 1.1.1.3             Active   1 ICMP                         OK   3
10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2, 1, 8

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ----------- -------- --- ---- ----- ---------------- -- ---
-------
  2                 1.1.1.4             Active   1 ICMP                         OK   4
10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3, 6, 7

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ----------- -------- --- ---- ----- ---------------- -- ---
-------
  3                 1.1.1.5             Active   1 ICMP                         OK   5
10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_4, 5
ACL Name                            Buckets
--------------------------------------------------------------------------------
APP2                               8

  Device Group
  ------------------------------------------------------------------------------
  dg2


  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ----------- -------- --- ---- ----- ---------------- -- ---
-------
  1                 2.1.1.1             Active   1 ICMP                         OK   6
10006

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_1, 6

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ----------- -------- --- ---- ----- ---------------- -- ---
-------
  2                 2.1.1.2             Active   1 ICMP                         OK   7
10007

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_2, 7

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
```

```
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                2.1.1.3             Active   1 ICMP                        OK   8
10008

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_3, 8

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                2.1.1.4             Active   1 ICMP                        OK   9
10009

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_4, 5

switch(config)# itd test
switch(config-itd)# itd session device-group dg1
switch(config-session-device-group)# node ip 1.1.1.2
switch(config-session-dg-node)# commit
switch(config)# sh itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           src-ip     ACTIVE   n/a

Source Interface
----------------

Device Group                                        Probe  Port
-------------------------------------------------- ----- ------

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
                               Eth1/3       UP       1

ACL Name                           Buckets
--------------------------------------------------------------------------------
APP1                             8

  Device Group
  ------------------------------------------------------------------------------
  dg1


  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  1                1.1.1.3             Active   1 ICMP                        OK   3
10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2, 1

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
```

```
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  2                 1.1.1.4             Active   1 ICMP                        OK   4
10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3, 6

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                 1.1.1.5             Active   1 ICMP                        OK   5
10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_4, 5

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                 1.1.1.2             Active   1 ICMP                        OK   2
10010

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_8, 7
ACL Name                            Buckets
--------------------------------------------------------------------------------
APP2                               8

  Device Group
  ------------------------------------------------------------------------------
  dg2


  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  1                 2.1.1.1             Active   1 ICMP                        OK   6
10006

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_1, 6

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  2                 2.1.1.2             Active   1 ICMP                        OK   7
10007

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_2, 7

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
```

```
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  3                2.1.1.3             Active   1 ICMP                        OK   8
10008

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_3, 8

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------ ---------- ------- --- ---- ----- --------------- -- ---
-------
  4                2.1.1.4             Active   1 ICMP                        OK   9
10009

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_acl_1_bucket_4, 5

switch(config)# sh run services

!Command: show running-config services
!Running configuration last done at: Sun Nov 15 12:09:30 2020
!Time: Sun Nov 15 12:10:18 2020

version 9.4(1) Bios:version N/A
feature itd

itd device-group dg1
  probe icmp frequency 1 timeout 1
  node ip 1.1.1.3
  node ip 1.1.1.4
  node ip 1.1.1.5
  node ip 1.1.1.2

itd device-group dg2
  probe icmp frequency 1 timeout 1
  node ip 2.1.1.1
  node ip 2.1.1.2
  node ip 2.1.1.3
  node ip 2.1.1.4

itd test
  ingress interface Eth1/3
  failaction node least-bucket
  load-balance method src ip
  access-list APP1 device-group dg1
  access-list APP2 device-group dg2
  no shut
```

次の例は、ACE をインクルード ACL に中断することなく追加する方法を示しています。

```
switch(config)#
switch(config-acl)# ip access-list acl1
switch(config-acl)# 1010 permit tcp any 10.220.0.0/16
switch(config-acl)# 1020 permit tcp any 20.1.1.0/24

switch(config)# show ip access-lists acl1

IP access list acl1
        1010 permit tcp any 10.220.0.0/16
        1020 permit tcp any 20.1.1.0/24

switch(config)# itd device-group dg1
```

```
switch(config-device-group)#   probe icmp
switch(config-device-group)#   node ip 1.1.1.1
switch(config-dg-node)#   node ip 2.1.1.1
switch(config-dg-node)#   node ip 3.1.1.1
switch(config-dg-node)#   node ip 4.1.1.1

switch(config-dg-node)# itd test
switch(config-itd)#   device-group dg1
switch(config-itd)#   ingress interface Eth1/11
switch(config-itd)#   load-balance method dst ip
Note: Configure buckets equal or more than the total number of nodes.

switch(config-itd)#   access-list acl1
switch(config-itd)#   no shut

switch(config)# show run service

!Command: show running-config services
!Time: Tue Sep 20 20:44:17 2016

version 7.0(3)I5(1)
feature itd


itd device-group dg1
  probe icmp
  node ip 1.1.1.1
  node ip 2.1.1.1
  node ip 3.1.1.1
  node ip 4.1.1.1


itd test
  device-group dg1
ingress interface Eth1/11
  load-balance method dst ip
  access-list acl1
  no shut

switch(config-itd)# ip access-list acl1
switch(config-acl)# 1030 permit tcp any 30.1.1.0/24
switch(config-acl)# exit
switch(config)# itd session access-list acl1 refresh
switch(config)# sh ip access-lists | grep n 4 itd_
IP access list test_itd_bucket_1
        1010 permit tcp any 10.220.0.0 0.0.63.255
        1020 permit tcp any 20.1.1.0 0.0.0.63
        1030 permit tcp any 30.1.1.0/26
IP access list test_itd_bucket_2
        1010 permit tcp any 10.220.64.0 0.0.63.255
        1020 permit tcp any 20.1.1.64 0.0.0.63
        1030 permit tcp any 30.1.1.64/26
IP access list test_itd_bucket_3
        1010 permit tcp any 10.220.128.0 0.0.63.255
        1020 permit tcp any 20.1.1.128 0.0.0.63
1030 permit tcp any 30.1.1.128/26
IP access list test_itd_bucket_4
        1010 permit tcp any 10.220.192.0 0.0.63.255
        1020 permit tcp any 20.1.1.192 0.0.0.63
        1030 permit tcp any 30.1.1.192/26
switch(config)# sh run rpm
interface Ethernet1/11
  ip policy route-map test_itd_pool
```

この例では、アクセス リストが適切に生成され、予想される ip 一致条件があることを確認します。Cisco Nexus リリース 9.3(3)F 以降では、show **ip access-list dynamic** コマンドを使用してシステム内の ACL を検索できます。

```
Nexus# show ip access-lists CiscoService_itd_vip_1_bucket_1 dynamic

IP access list CiscoService_itd_vip_1_bucket_1
        10 permit ip 1.1.1.0 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_2 dynamic

IP access list CiscoService_itd_vip_1_bucket_2
        10 permit ip 1.1.1.32 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_3 dynamic

IP access list CiscoService_itd_vip_1_bucket_3
        10 permit ip 1.1.1.64 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_4 dynamic

IP access list CiscoService_itd_vip_1_bucket_4
        10 permit ip 1.1.1.96 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_5 dynamic

IP access list CiscoService_itd_vip_1_bucket_5
        10 permit ip 1.1.1.128 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_6 dynamic

IP access list CiscoService_itd_vip_1_bucket_6
        10 permit ip 1.1.1.160 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_7 dynamic

IP access list CiscoService_itd_vip_1_bucket_7
        10 permit ip 1.1.1.192 255.255.255.31 192.168.255.1/32
513E-A-15-C9336C-FX-2-1# show ip access-lists CiscoService_itd_vip_1_bucket_8 dynamic

IP access list CiscoService_itd_vip_1_bucket_8
        10 permit ip 1.1.1.224 255.255.255.31 192.168.255.1/32
```

次の例は、インクルード ACL から ACE を中断なく削除する方法を示しています。

```
switch(config)# feature itd

switch(config-acl)# ip access-list acl1
switch(config-acl)# 1010 permit tcp any 10.220.0.0/16
switch(config-acl)# 1020 permit tcp any 20.1.1.0/24
switch(config-acl)# 1030 permit tcp any 30.1.1.0/24

switch(config)# itd device-group dg1
switch(config-device-group)#   probe icmp
switch(config-device-group)#   node ip 1.1.1.1
switch(config-dg-node)#   node ip 2.1.1.1
switch(config-dg-node)#   node ip 3.1.1.1
switch(config-dg-node)#   node ip 4.1.1.1
switch(config-dg-node)#
switch(config-dg-node)# itd test
switch(config-itd)#   device-group dg1
switch(config-itd)#   ingress interface Eth1/11
switch(config-itd)#   load-balance method dst ip
Note: Configure buckets equal or more than the total number of nodes.

switch(config-itd)#   access-list acl1
switch(config-itd)#   no shut


switch(config-acl)# sh itd test
```

```
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
-------------------------------
Device Group                                        Probe  Port
-------------------------------------------------- ----- ------
dg1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/11      UP       2

ACL Name
-------------------------------
acl1


  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                       OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1
Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                       OK   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  3           3.1.1.1  Active   1 ICMP                       OK   5   10005

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  4           4.1.1.1  Active   1 ICMP                       OK   6   10006

      Bucket List
      ----------------------------------------------------------------------------
test_itd_bucket_4

switch(config)# show itd test

Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive
Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
test           dst-ip     ACTIVE   4

Exclude ACL
-------------------------------
```

```
Device Group                                          Probe  Port
------------------------------------------------ ----- ------
dg1                                                   ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
test_itd_pool                  Eth1/11      UP       2

ACL Name
------------------------------
acl1
Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  1           1.1.1.1  Active   1 ICMP                      OK   3   10003

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_1

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  2           2.1.1.1  Active   1 ICMP                      OK   4   10004

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_2

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  3           3.1.1.1  Active   1 ICMP                      OK   5   10005

      Bucket List
      ----------------------------------------------------------------------------
test_itd_bucket_3

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------ ------- --- ---- ----- --------------- -- --- -------
  4           4.1.1.1  Active   1 ICMP                      OK   6   10006

      Bucket List
      ----------------------------------------------------------------------------
      test_itd_bucket_4

switch(config)# sh run rpm
```

次の例は、ITD over VXLAN を構成する方法を示しています。

```
switch(config)# sh itd brief

Legend:
C-S(Config-State):A-Active,S-Standby,F-Failed
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets  Interface
-------------- ---------- -------- -------  -----------
ser1           src-ip     ACTIVE   256      VLAN100,Eth1/1

Source Interface
-------------------------------
loopback9
VRF-Name
-------------------------------Org1:vrf1
```

```
Device Group                                        Probe  Port
------------------------------------------------- ----- ------
sf
Virtual IP                    Netmask/Prefix   Protocol   Port
------------------------------ ------------     -------- ---------
6.6.6.1 / 255.255.255.0                          IP        0

Node      IP              Cfg-S      WGT   Probe    Port     Probe-IP   STS
  ------------------      -------   ----   -----    ------  ---------   --
  1       10.200.1.2      Active     1                                  OK
  2       10.200.6.2      Active     1                                  OK
```

次の例は、vPC のバケット配布を使用して ITD NAT を構成する方法を示しています。

```
itd device-group dg
probe icmp
node ip 10.10.10.2
node ip 11.11.11.2
node ip 12.12.12.2
node ip 13.13.13.2
itd test
device-group dg
virtual ip 20.20.20.20.255.255.255.255 tcp 80 advertise enable
ingress interface Eth1/9
nat destination
failaction bucket distribute
load-balance buckets 16
no shut
```

次の例は、vPC の fail-action バケット配布の出力を示しています。

```
switch# show itd brief
Legend:
C-S(Conftg-State): A-Act1ve.S-Standby.F-Failed
ST(Status): ST-Standby.lF-L1nk Failed.PF-Probe Failed, PD-Peer Down, IA-
SH-Shut, HD-Hold-down
Name             LB Scheme     Status     Buckets Interface
---------------- ---------------- ---------- -------- --------
test             src-lp         ACTIVE       16     Ethl/9
Source Interface
-------------------------------------------------------------------
Device Group               Probe       Port         VRF
------------------------- ----------- ------------ -------------
dg
Virtual IP        Netmask/Prefix       Protocol     Port
------------- --------------------- ------------ ----------
20.20.20.20 /     255.255.255.255       TCP         80
Node     IP       Cluster-id C-S WGT Probe Port Porbe-IP  STS
----------------- ---------- --- ---- ---- ---- -------- ------
1       10.10.10.11           A   1   ICMP                OK
2       10.10.10.12           A   1   ICMP                OK
3       10.10.10.11           A   1   ICMP                OK
4       10.10.10.12           A   1   ICMP                OK

switch# show itd test statistics
Service         Device Group         VIP/mask                      #Packets
-------------------------------------------------------------------------------
test               dg             20.20.20.20 / 255.255.255.255   5662755(100.00%)
Traffic Bucket            Assigned to   Mode    Original Node #Packets
------------------------- ----------- --------- -------------  ----------
test_itd_vip_2_bucket_1  10.10.10.2   Redirect  10.10.10.2     2015671 (35.60%)
Traffic Bucket            Assigned to   Mode     Original Node #Packets
------------------------- ----------- --------- -------------  ----------
test_itd_vip_2_bucket_2  11.11.11.2   Redirect   11.11.11.2    1539347 (27.18%)
```

```
Traffic Bucket            Assigned to   Mode    Original Node   #Packets
------------------------ ----------- --------- -------------  ---------
test_itd_vip_2_bucket_3   12.12.12.2   Redirect  12.12.12.2    1192501 (21.06%)
Traffic Bucket            Assigned to   Mode    Original Node   #Packets
-----------------------  -----------    -------   -------------  ---------
test_itd_vip_2_bucket_4   13.13.13.2   Redirect  13.13.13.2     915236 (16.16%)

Return Traffic from Node                   #Packets
------------------------------     --------------------------------
10.10.10.2                                 2180262 (38.39%)
11.11.11.2                                 1560862 (27.49%)
12.12.12.2                                 1117360 (19.68%)
13.13.13.2                                  820226 (14.44%)
                            Total packets: 5678710 (100.00%)
switch#
```

次の例は、バケット配布を使用して ITD ノード レベル スタンバイを構成する方法を示しています。

```
itd device-group dg
probe icmp
node ip 10.10.10.2
standby ip 13.13.13.2
node ip 11.11.11.2
standby ip 12.12.12.2
node ip 12.12.12.2
standby ip 11.11.11.2
node ip 13.13.13.2
standby ip 10.10.10.2
itd test
device-group dg
virtual ip 20.20.20.20.255.255.255.255 tcp 80 advertise enable
ingress interface Eth1/9
failaction bucket distribute
load-balance buckets 16
no shut
```

次の例は、バケット配布を使用した ITD ノード レベル スタンバイの出力を示しています。

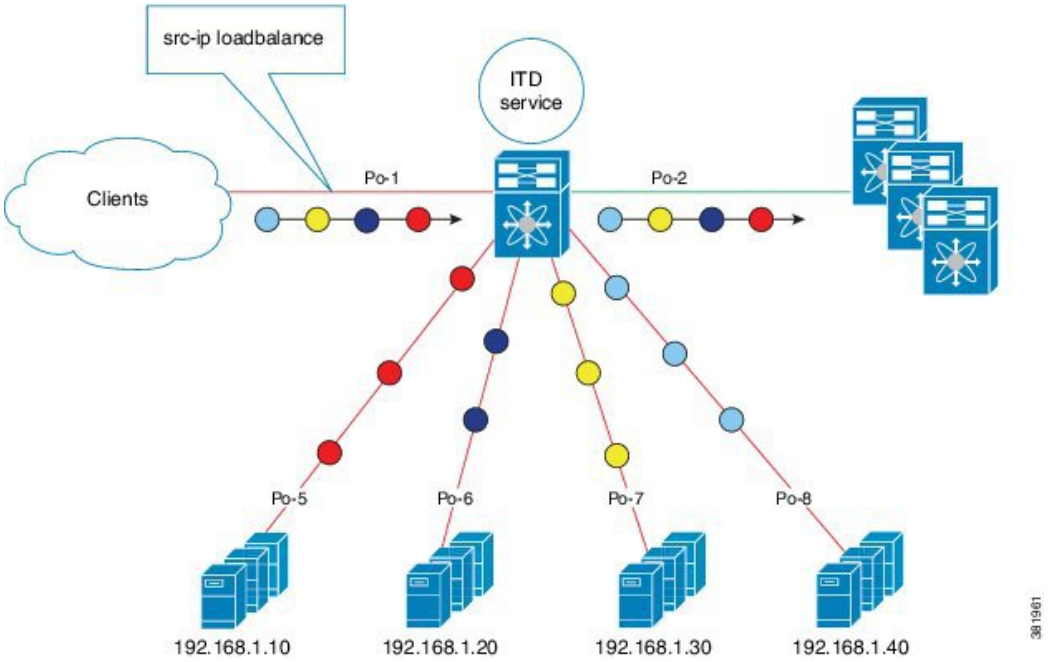
```
switch# show itd brief
Legend:
C-S(Conftg-State): A-Act1ve.S-Standby.F-Failed
ST(Status): ST-Standby.lF-L1nk Failed.PF-Probe Failed, PD-Peer Down, IA-
SH-Shut, HD-Hold-down
Name              LB Scheme       Status    Buckets Interface
--------------- ---------------- ---------- -------- ---------
test              src-lp           ACTIVE     16     Eth1/9

Source Interface
-------------------------------------------------------------------
Device Group                 Probe       Port         VRF
------------------------- ----------- ------------ -------------
Dg                           ICMP
Virtual IP         Netmask/Prefix     Protocol       Port
---------------------------------- ------------ -----------
20.20.20.20 / 255.255.255.255           TCP           80

Node       IP     Cluster-id C-S WGT Probe Port  Porbe-IP STS
-----  ---------- ---------- --- ---- ---- ---- -------- ------
1       10.10.10.11           A   1   ICMP                OK
        13.13.13.2                                ST
2       10.10.10.12           A   1   ICMP                OK
        12.12.12.2                                ST
3       10.10.10.11           A   1   ICMP                OK
```

```
        11.11.11.2                              ST
4       10.10.10.12           A    1    ICMP                 OK
        10.10.10.2                              ST
```

構成例：ワンアーム展開モード

以下の構成は次の図のトポロジを使用します。

図 *15:* ワンアーム展開モード



ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

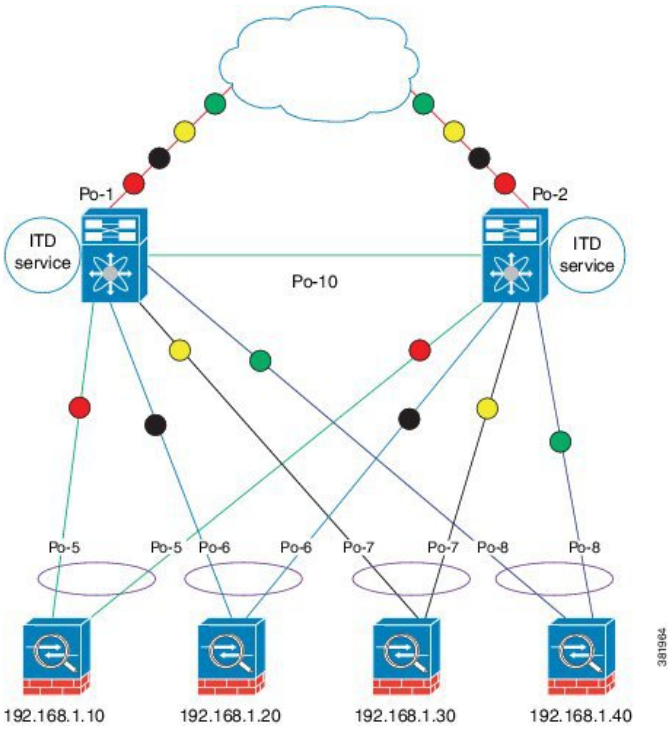
ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

構成例：vPC でのワンアーム展開モード

以下の構成は次の図のトポロジを使用します。

図 *16 : VPC* でのワンアーム展開モード



デバイス 1

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

デバイス2

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
```

```
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

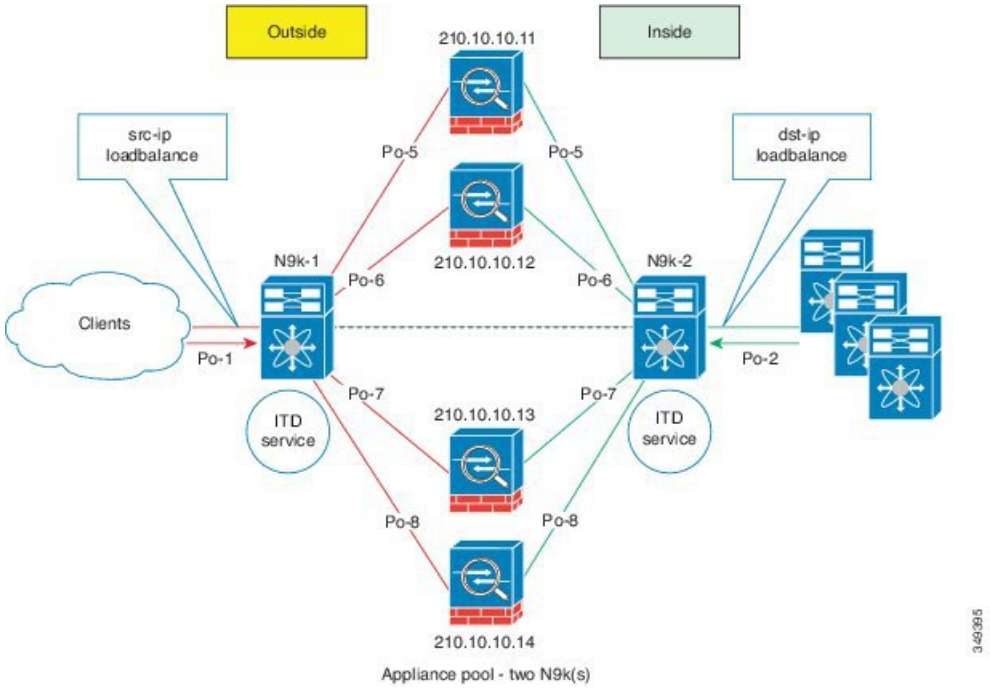
ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

構成例：サンドイッチ展開モード

以下の構成は次の図のトポロジを使用します。

図 *17:* サンドイッチ展開モード



デバイス 1

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 210.10.10.11
switch(config-device-group)# node ip 210.10.10.12
switch(config-device-group)# node ip 210.10.10.13
switch(config-device-group)# node ip 210.10.10.14
switch(config-device-group)# probe icmp
```

ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# load-balance method src ip
switch(config-itd)# no shutdown
```

デバイス2

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 220.10.10.11
switch(config-device-group)# node ip 220.10.10.12
switch(config-device-group)# node ip 220.10.10.13
switch(config-device-group)# node ip 220.10.10.14
switch(config-device-group)# probe icmp
```

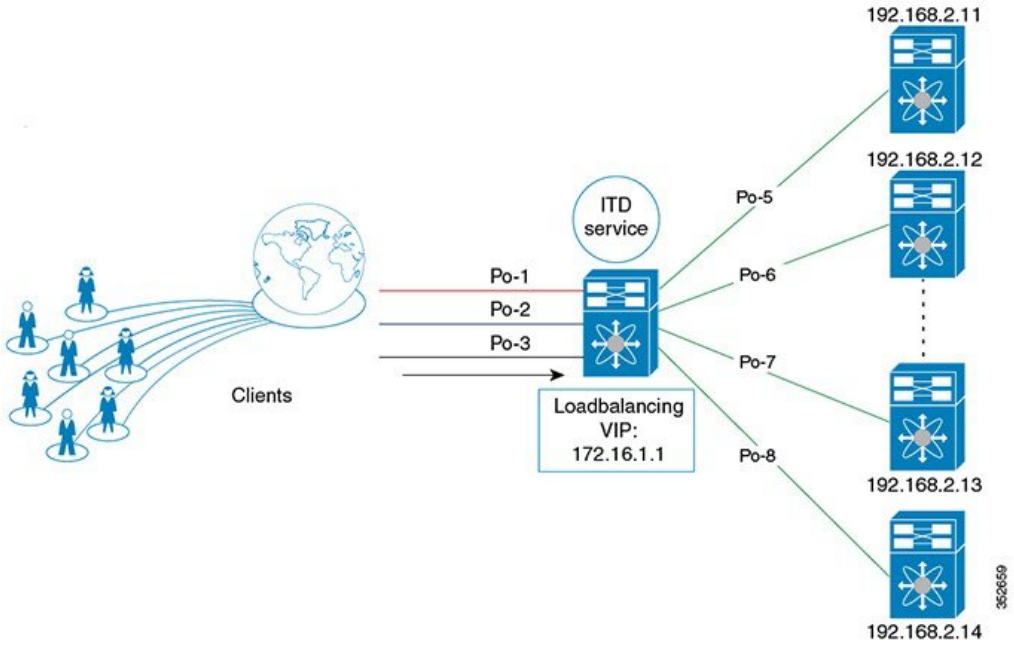
ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# device-group DG
switch(config-itd)# load-balance method dst ip
switch(config-itd)# no shutdown
```

構成例：サーバー ロードバランシング展開モード

以下の構成は次の図のトポロジを使用します。

図 *18 : VIP* を使用した *ITD* 負荷分散



ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group DG
switch(config-device-group)# node ip 192.168.2.11
switch(config-device-group)# node ip 192.168.2.12
switch(config-device-group)# node ip 192.168.2.13
switch(config-device-group)# node ip 192.168.2.14
switch(config-device-group)# probe icmp
```

ステップ 2：ITD サービスを定義します。

```
switch(config)# itd HTTP
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# ingress interface port-channel 2
switch(config-itd)# ingress interface port-channel 3
switch(config-itd)# device-group DG
Switch(config-itd)# virtual ip 172.16.1.1 255.255.255.255
switch(config-itd)# no shutdown
```

構成例：WCCP として ITD を再配置する（Web プロキシ展開モード）

プロキシサーバーは、他のサーバーからのリソースを求めるクライアントからの要求の仲介として機能します。Web プロキシサーバーは、特にローカル ネットワークとインターネット間の仲介役として機能します。通常、Web プロキシサーバーでは、ネットワーク デバイスがインターネットに向かう Web トラフィックを自分にリダイレクトする必要があります（転送フロー）。ただし、後続のパケット転送では、ネットワーク デバイスがパケットを定期的に転送するだけで済みます。

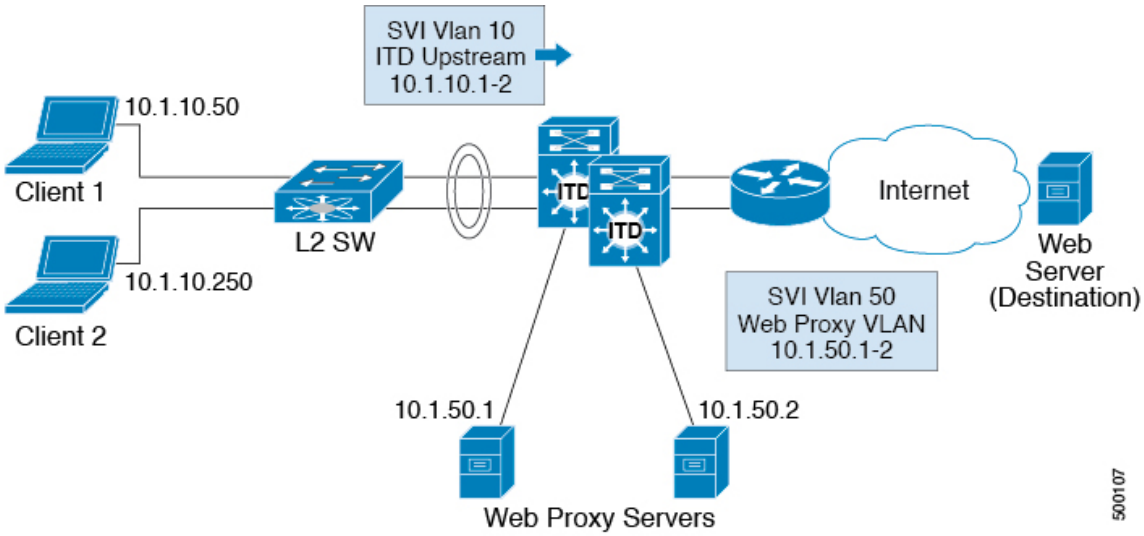
ITD を使用した Web プロキシ展開では、スイッチはインターネットに向かう Web トラフィックを照合し、プロキシサーバーに向けて負荷を分散します。プロキシサーバーは自律モード（WCCP から独立してアクティブ-アクティブ）で動作し、プロキシサーバーにリダイレクトされるトラフィックを処理します。ITD を介して実行されるノード ヘルス プローブは、ノードの状態を追跡し、可用性に基づいて適切にノードを削除または追加するという目的を果たします。スタンバイ サーバーは、冗長性のためにグループ レベルまたはノード レベルで構成することもできます。

ITD リダイレクションは、通常、クライアント側 VLAN の順方向でのみ必要です。その後、パケットは ITD リダイレクションまたは配布なしでルーティングまたは転送されます。このような Web プロキシ展開を使用する ITD には、順方向用に構成された 1 つの ITD サービスのみが必要です。ただし、送信元レイヤ 4 ポートに基づいてトラフィックを選択して、リバース トラフィック リダイレクションが必要です。LB パラメータを逆にして、フローの対称性も維持する必要があります。

Web プロキシ展開の ITD では、ITD プローブを使用して Web プロキシサーバーの可用性をチェックします。これは、障害が発生したプロキシサーバーに送信されたトラフィックが失われるため重要です。

以下の構成は次の図のトポロジを使用します。

図 *19 : Web* プロキシ展開モード



この例では、インターネットへの宛先ポート 80/443（入力 VLAN 10）が Web プロキシサーバー 10.1.50.1 および 10.1.50.2 に配布されます。プライベートネットワーク（10.0.0.0/8、192.168.0.0/16、172.16.0.0/12）宛ての VLAN 10 上のトラフィックは、プロキシに送信されません。

ステップ 0：アクセスリストの構成

```
ip access-list ACL1
  10 permit ip any any tcp 80
  20 permit ip any any tcp 443
```

ステップ 1：ITD デバイス グループの Web プロキシサーバーを設定し、サーバーの IP アドレスを指定します。

```
itd device-group Web_Proxy_Servers
  probe icmp
  node ip 10.1.50.1
  node ip 10.1.50.2
```

ステップ 2：プライベート IP アドレス宛てのすべてのトラフィックを除外するように除外 ACL を構成します。

```
ip access-list itd_exclude_ACL
  10 permit ip any 10.0.0.0/8
  20 permit ip any 192.168.0.0/16
  30 permit ip any 172.16.0.0/12
```

ステップ 3：除外 ACL を適用します。

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_ACL
  access-list ACL1
  ingress interface Vlan 10
  failaction node reassign
  load-balance method src ip
  no shutdown
```

なんらかの理由でリターントラフィックのリダイレクトも必要な場合は、次の追加の構成手順が必要です。

（注） レイヤ 4 範囲演算子を使用したポート フィルタリングのみが可能です。また、除外 ACL は許可エントリのみをサポートします。

ステップ 4：ポート 80 と 443 を除くすべてを除外するように、リターン除外 ACL を構成します。

```
ip access-list itd_exclude_return
  10 permit tcp any range 0 79 any
  20 permit tcp any range 81 442 any
  30 permit tcp any range 444 65535 any
```

ステップ 5：リターン トラフィックのリターン ITD サービスを構成し、除外 ACL を適用します。

```
Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_return
  ingress interface Vlan 20   <- Internet-facing ingress interface on the Nexus switch
  failaction node reassign
  load-balance method dst ip  <- Flow symmetry between forward/return flow achieved by
flipping the LB parameter
  no shutdown
```

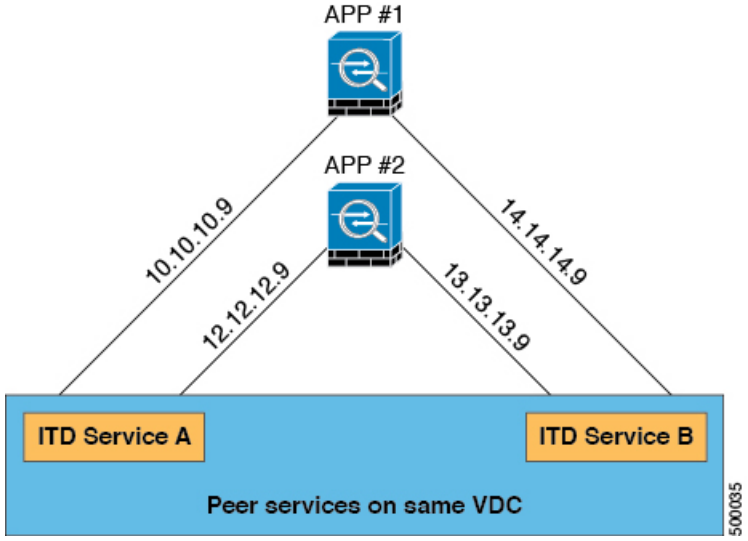
構成例：サンドイッチ モード向けピア同期

ITD ピア サービス上のサンドイッチ アプライアンスへのリンクがダウンすると、サービスはノードへのリンクがダウンしていることを示す通知をピアに送信します。次に、ピア サービスはリンクをダウンさせ、トラフィックがそのリンクを通過しないようにします。

ピア同期なしで、ITD サービス A のアプライアンス APP #1 に接続されているリンクが次のトポロジでダウンし、ITD サービス B に通知されない場合、サービス B は引き続き APP #1 にトラフィックを送信し、トラフィックはドロップされます。

以下の構成では、このトポロジを使用します。

図 *20* : サンドイッチ モードのピア同期



デバイス 1

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group dev-A
switch(config-device-group)# node ip 10.10.10.9 ---> Link to app #1
switch(config-device-group)# node ip 12.12.12.9 ---> Link to app #2
switch(config-device-group)# probe icmp
```

ステップ 2：ピア同期を有効にして ITD サービスを定義します。

```
switch(config)# itd service-A
switch(config-itd)# device-group dev-A
switch(config-itd)# ingress interface ethernet 7/4
switch(config-itd)# peer local service service-B
switch(config-itd)# no shutdown

switch(config-itd)# show itd
Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------
Service-A      ICMP  src-ip     ACTIVE   2

Device Group                                        VRF-Name
--------------------------------------------------- -------------
Dev-A


Route Map                      Interface    Status Track_id
------------------------------ ------------ ------ ---------
Service-A_itd_pool             Eth7/45      UP       3

  Node  IP                 Config-State Weight Status     Track_id  Sla_id
  ------------------------ ------------ ------ ---------- --------- ---------
  1     10.10.10.9         Active       1      Peer Down    1         10001

        IP Access List
```

```
      ------------------------------------------------------------------------
      Service-A_itd_bucket_0


  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  2     12.12.12.9        Active       1      OK           2         10002

      IP Access List
      ------------------------------------------------------------------------
      Service-A_itd_bucket_1
```

デバイス2

ステップ 1：デバイス グループを定義します。

```
switch(config)# itd device-group dev-B
switch(config-device-group)# node ip 14.14.14.9 ---> Link to app #1
switch(config-device-group)# node ip 13.13.13.9 ---> Link to app #2
switch(config-device-group)# probe icmp
```

ステップ 2：ピア同期を有効にして ITD サービスを定義します。

```
switch(config)# itd service-B
switch(config-itd)# device-group dev-B
switch(config-itd)# ingress interface ethernet 7/45
switch(config-itd)# peer local service service-A
switch(config-itd)# no shutdown

switch(config-itd)# show itd
Name           Probe LB Scheme  Status   Buckets
-------------- ----- ---------- -------- -------
Service-B      ICMP  src-ip     ACTIVE   2

Device Group                                        VRF-Name
-------------------------------------------------- -------------
Dev-B


Route Map                      Interface    Status Track_id
------------------------------ ------------ ------ ---------
Service-B_itd_pool             Eth7/45      UP       3

  Node  IP                Config-State Weight Status       Track_id  Sla_id
  ----------------------- ------------ ------ ----------   --------- ---------
  1     14.14.14.9        Active       1      Probe Failed    3        10003

      IP Access List
      ------------------------------------------------------------------------
      Service-B_itd_bucket_0


  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  2     13.13.13.9        Active       1      OK           4         10004

      IP Access List
      ------------------------------------------------------------------------
      Service-B_itd_bucket_1
```

構成例：スティックのファイアーウォール

ITD サービス

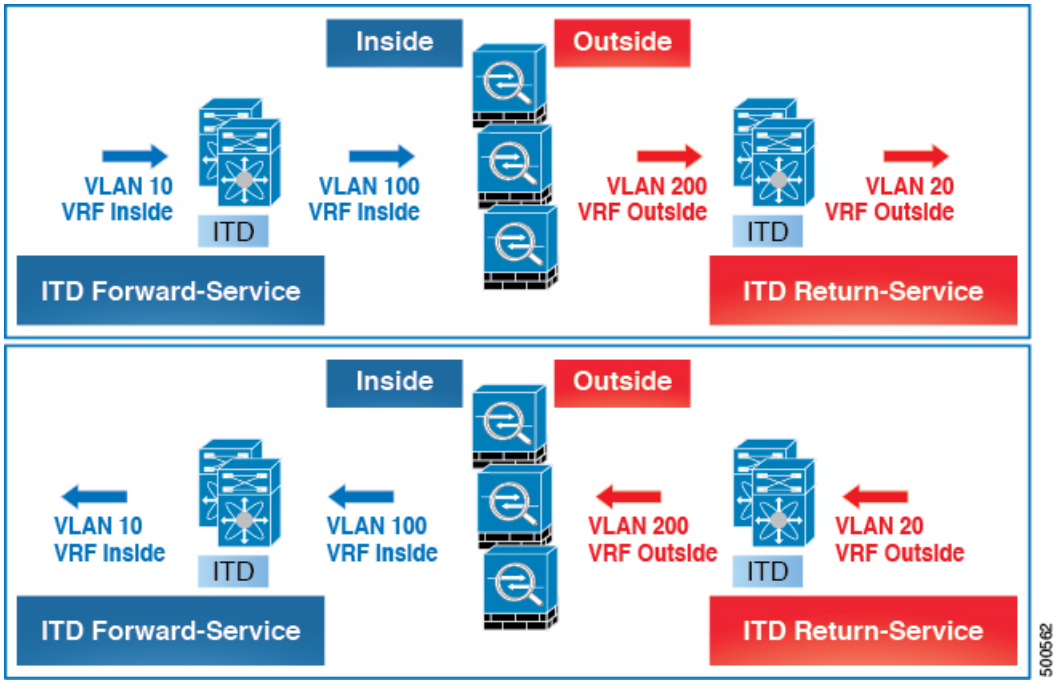
ITD サービス構成は、トラフィック フローの特定の方向に対する ITD トラフィック分散を定義します。フローの両方向をリダイレクトする必要がある場合は、2 つの ITD サービスを設定する必要があります。1 つは転送トラフィック フロー用、もう 1 つはリターン トラフィック フロー用です。ASA には異なる内部インターフェイスと外部インターフェイスの IP アドレスがあるため、2 つの異なるデバイス グループも、対応する内部および外部 IP アドレスを指すように構成する必要があります。

ASA VLAN

ITD 転送およびリターン サービスは、Nexus スイッチの内部および外部 VLAN SVI に接続されます。ファイアウォールなどのセキュリティアプリケーションはすべてのトラフィックを検査する必要があるため、サービスでトラフィックフィルタリングは構成されません。その結果、SVI に到達するトラフィックはすべて、対応する ASA インターフェイスにリダイレクトされます。

ASA インターフェイスがスイッチの VLAN と同じ VLAN で構成されている場合、ファイアウォールからスイッチに向かうトラフィックは、スイッチの別の VLAN に ITD サービスが存在するため、ASA にリダイレクトされます。したがって、ファイアウォールと Nexus スイッチ間のトラフィック ループを防止するには、個別の VLAN のペアが必要です。

図 *21 : ITD ASA* の展開



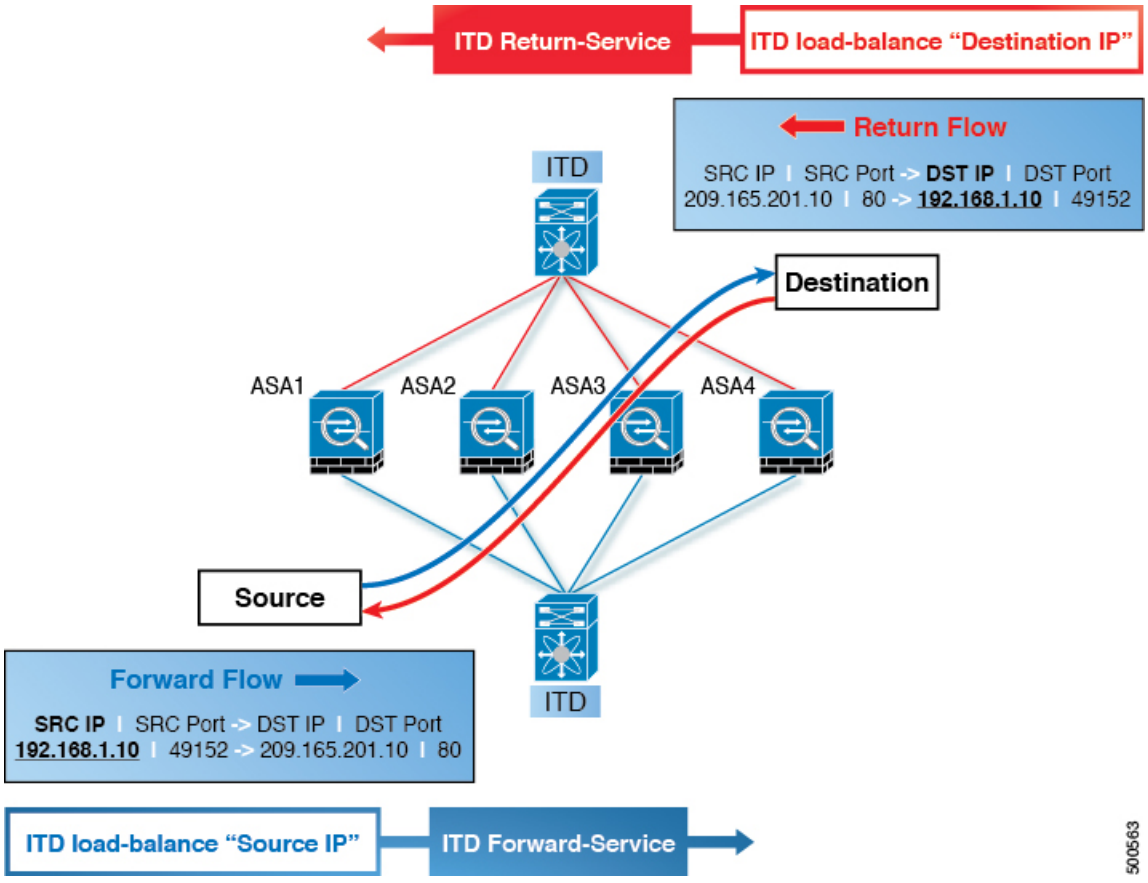
この図は、VLAN 10 および 20 を、ネットワーク上の送信元および接続先への内部および外部インターフェイスとして示しています。VLAN 100 および 200 は、ループのないトラフィックを確保するために ASA に対して使用されます。

フローの対称性

ファイアウォールは通常、順方向と戻り方向の両方のトラフィック フローを検査します。インスペクションのステートフルな性質により、通常、クラスタ化されていないファイアウォールの通常の操作中にフローの対称性を維持する必要があります。クラスタ化されたファイアウォールの場合でも、トラフィック フローの非対称性により、クラスタ制御リンクを介したフローのリダイレクトが増加します。非対称フローが増えると、ファイアウォールに不要なオーバーヘッドが追加され、パフォーマンスが低下します。

フローの対称性は、固有の IP 永続性と ITD アルゴリズムの決定論的性質を使用して実現できます。ファイアウォールの一般的な ITD 構成では、転送フローに 1 つの ITD サービスを使用し、リターン フローに 1 つの ITD サービスを使用します。ロード バランス パラメータの値が両方のサービスで同じになるようにこれら 2 つの ITD サービスを設定すると、フローの対称性が確実に維持されます。

図 *22 : ITD ASA* 展開におけるフローの対称性

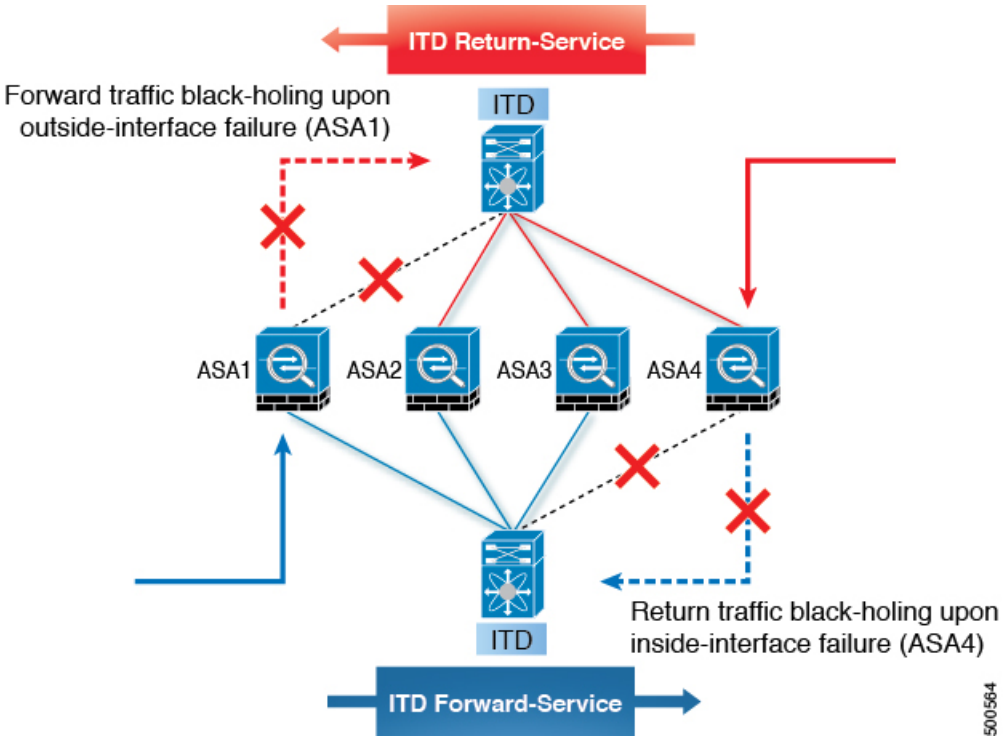


この図は、順方向フローの送信元 IP アドレスと逆方向フローの宛先 IP アドレスがどのように一定であるかを示しています。各 ITD サービスに適切なパラメータを選択すると、ITD IP の永続性によるフローの対称性が保証されます。

Link Failures

ASA の内部または外部インターフェイスに障害が発生すると、トラフィックの出力インターフェイスがダウンしているため、その ASA の反対側に着信するトラフィックが失われる可能性があります。ITD ピア スイッチ ノード状態同期機能は、ASA のリモート側を ITD から削除し、スイッチ間でノード状態を同期することにより、この問題を解決できます。

図 *23 : ASA* 障害シナリオ

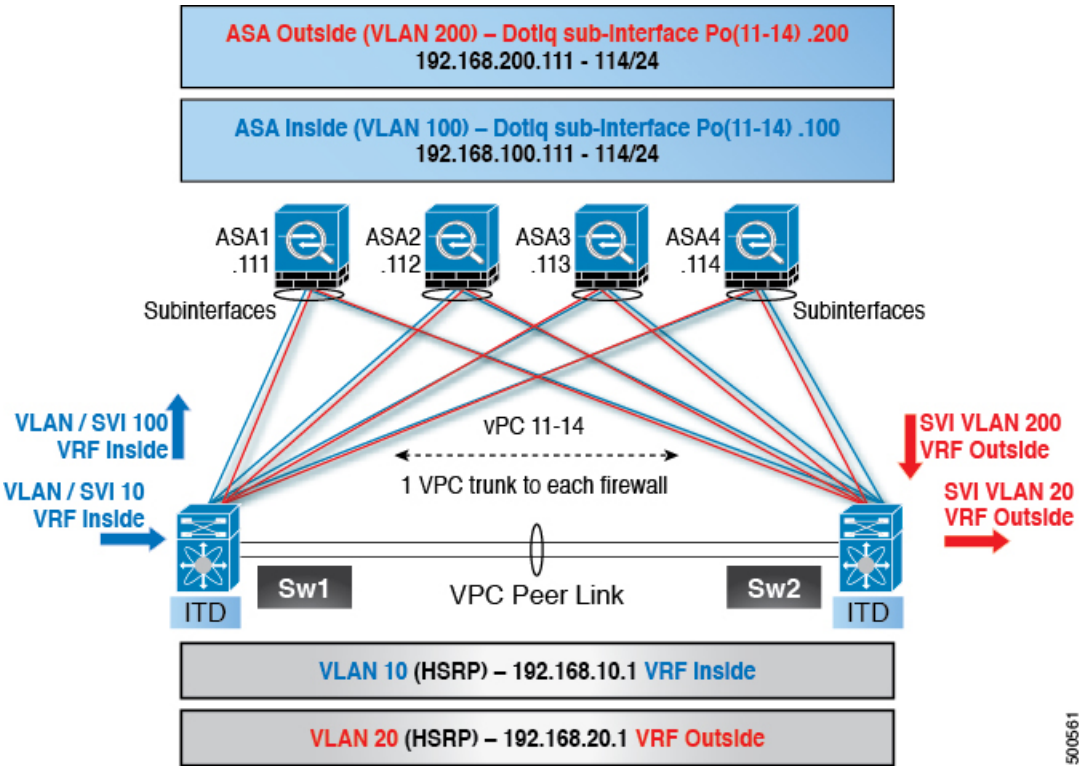


ITD ピア スイッチ ノード状態同期機能は、デュアル スイッチの非 vPC（またはシングル スイッチ）トポロジでのみサポートされます。ASA クラスタリングは、このような障害が発生した場合に ASA が完全に停止することを保証するため、この問題も解決します。ファイアウォール オン スティックの実装（シングル リンクまたは vPC）では、この問題に対処できません。これは、ASA の内部インターフェイスと外部インターフェイスが同じ物理（または仮想）インターフェイスに属しているためです。

設定例

スティック展開のファイアウォールでは、通常、vPC ポート チャネル（または単一ポート）トランクを使用して ASA をスイッチに接続します。この設定では、内部インターフェイスと外部インターフェイスは dot1q サブインターフェイス（VLAN 100 および 200）であり、スイッチには内部および外部コンテキストにそれぞれ 2 つの VLAN または SVI があり、それらの間で物理ポートが分離されていません。

図 *24 :* スティック（*vPC* を使用）展開のファイアウォール



ステップ 1：スイッチの構成

（注） この例は、スイッチ Sw1 の構成の一部を示しています。構成は、同様にすべての ASA に向けて適切に拡張する必要があります。他の機能は、すでに構成されていると想定されます。

```
interface vlan 10
  description Inside_Vlan_to_Network
  vrf member INSIDE
  ip address 192.168.10.10/24
  hsrp 10
    ip address 192.168.10.1

interface vlan 20
  description Outside_Vlan_to_Network
  vrf member OUTSIDE
  ip address 192.168.20.10/24
  hsrp 20
    ip address 192.168.20.1

interface vlan 100
  description Inside_Vlan_to_ASA
  vrf member INSIDE
  ip address 192.168.100.10/24
  hsrp 100
    ip address 192.168.100.1

interface vlan 200
```

```
  description Outside_Vlan_to_ASA
  vrf member OUTSIDE
  ip address 192.168.200.10/24
  hsrp 200
    ip address 192.168.200.1

interface port-channel 11
  description VPC_TO_ASA1
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  vpc 11
  no shutdown

interface ethernet 4/25
  description Link_To_ITD-ASA-1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100,200
  channel-group 11 mode active
  no shutdown

interface port-channel 41
  description Downstream_vPC_to_network
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  vpc 41
  no shutdown

interface ethernet 5/1-4
  description Downstream_vPC_member
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20
  channel-group 41
  no shutdown


itd device-group FW_INSIDE
    #Config Firewall Inside interfaces as nodes
  node ip 192.168.100.111
  node ip 192.168.100.112
  node ip 192.168.100.113
  node ip 192.168.100.114
probe icmp frequency 5 timeout 5 retry-count 1

itd device-group FW_OUTSIDE
    #Config Firewall Outside interfaces as nodes
  node ip 192.168.200.111
  node ip 192.168.200.112
  node ip 192.168.200.113
  node ip 192.168.200.114
probe icmp frequency 5 timeout 5 retry-count 1

itd INSIDE
  vrf INSIDE
    #applies ITD service to VRF 'INSIDE'
  device-group FW_INSIDE
    #FW inside interfaces attached to service.
  ingress interface vlan 10
    #applies ITD route map to vlan 1101 interface
  failaction node reassign
    #To use the next available Active FW if an FW goes offline
  load-balance method src ip buckets 16
    #distributes traffic into 16 buckets
```

```
    #load balances traffic based on Source IP.
    #OUTSIDE service uses Dest IP.
  no shut

itd OUTSIDE
  vrf OUTSIDE
    #applies ITD service to VRF 'OUTSIDE'
  device-group FW_OUTSIDE
  ingress interface vlan 20
  failaction node reassign
  load-balance method dst ip buckets 16
    #load balances traffic based on Dest IP.
    #INSIDE service uses Src IP.
  no shut
```

ステップ 2：ASA の構成。

```
interface port-channel 11
  nameif aggregate
  security-level 100
  no ip address

interface port-channel 11.100
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 11.200
  description OUTSIDE
  vlan 200
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level
```

このトポロジ例には、次の点が当てはまります。

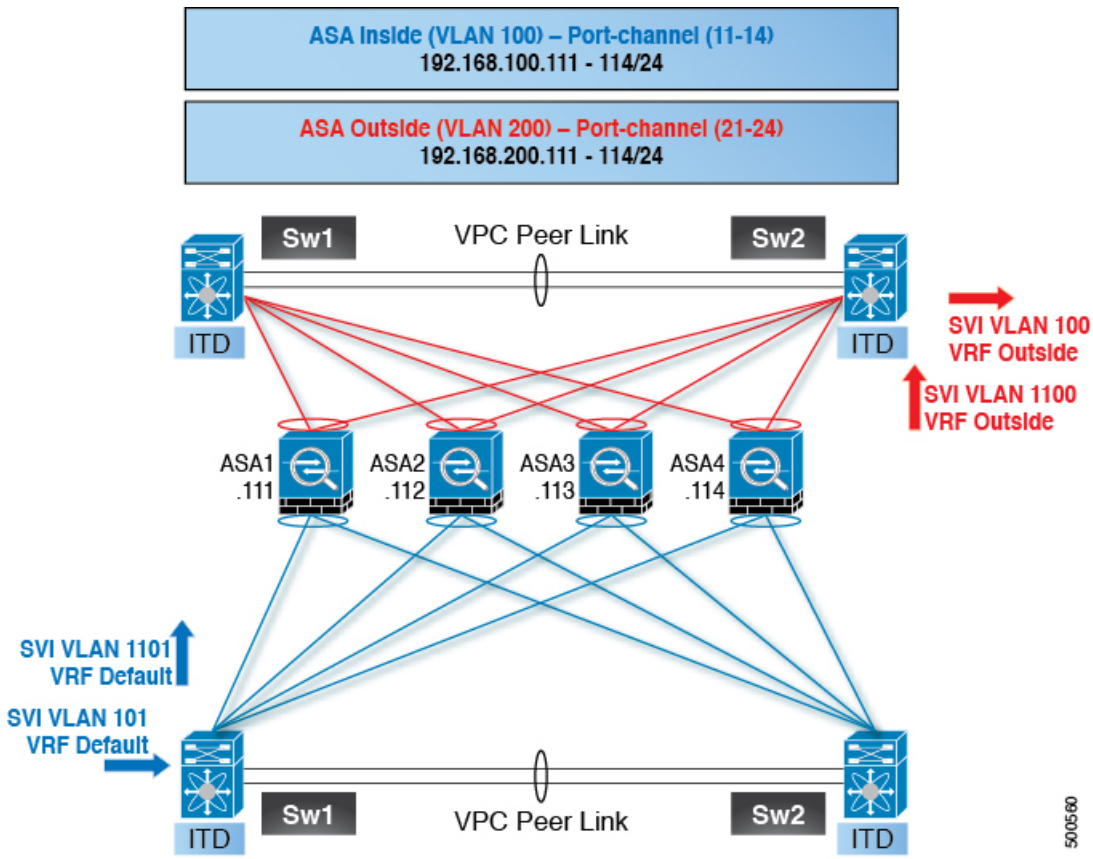
- VLAN 10、20、100、および 200 とそれらの SVI は、適切な VRF にマッピングされます。
- この例では、ITD ロードバランシング設定を使用してフローの対称性を実現しています。
- vPC シナリオでは、vPC の 1 つのメンバーが稼働している限り、ITD に変更はありません。vPC レッグに障害が発生したスイッチの ITD リダイレクションは、通常の vPC 配置の場合と同様に、ピア リンクを介してピア スイッチを通過します。

- このトポロジでは、内部インターフェイスと外部インターフェイスが ASA の同じ物理インターフェイスまたは仮想インターフェイス（dot1q サブインターフェイス）に結び付けられているため、物理リンクの障害時にトラフィックが失われることはありません。
- vPC 上のルーティング プロトコル ネイバーをサポートするには、layer3 peer-router コマンドを vPC ドメイン内で構成する必要があります。
- レイヤ3インターフェイスはファイアウォールの内側と外側の両方のインターフェイスに接続するために使用されるため、VRF が必要です。VRF は、特定の場合にトラフィックがファイアウォールを迂回して（VLAN間）ルーティングされるのを防ぐために配置されます。
- トラフィックはポリシーベース ルーティングを使用して ASA に向けられるため、ルートは必要ありません。

構成例：vPC を使用したデュアル スイッチ サンドイッチ モードのファイアウォール

vPC を使用したサンドウィッチ モードの場合、内部および外部 ASA インターフェイスはそれぞれ別のポート チャネル バンドルに割り当てられます。vPC の結果として、単一のリンク障害がトラフィック フローを妨げることはなく、ITD は引き続きピア スイッチのリンクを介して ASA に転送します。

図 *25 : vPC* を使用したデュアル スイッチ サンドイッチ モード



ステップ 1：2 つのスイッチを構成します。

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24

interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

ステップ 2：ASA の構成。

```
interface port-channel 11
  description INSIDE
  vlan 100
  nameif inside
  security-level 100
  ip address 192.168.100.111 255.255.255.0

interface port-channel 21
  description OUTSIDE
  vlan 100
  nameif outside
  security-level 100
  ip address 192.168.200.111 255.255.255.0

same-security-traffic permit inter-interface

interface TenGigabitEthernet 0/6
```

```
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/7
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 11 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/8
  description CONNECTED_TO_SWITCH-A-VPC
  channel-group 21 mode active
  no nameif
  no security-level

interface TenGigabitEthernet 0/9
  description CONNECTED_TO_SWITCH-B-VPC
  channel-group 21 mode active
  no nameif
  no security-level
```

このトポロジ例には、次の点が当てはまります。

- この例では、ITD ロードバランシング設定を使用してフローの対称性を実現しています。
- vPC シナリオでは、vPC の 1 つのメンバーが稼働している限り、ITD に変更はありません。vPC レッグに障害が発生したスイッチの ITD リダイレクションは、通常の vPC 配置の場合と同様に、ピア リンクを介してピア スイッチを通過します。
- このトポロジでは、ASA のポート チャネルの 1 つ（または非 vPC トポロジの単一の物理リンク）に障害が発生すると、トラフィック損失が発生する可能性があります。
- vPC 上のルーティング プロトコル ネイバーをサポートするには、layer3 peer-router コマンドを vPC ドメイン内で構成する必要があります。
- トラフィックはポリシーベース ルーティングを使用して ASA に向けられるため、ルートは必要ありません。

構成例：レイヤ 3 クラスタリングのファイアウォール

ASA クラスタは、1 つのユニットとして機能する複数の ASA から構成されます。複数の ASA を単一論理デバイスとしてグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。

ITD は、個々のモードのレイヤ 3 ASA クラスタにロードバランシングできます。ITD はクラスタリングを補完するものであり、ITD は各ファイアウォールによってどのフローが処理されるかを予測できるようにします。OSPF ECMP およびポート チャネル ハッシュ アルゴリズムに依存する代わりに、ITD バケットを使用してこれらのフローを決定できます。

レイヤ3クラスタでは、バケット割り当てに基づいてフローの所有者を事前に決定できます。ITD およびレイヤ 3 クラスタリングがない場合、所有者の最初の選択は通常、予測できません。ITD では、所有者を事前に決定できます。

ASA クラスタリングでは、バックアップ フローの所有者も使用します。クラスタ内の特定のファイアウォールを通過するすべてのフローについて、別のファイアウォールがそのフローの状態と、フローを所有する ASA を保存します。実際のアクティブなフローの所有者が失敗した場合、ITD failaction の再割り当てにより、失敗した所有者の ASA からのすべてのフロー（バケット）が、デバイス グループにリストされている次のアクティブ ノードに移動します。このトラフィックを受信する新しいファイアウォールが、受信するフローのバックアップの所有者でない場合、バックアップの所有者からフロー状態情報を受信し、トラフィックをシームレスに処理する必要があります。

ITD で ASA クラスタリングを使用する場合の潜在的な欠点は、バックアップ フローおよびその他のクラスタ テーブル操作が、非クラスタ化ファイアウォールでは消費されないメモリと CPU リソースを消費することです。したがって、非クラスター化ファイアウォールを使用すると、ファイアウォールのパフォーマンスが向上する場合があります。

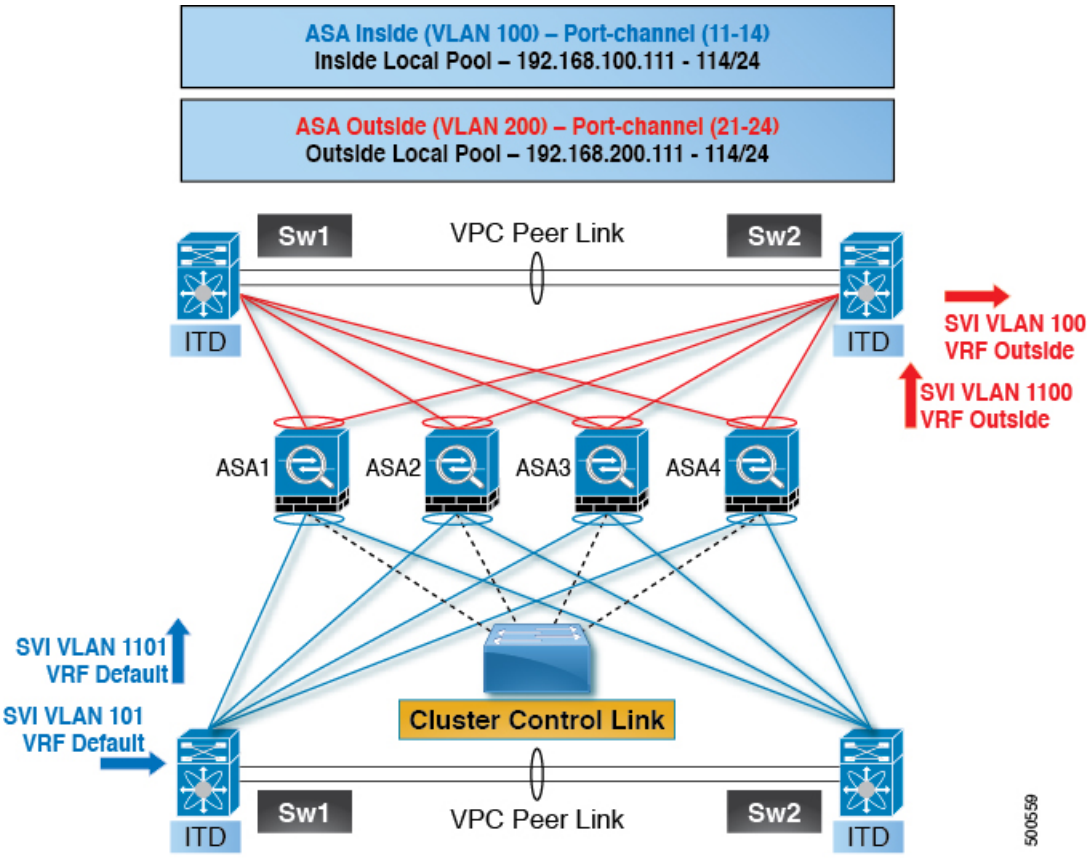
次の表は、ASA デバイスのステータスが変化したときに、ECMP と ITD で発生するクラスタ制御リンク（CCL）への影響の概要を比較したものです。

表 *3: ECMP* と *ITD - CCL* の影響の概要の比較

ASA ステータス	ITD	ECMP
定常状態	CCL 上の最小限のトラフィックと予想されるトラフィック タイプ。 ラインカードとスイッチのタイプに関係なく、まったく同じ負荷分散。	同じラインカード タイプとスイッチ モデルがすべての場所で使用されている場合、CCL 上の最小限のトラフィック。 異なるハードウェアが使用されている場合、より高いレベルの非対称性が発生し、CCL ネットワークでトラフィックが発生する可能性があります。ハードウェアごとに異なるハッシュ関数があります。 2 つのスイッチ（たとえば、vPC 内）が同じフローを異なる ASA デバイスに送信し、CCL トラフィックが発生する可能性があります。

ASA ステータス	ITD	ECMP
1 つの ASA で障害が発生	CCL に追加のトラフィックはありません。 ITD は、IP スティッキ性と復元力のあるハッシュを提供します。	すべてのフローが再ハッシュされ、追加のトラフィック リダイレクションが CCL で発生します。クラスタ内のすべての ASA デバイスへのトラフィックが影響を受ける可能性があります。
単一 ASA のリカバリ	トラフィック リダイレクションは、クラスタ内の 2 つの ASA デバイス間で CCL で発生する可能性があります。つまり、バケットを受信する回復された ASA と、以前にそのバケットにサービスを提供していた ASA です。	追加のトラフィック リダイレクションは、CCL で発生する可能性があります。クラスタ内のすべての ASA デバイスへのトラフィックが影響を受ける可能性があります。
ASA 追加	CCL の最小限の追加トラフィック。	すべてのフローが再ハッシュされ、追加のトラフィック リダイレクションが CCL で発生します。クラスタ内のすべての ASA デバイスへのトラフィックが影響を受ける可能性があります。

図 *26 : vPC* を使用したデュアル スイッチ サンドイッチを備えた *ASA* クラスタ



ステップ 1：2 つのスイッチを構成します。

（注） クラスタリングを導入しても、ITD 構成は変更されません。ITD の設定は、トポロジのタイプによって異なります。この例では、設定は vPC トポロジを使用したデュアル スイッチ サンドイッチと同じです。

```
switch #1:
interface vlan 10
  description INSIDE_VLAN
  ip address 192.168.10.10/24

interface vlan 100
  description FW_INSIDE_VLAN
  ip address 192.168.100.10/24

interface port-channel 11
  description To_ASA-1_INSIDE
  switchport mode access
  switchport access vlan 100
  vpc 11

interface ethernet 4/1
  description To_ASA-1_INSIDE
```

```
  switchport mode access
  switchport access vlan 100
  channel-group 11 mode active


switch #2:
interface vlan 20
  description OUTSIDE_VLAN
  ip address 192.168.20.10/24

interface vlan 200
  description FW_OUTSIDE_VLAN
  ip address 192.168.200.10/24

interface port-channel 21
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  vpc 11

interface ethernet 4/25
  description To_ASA-1_OUTSIDE
  switchport mode access
  switchport access vlan 200
  channel-group 21 mode active
```

ステップ 2：ASA を構成します。

```
cluster group ASA-CLUSTER-L3
  local-unit ASA1
  cluster-interface port-channel 31
  ip address 192.168.250.100 255.255.255.0
  piority 1
  health-check holdtime 1.5
  clacp system-mac auto system-priority 1
  enable

mac-address pool MAC-INSIDE aaaa.0101.0001 - aaaa.0101.0008
mac-address pool MAC-OUTSIDE aaaa.0100.0001 - aaaa.0100.0008
ip local pool IP-OUTSIDE 192.168.200.111-192.168.200.114
ip local pool IP-INSIDE 192.168.100.111-192.168.100.114

interface port-channel 11
  description INSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-INSIDE
  nameif inside
  security-level 100
  ip address 192.168.100.11 255.255.255.0 cluster-pool IP-INSIDE

interface port-channel 21
  description OUTSIDE
  lacp max-bundle 8
  mac-address cluster-pool MAC-OUTSIDE
  nameif outside
  security-level 100
  ip address 192.168.200.11 255.255.255.0 cluster-pool IP-OUTSIDE

interface port-channel 31
  description Clustering Interface
  lacp max-bundle 8

interface TenGigabitEthernet 0/6
  channel-group 11 mode active
```

```
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/7
  channel-group 11 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/8
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 0/9
  channel-group 21 mode active
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/0
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address

interface TenGigabitEthernet 1/1
  channel-group 31 mode on
  no nameif
  no security-level
  no ip address
```

この例では、ポート チャネル 11 および 21 が内部インターフェイスと外部インターフェイスに使用されています。ポート チャネル 31 はクラスタリング インターフェイスです。個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メイン クラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在のプライマリ ユニットに属します。同様に、MAC アドレス プールも構成され、対応する内部または外部ポート チャネルの下で使用されます。

ITD レイヤ 2 の構成例

次の例は、ITD-L2 を構成する方法を示しています。

ITD レイヤ 2 機能を有効にします。

```
(config) feature itd
(config) itd Port-group 100
(config-port-group) int eth 1/11
(config-port-group) int eth 1/12
(config) itd SER3
(config-itd) port-group 100
(config-itd) source vlan 2010-2015
(config-itd) no shutdown
```

ITD-L2 構成を確認します。

```
s!Command: show running-config services
!Running configuration last done at: Thu Dec  5 00:04:35 2019
!Time: Thu Dec  5 20:44:06 2019

version 9.3(3u)I9(1u) Bios:version 08.36
feature itd


itd port-group PG100
  interface Eth1/11
  interface Eth1/12
  interface Eth1/13
  interface Eth1/14
  interface Eth1/15
  interface Eth1/16
  interface Eth1/17
  interface Eth1/18
  interface Eth1/19
  interface Eth1/20
  interface Eth1/21
  interface Eth1/22
  interface Eth1/23

itd SER1
  port-group PG100
  source vlan 10-15
  no shut


itd SER2
  port-group PG100
  source vlan 1010-1015
  no shut
```

レイヤ 3 ITD 構成の確認

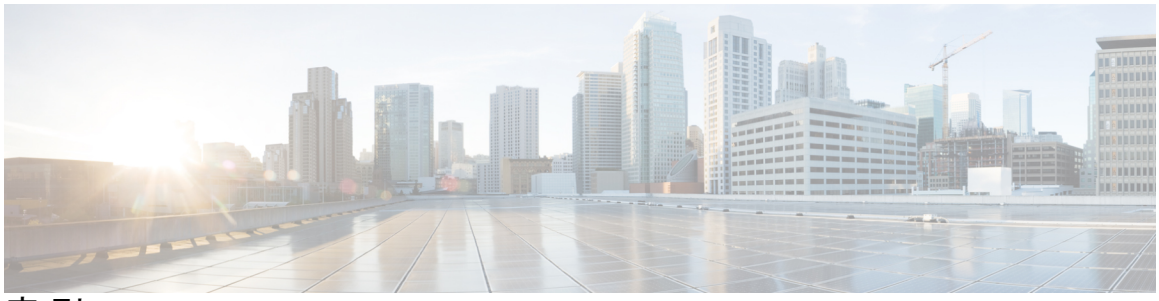
ITD 構成を確認するには、次のコマンドを使用します。

コマンド	目的
show ip/ipv6 policy vrf <context>	指定された入力インターフェイスに適用されるレイヤ 3 ITD 非 NAT サービス用に作成された IPv4/IPv6 ルートマップ ポリシーを表示します。
show route-map dynamic <route-map name>	レイヤ 3 ITD 非 NAT サービスの転送トラフィックに使用される、特定のバケット アクセス リストのトラフィック リダイレクション用に構成されたネクストホップを表示します。
show ip/ipv6 access-list <access-list name> dynamic	ITD で使用されるバケット アクセス リストのトラフィック一致基準を表示します。

コマンド	目的
show ip sla configuration dynamic	プローブが有効になっている場合に、デバイス グループ内のノードに対して ITD によって生成された IP SLA 設定を表示します。
show track dynamic	プローブが有効な場合、デバイス グループ内のノードについて ITD によって生成されたトラックを表示します。
show nat itd	レイヤ 3 ITD NAT サービスの転送トラフィックおよび変換に使用される、特定のバケット アクセス リストのトラフィック リダイレクション用に構成されたネクスト ホップを表示します。

関連資料

関連項目	マニュアル タイトル
IP SLA	『*Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide*』



索 引

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。