Cisco Nexus 3600 スイッチ NX-OS Intelligent Traffic Director 構成ガイド、リリース 10.6(X)

最終更新：2025 年 12 月 15 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/

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、ユーザが値を入力する引数です。
[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、角カッコで囲み、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ません。引用符を使用すると、その引用符も含めて string とみなされます。

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、太字のスクリーン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 3600 プラットフォーム スイッチの関連資料

Cisco Nexus 3600 プラットフォーム 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/c/en/us/support/switches/nexus-3000-series-switches/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。

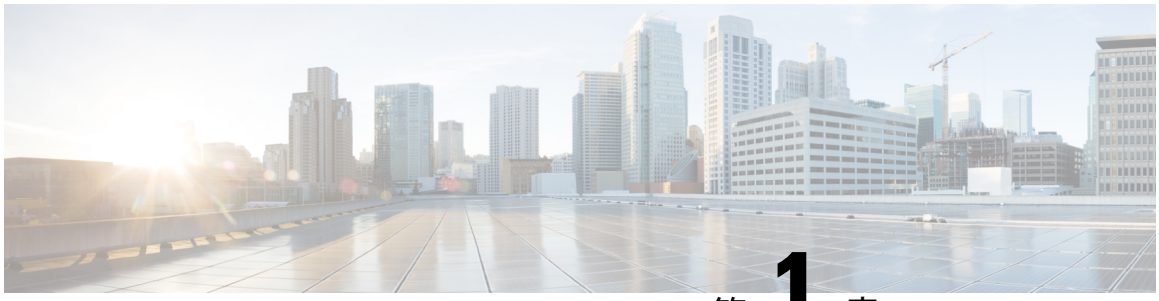
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



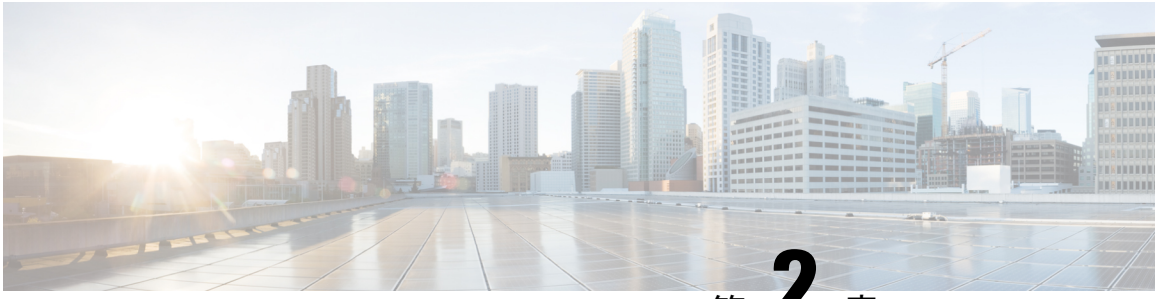
第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.6(1)F	N/A

新機能および変更された機能に関する情報



第 2 章

Intelligent Traffic Director のプラットフォーム サポート

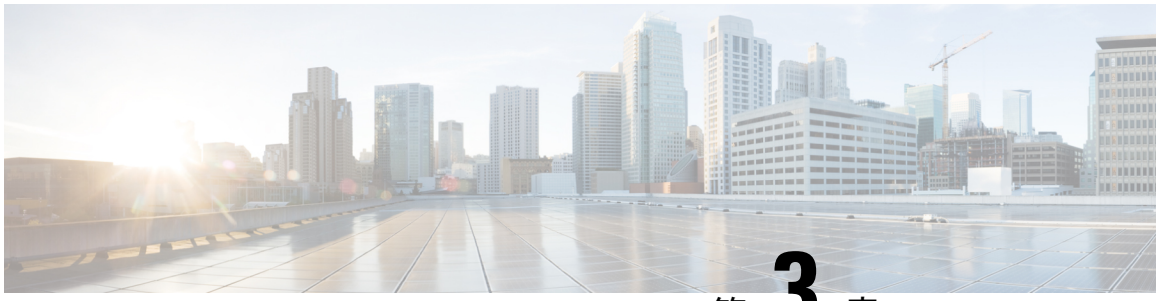
この章では、Cisco Nexus プラットフォーム スイート全体でサポートされていない機能のプラットフォーム サポートについて定義します。

Intelligent Traffic Director のプラットフォーム サポート

次の表で、Cisco プラットフォーム スイート全体でサポートされていない機能のプラットフォーム サポートについて定義します。初期製品のリリースでサポートされるプラットフォームについて詳細について、各リリースのインストール ガイドおよびリリース ノートを参照する必要があります。

機能	サポートされるプラットフォームまたはライン カード	サポートされるようになった最初のリリース	プラットフォームの例外
ITD、IPv4、IPv6	C36180YC-R および C3636C-R スイッチのサポートが追加されました。	Cisco Nexus NX-OS リリース 10.1(1)	

Intelligent Traffic Director のプラットフォーム サポート



第 3 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

- 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：

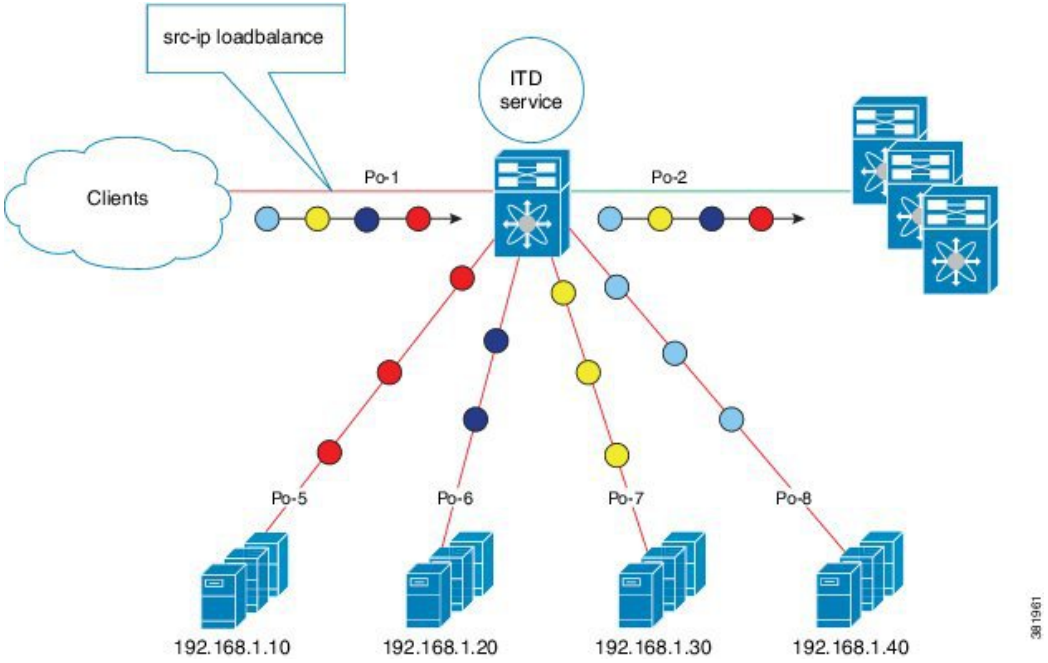
- ファイアウォールのクラスタへの負荷分散。
- NX-OS デバイスへのロードバランシングにより、IPS、IDS、および WAF を拡張します。
- 低コストの VM / コンテナ ベースの NFV にロードバランシングすることにより、NFV ソリューションを拡張します。
- WAAS / WAE ソリューションをスケーリングします。Wide Area Application Services（WAAS）または Web Accelerator Engine（WAE）ソリューションのトラフィック リダイレクト メカニズム
- VDS-TC（ビデオ キャッシュ）ソリューションのスケーリング
- 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

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 *1:* ワンアーム展開モード

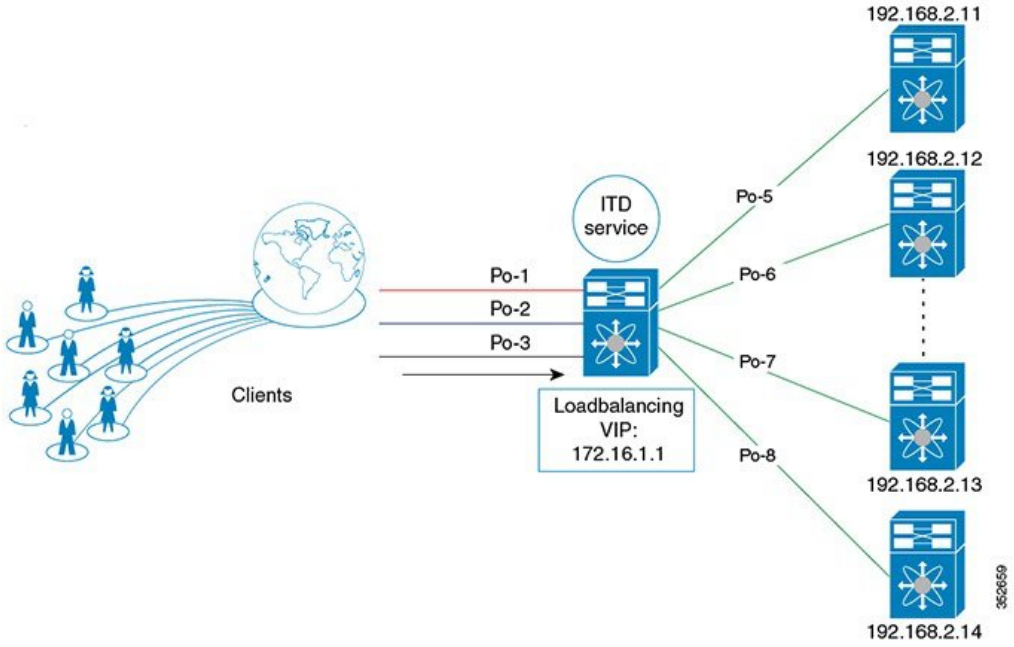


サーバー ロードバランシング展開モード

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 *2 : VIP* を使用した *ITD* 負荷分散



デバイスグループ

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。

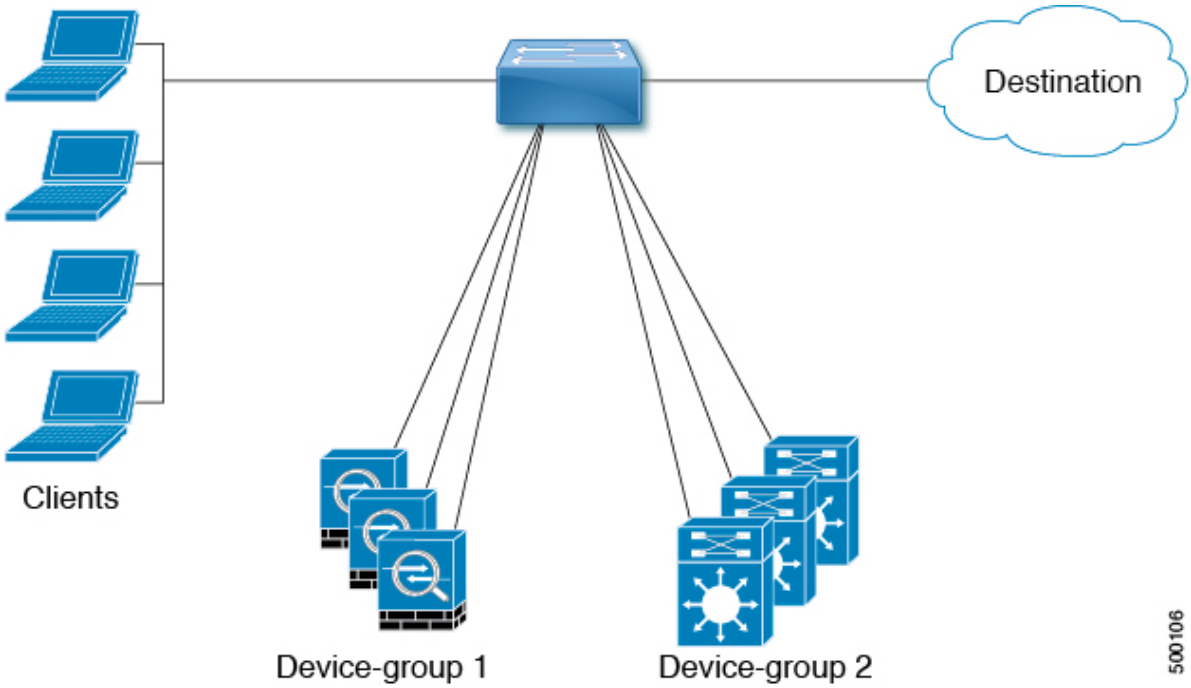
ITD サービス内の複数のデバイス グループ

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 *3 : 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、 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。

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。

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。

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。

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。

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。

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。

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) 以降では、Nexus スイッチ プラットフォーム サポート マトリクスに基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するために、どの Cisco NX-OS リリースが必要かを確認してください。

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 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 • UDP	• TCP • ICMPv3	Cisco NX-OS リリース 10.1(1) で導入済み
ノードごとのプローブ レベル	○	○	Cisco NX-OS リリース 10.1(1) で導入済み
Hot-Standby	○	○	Cisco NX-OS リリース 10.1(1) で導入済み
重量	○	○	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	○	○	Cisco NX-OS リリース 10.1(1) で導入済み
プライマリ ノード	○	○	Cisco NX-OS リリース 10.1(1) で導入済み
重みのあるプライマリ ノード	○	○	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	非対応	非対応	Cisco NX-OS リリース 10.1(1) で導入済み
サービス レベル			
インクルード ACL	○	○	Cisco NX-OS リリース 10.1(1) で導入済み

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) で導入済み
除外-ACL	○	○	Cisco NX-OS リリース 10.1(1) で導入済み 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	Cisco Nexus C36180YC-R および C3636C-R スイッチ	Cisco Nexus C36180YC-R および C3636C-R スイッチ	Cisco NX-OS リリース 10.1(1) で導入済み

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

手順

	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。

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。

手順の概要

1. **configure terminal**
2. [**no**] **itd device-group** *name*
3. [**no**] **node {ip | ipv6} {***ipv4-address* **|** *ipv6-address***}**
4. [**no**] **weight** *weight*
5. [**no**] **mode hot-standby**
6. **exit**
7. ノードごとに手順 3 ～ 5 を繰り返します。
8. [**no**] **probe** {**icmp** | **http** | **tcp port** *port-number* | **udp port** *port-number* | **dns** [**frequency** *seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout** *seconds*]

9. （任意） **copy running-config startup-config**

手順の詳細

手順

	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	[**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 4	[**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 5	[**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 6	**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 7	ノードごとに手順 3 ～ 5 を繰り返します。	
ステップ 8	[**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 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 9	（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**
   - [**no**] **failaction node least-bucket**
   - [**no**] **failaction bucket distribute**
   - [**no**] **failaction node per-bucket**
8. [**no**] **vrf** *vrf-name*
9. [**no**] **exclude access-list** *acl-name*
10. **no shutdown**
11. （任意） **show itd** [*itd-name*]
12. （任意） **copy running-config startup-config**

手順の詳細

手順

	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。

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） 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`	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。

	コマンドまたはアクション	目的
		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。 • 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：	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

	コマンドまたはアクション	目的

	`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`
		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）
		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。
		（注）
		次の **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** • [**no**] **failaction node least-bucket** • [**no**] **failaction bucket distribute** • [**no**] **failaction node per-bucket** 例： `switch(config-itd)# failaction node reassign`	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。

	コマンドまたはアクション	目的

	例：
	`switch(config-itd)# failaction node least-bucket`
	
	例：
	`switch(config-itd)# failaction bucket distribute`
	
	例：
	`switch (config-itd)# failaction node per-bucket`	

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。
ステップ 10	**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 11	（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 12	（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。

ACL を ITD サービスに割り当てる

インクルードアクセス コントロール リスト（ACL）機能を使用して、ITD サービスに ACL を割り当てることができます。この機能は、ACL 内の **permit** メソッドを使用するアクセス コントロール エントリ（ACE）ごとに、不要なトラフィックをフィルタリングし、IP アクセス リストとルートマップを生成して、許可されたトラフィックのロードバランシングを行います。ロードバランシングは、送信元または宛先 IP アドレスのいずれかを使用してサポートされます。

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。

ITD サービスに割り当てられる ACL 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** *itd-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*}
6. [**no**] **failaction node-per-bucket**
7. **access-list** *acl-name*
   - IPv4 の場合： **access-list** *acl4-name*
   - IPv6 の場合： **access-list IPv6** *acl6-name*
8. [**no**] **shutdown**
9. （任意） **copy running-config startup-config**

手順の詳細

手順

	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** *itd-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。

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。
ステップ 4	[**no**] **ingress interface** *interface* 例： `switch(config-itd)# ingress interface ethernet 4/1-10`	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。

	コマンドまたはアクション	目的
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*} 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。
ステップ 6	[**no**] **failaction node-per-bucket** 例： `switch(config-itd)# failaction node-per-bucket`	ノード障害が発生すると、このノードに割り当てられたバケットは、残りのアクティブ ノードに分散されます。重みがノードに割り当てられている場合、分布はノードの重みに基づいています。

ステップ 7	**access-list** *acl-name*
	• IPv4 の場合： **access-list** *acl4-name*
	• IPv6 の場合： **access-list IPv6** *acl6-name*
	例：
	IPv4：
	`switch(config-itd)# access-list itd_d`
	例：
	IPv6
	`switch(config-itd)# access-list ipv6 itd1_d`
	例：
	マルチ ACL：
	`switch(config-itd)# access-list test1 device-group-dg1`
	`switch(config-itd)# access-list test2 device-group-dg2`
		ITD サービスに ACL を割り当てます。
		（注）
		Cisco NX-OS リリース 9.3(3) 以降、ユーザーは 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、それぞれを独自のデバイス グループ（マルチ ACL）に関連付けるオプションを使用できます。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。

ステップ 8	[**no**] **shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	（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。

無停止でのノードの追加または削除

ITD サービスをシャットダウンせずにデバイス グループ内のノードを追加または削除できる ITDセッションを構成できます。それによって、ITDサービスのシャットダウン時にトラフィックの中断を最小限にすることができます。

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 グループと ITD サービスが構成されたことを確認します。

手順の概要

1. **configure terminal**
2. **itd session device-group** *device-group-name*
3. [**no**] **{node ip | node ipv6}** {*ipv4-address* | *ipv6-address*}
4. {**commit** | **abort**}
5. （任意） **show itd session device-group** [*name*]
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	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	**itd session device-group** *device-group-name*
	例：
	`switch(config)# itd session device-group dg1`
	`switch(config-session-device-group)#`
		指定されたデバイス グループのITDセッションを作成します。

	コマンドまたはアクション	目的

ステップ 3	[**no**] **{node ip | node ipv6}** {*ipv4-address* | *ipv6-address*}
	例：
	`switch(config-session-device-group)# node ip 2.2.2.1`
	例：
	`switch(config-session-device-group)#  node ipv6 10:1::1:2`
		指定されたノードをITDデバイス グループに追加します。このコマンドの **no** 形式は、指定されたノードを ITD デバイス グループから削除します。
		追加または削除するノードごとに、この手順を繰り返します。
		（注）
		ノードあたりのバケットの最大制限は32です。ITDセッション中に、ノードが（通常のコマンドまたは中断のないコマンドによって）削除され、残りのアクティブ ノードのノードあたりのバケット数が 32 を超えると、次のエラー メッセージが表示されます。
		`ERROR: Cannot delete node, exceeding maximum 32 buckets per Node. Shut service to make changes`

ステップ 4	{**commit** | **abort**} 例： `switch(config-session-device-group)# commit switch(config)#`	**commit** コマンドは、新しいノード セットまたは変更されたノード セットで ITD デバイス グループを更新し、バケットを再割り当てして、ITD セッション設定をクリーンアップします。 **abort** コマンドはITDセッション設定を無視し、ITD デバイス グループを更新しません。 （注） リブートする前に、中断のないセッションの**commit** コマンドを入力します。**copy running-config startup-config** コマンドを入力してスイッチをリブートすると、ITD デバイス グループの構成が保存されますが、**commit** は有効になりません。
ステップ 5	（任意） **show itd session device-group** [*name*] 例： `switch(config)# show itd session device-group dg1`	構成されたすべてのITDセッションまたは指定されたデバイス グループの ITD セッションを表示します。
ステップ 6	（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。

インクルードまたは除外 ACL での ACE の無停止の追加または削除

ITD サービスをシャットダウンせずに、インクルードまたは除外 ACL のアクセス コントロールエントリ（ACE）を追加または削除できます。それによって、ITD サービスのシャットダウン時にトラフィックの中断を最小限にすることができます。

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 グループと ITD サービスが構成されたことを確認します。

ACL が ITD サービスに割り当てられていることを確認します。

手順の概要

1. **configure terminal**
2. **itd session access-list** *acl-name* **refresh**
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	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	**itd session access-list** *acl-name* **refresh** 例： `switch(config)# itd session access-list test1 refresh`	インクルード ACL を内部的に読み取り、TCAM をプログラムします。ITD は、古い ACL ACE と新しい ACL ACE をチェックし、ITD によって生成された ACL を更新します。 （注） このコマンドは、インクルード ACL にのみ必要です。除外 ACL は自動的にプログラムされるため、このコマンドは必要ありません。
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。

ITD レイヤ 3 構成の確認

ITD レイヤ 3 構成を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show itd [*itd-name*] [**brief** | **vrf** [*vrf-name*]]	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。 • 特定の ITD インスタンスのステータスおよび構成を表示するには、*itd-name* 引数を使用します。 • ステータスおよび構成の要約情報を表示するには、**brief** キーワードを使用します。 • **vrf** キーワードを使用して、指定された ITD インスタンスの VRF を表示します。
show itd session device-group [*name*]	構成されたすべての ITD セッションまたは指定されたデバイス グループの ITD セッションを表示します。
show running-config services	構成された ITD デバイス グループとサービスを表示します。
show ip/ipv6 policy vrf <context>	NAT 接続先機能がイネーブルになっていない ITD レイヤ 3 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> **show route-map dynamic**	NAT 接続先機能が有効になっていない ITD レイヤ 3 サービス用に生成された、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設定されたネクスト ホップを表示します。
show nat itd	NAT 接続先機能が有効になっている ITD レイヤ 3 サービス用に生成された、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設定されたネクスト ホップを表示します。
show ip access-list <access-list name> dynamic	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 **show ip sla configuration (Entry-number) 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 **show track dynamic brief**	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。

（注） 10.2(1)F リリース以降、ITD で生成された構成は、ダイナミック show CLI を介して表示されます。

以下に、ITD 構成を確認する例を示します。

```
switch# show itd

Name            Probe LB Scheme  Status   Buckets
--------------- ----- ---------- -------- -------
WEB             ICMP  src-ip     ACTIVE   2

Device Group                                    VRF-Name
----------------------------------------------- -------------
WEB-SERVERS


Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
WEB_itd_pool                   Po-1         UP       -

Virtual IP     Netmask/Prefix            Protocol   Port
-------------------------------------- ---------- -----
10.10.10.100 / 255.255.255.255           IP           0

  Node  IP                Config-State Weight Status     Track_id
  ----------------------- ------------ ------ ---------- ---------
  1     10.10.10.11       Active       1      OK           -

        Bucket List
        ------------------------------------------------------------------------
        WEB_itd_vip_1_bucket_1


  Node  IP                Config-State Weight Status     Track_id
  ----------------------- ------------ ------ ---------- ---------
  2     10.10.10.12       Active       1      OK           -

        Bucket List
        ------------------------------------------------------------------------
        WEB_itd_vip_1_bucket_2
```

この例は、ITD NAT 統計の出力を示しています。

```
switch# sh itd test statistics

Service            Device Group                 VIP/mask
```

```
      #Packets
-------------------------------------------------------------------------------
-------------------------------------------------------------
test                  dg              20.20.20.20 / 255.255.255.255             158147
 (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             22820
 (14.43%)
test_itd_vip_2_bucket_5      10.10.10.2         Redirect     10.10.10.2             22894
 (14.48%)

Traffic Bucket               Assigned to          Mode        Original Node
#Packets
---------------              --------------       -----       --------------
---------
test_itd_vip_2_bucket_2     11.11.11.2          Redirect     11.11.11.2
24992 (15.80%)
test_itd_vip_2_bucket_6     11.11.11.2          Redirect     11.11.11.2
25916 (16.39%)

Traffic Bucket               Assigned to          Mode        Original Node
#Packets
---------------              --------------       -----       --------------
---------
test_itd_vip_2_bucket_3     12.12.12.2          Redirect     12.12.12.2             17537
 (11.09%)
test_itd_vip_2_bucket_7     12.12.12.2          Redirect     12.12.12.2             18048
 (11.41%)

Traffic Bucket               Assigned to          Mode        Original Node
#Packets
---------------              --------------       -----       --------------
---------
test_itd_vip_2_bucket_4    13.13.13.2           Redirect     13.13.13.2             20727
 (13.11%)
test_itd_vip_2_bucket_8    13.13.13.2           Redirect     13.13.13.2              5213
  (3.30%)

Return Traffic from Node            #Packets
-------------------------------------------------------------------
10.10.10.2                        58639 (28.86%)
11.11.11.2                        65695 (32.33%)
12.12.12.2                        45710 (22.49%)
13.13.13.2                        33175 (16.32%)

Total packets: 203219 (100.00%)
switch#
~
```

ITD の構成例

この例は、ITDおよびその他の前提条件の機能を設定し、ITDデバイス グループを構成する方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# feature itd
```

```
switch-1(config)# feature sla sender
switch-1(config)# feature pbr
switch-1(config)#
switch-1(config)#  itd device-group DG1
switch-1(config-device-group)#    probe icmp frequency 2 retry-down-count 2 retry-up-count
 1 timeout 1
switch-1(config-device-group)#    node ip 10.200.1.2
switch-1(config-dg-node)#   node ip 10.200.2.2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd device-group DG2
switch-1(config-device-group)#    probe icmp
switch-1(config-device-group)#    node ipv6 2007::2
switch-1(config-dg-node)#   node ipv6 2008::2
switch-1(config-dg-node)#
switch-1(config-dg-node)# end
switch-1#
```

次の例は、バケットごとのノードとして failaction を使用し、静的バケット カウントを使用して宛先ベースのロードバランス方式を使用して ITD サービスを作成し、デバイス グループをサービスに関連付ける方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)#    device-group DG1
switch-1(config-itd)#    ingress interface Ethernet1/17
switch-1(config-itd)#    failaction node per-bucket
switch-1(config-itd)#    load-balance method dst ip buckets 4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#
switch-1(config-itd)# itd SER2
switch-1(config-itd)#    device-group DG2
switch-1(config-itd)#    ingress interface Ethernet1/18
switch-1(config-itd)#    failaction node per-bucket
switch-1(config-itd)#    load-balance method dst ip buckets 4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)# end
switch-1#
switch-1# sh run services
!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 21:05:40 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.1.2
  node ip 10.200.2.2


itd device-group DG2
  probe icmp
  node ipv6 2007::2
```

```
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node per-bucket
  load-balance method dst ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node per-bucket
  load-balance method dst ip buckets 4
  no shut
switch-1#
switch-1# show 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           dst-ip     ACTIVE   4          Eth1/17

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


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG1                                                ICMP


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ----- ----- --------------- --
1             10.200.1.2             A   1 ICMP                        OK
2             10.200.2.2             A   1 ICMP                        OK

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
-------------- ---------- -------- ---------  --------------
SER2           dst-ip     ACTIVE   4          Eth1/18

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


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG2                                                ICMP


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
  STS
------------------------------------------- ---------- --- --- ----- ----- ---------------
 --
1                                  2007::2             A   1 ICMP
  OK
2                                  2008::2             A   1 ICMP
```

```
  OK


switch-1#
switch-1# sh itd

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

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
SER1           dst-ip     ACTIVE   4

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


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG1                                                 ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
SER1_itd_pool                  Eth1/17      UP       1


  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  1             10.200.1.2             Active   1 ICMP                       OK   2
10002

      Bucket List
      ----------------------------------------------------------------------------
      SER1_itd_bucket_1, 3

  Node  IP                  Cluster-id Cfg-S   WGT Probe Port     Probe-IP   STS Trk#
Sla_id
  ------------------------- ---------- ------- --- ---- ----- --------------- -- ---
-------
  2             10.200.2.2             Active   1 ICMP                       OK   3
10003

      Bucket List
      ----------------------------------------------------------------------------
      SER1_itd_bucket_2, 4
Legend:
 ST(Status): ST-Standby,LF-Link Failed,PF-Probe Failed,PD-Peer Down,IA-Inactive

Name           LB Scheme  Status   Buckets
-------------- ---------- -------- -------
SER2           dst-ip     ACTIVE   4

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


Device Group                                       Probe  Port
-------------------------------------------------- ----- ------
DG2                                                 ICMP

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

```
SER2_itd_pool                  Eth1/18      UP       4


  Node  IP                                     Cluster-id Cfg-S  WGT
  ------------------------------------------ ---------- ------- ---
  1                                  2007::2             Active   1

      Probe Port    Probe-IP    STS Trk# Sla_id
      ---- ----- --------------- -- --- -------
      ICMP                       OK   5   10004

      Bucket List
      ----------------------------------------------------------------------------
      SER2_itd_bucket_1, 3

  Node  IP                                     Cluster-id Cfg-S  WGT
  ------------------------------------------ ---------- ------- ---
  2                                  2008::2             Active   1

      Probe Port    Probe-IP    STS Trk# Sla_id
      ---- ----- --------------- -- --- -------
      ICMP                       OK   6   10005

      Bucket List
      ----------------------------------------------------------------------------
      SER2_itd_bucket_2, 4

switch-1#

switch-1# sh run rpm

!Command: show running-config rpm
!No configuration change since last restart
!Time: Tue Jan  5 21:08:12 2021

version 10.1(1) Bios:version 01.14
feature pbr

route-map SER1_itd_pool permit 10
  match ip address SER1_itd_bucket_1
  set ip next-hop verify-availability 10.200.1.2 track 2 force-order
route-map SER1_itd_pool permit 11
  match ip address SER1_itd_bucket_2
  set ip next-hop verify-availability 10.200.2.2 track 3 force-order
route-map SER1_itd_pool permit 12
  match ip address SER1_itd_bucket_3
  set ip next-hop verify-availability 10.200.1.2 track 2 force-order
route-map SER1_itd_pool permit 13
  match ip address SER1_itd_bucket_4
  set ip next-hop verify-availability 10.200.2.2 track 3 force-order
route-map SER2_itd_pool permit 10
  match ipv6 address SER2_itd_bucket_1
  set ipv6 next-hop verify-availability 2007::2 track 5 force-order
route-map SER2_itd_pool permit 11
  match ipv6 address SER2_itd_bucket_2
  set ipv6 next-hop verify-availability 2008::2 track 6 force-order
route-map SER2_itd_pool permit 12
  match ipv6 address SER2_itd_bucket_3
  set ipv6 next-hop verify-availability 2007::2 track 5 force-order
route-map SER2_itd_pool permit 13
  match ipv6 address SER2_itd_bucket_4
  set ipv6 next-hop verify-availability 2008::2 track 6 force-order
```

```
interface Ethernet1/17
  ip policy route-map SER1_itd_pool

interface Ethernet1/18
  ipv6 policy route-map SER2_itd_pool

switch-1#
switch-1# show ip access-lists dynamic

IP access list SER1_itd_bucket_1
        10 permit ip any 1.1.1.0 255.255.255.63
IP access list SER1_itd_bucket_2
        10 permit ip any 1.1.1.64 255.255.255.63
IP access list SER1_itd_bucket_3
        10 permit ip any 1.1.1.128 255.255.255.63
IP access list SER1_itd_bucket_4
        10 permit ip any 1.1.1.192 255.255.255.63
switch-1#
switch-1# show run track

!Command: show running-config track
!No configuration change since last restart
!Time: Tue Jan  5 21:09:25 2021

version 10.1(1) Bios:version 01.14
track 1 interface Ethernet1/17 line-protocol
track 2 ip sla 10002 reachability
 delay up 2 down 4

track 3 ip sla 10003 reachability
 delay up 2 down 4

track 4 interface Ethernet1/18 line-protocol
track 5 ip sla 10004 reachability
 delay up 30 down 30

track 6 ip sla 10005 reachability
 delay up 30 down 30

switch-1#
switch-1# sh track
Track 1
  Interface Ethernet1/17 Line Protocol
  Line Protocol is UP
  1 changes, last change 00:05:54
  Tracked by:
    ISCM Configuration

Track 2
  IP SLA 10002 Reachability
  Reachability is UP
  2 changes, last change 00:05:50
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 2 secs, down 4 secs

Track 3
  IP SLA 10003 Reachability
  Reachability is UP
  2 changes, last change 00:05:50
  Latest operation return code: OK
```

```
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 2 secs, down 4 secs

Track 4
  Interface Ethernet1/18 Line Protocol
  Line Protocol is UP
  1 changes, last change 00:05:32
  Tracked by:
    ISCM Configuration

Track 5
  IP SLA 10004 Reachability
  Reachability is UP
  2 changes, last change 00:04:51
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 30 secs, down 30 secs
Track 6
  IP SLA 10005 Reachability
  Reachability is UP
  2 changes, last change 00:04:51
  Latest operation return code: OK
  Latest RTT (millisecs): 1
  Tracked by:
    ISCM Configuration
    Route Map Configuration
  Delay up 30 secs, down 30 secs
switch-1#
switch-1# show ip sla stat

IPSLAs Latest Operation Statistics

IPSLA operation id: 10002
        Latest RTT: 1 milliseconds
Latest operation start time: 21:11:12.861 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 210
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10003
        Latest RTT: 1 milliseconds
Latest operation start time: 21:11:12.901 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 210
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10004
        Latest RTT: 2 milliseconds
Latest operation start time: 21:11:04.995 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 39
Number of failures: 1
Operation time to live: forever

IPSLA operation id: 10005
        Latest RTT: 1 milliseconds
```

```
Latest operation start time: 21:11:05.034 UTC Tue Jan 05 2021
Latest operation return code: OK
Number of successes: 39
Number of failures: 1
Operation time to live: forever
switch-1#
```

この例は、送信元 IP ベースのロードバランシング方式を使用して、ノードの再割り当てとしての失敗アクションとノードの最小バケットとしての failaction を使用して ITD サービスを構成する方法を示しています。

```
switch-1(config)# feature itd
switch-1(config)#
switch-1(config)#
switch-1(config)# itd device-group DG1
switch-1(config-device-group)#   probe icmp frequency 2 timeout 1 retry-down-count 2
retry-up-count 1
switch-1(config-device-group)#   node ip 10.200.1.2
switch-1(config-dg-node)#   node ip 10.200.2.2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd device-group DG2
switch-1(config-device-group)#   probe icmp
switch-1(config-device-group)#   node ipv6 2007::2
switch-1(config-dg-node)#   node ipv6 2008::2
switch-1(config-dg-node)#
switch-1(config-dg-node)#
switch-1(config-dg-node)# itd SER1
switch-1(config-itd)#   device-group DG1
switch-1(config-itd)#   ingress interface Eth1/17
switch-1(config-itd)#   failaction node reassign
switch-1(config-itd)#   load-balance method src ip buckets 4
switch-1(config-itd)#   no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#
switch-1(config-itd)# itd SER2
switch-1(config-itd)#   device-group DG2
switch-1(config-itd)#   ingress interface Eth1/18
switch-1(config-itd)#   failaction node least-bucket
switch-1(config-itd)#   load-balance method src ip
switch-1(config-itd)#   no shut
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 21:21:41 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.1.2
  node ip 10.200.2.2

itd device-group DG2
  probe icmp
  node ipv6 2007::2
  node ipv6 2008::2
```

```
itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  no shut

switch-1#
```

この例は、ITDセッションを使用してITDノードを追加および削除し、サービスがアクティブなときにITD構成を変更できるようにする方法を示しています。

```
switch-1(config)# itd session device-group DG1
switch-1(config-session-device-group)#                    no node ip 10.200.1.2
switch-1(config-session-device-group)#                    node ip 10.200.3.2
switch-1(config-session-dg-node)#                    node ip 10.200.4.2
switch-1(config-session-dg-node)#                    commit
switch-1(config)#                itd session device-group DG2
switch-1(config-session-device-group)#                    no node ipv6 2007::2
switch-1(config-session-device-group)#                    node ipv6 2009::2
switch-1(config-session-dg-node)#                    commit
switch-1(config)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 22:49:07 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  no shut
```

```
switch-1#
switch-1# 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   4          Eth1/17

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


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG1                                                ICMP


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ---- ----- --------------- --
1             10.200.3.2             A   1 ICMP                        OK
2             10.200.2.2             A   1 ICMP                        OK
3             10.200.4.2             A   1 ICMP                        OK

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
-------------- ---------- -------- ---------  --------------
SER2           src-ip     ACTIVE   2          Eth1/18

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


Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG2                                                ICMP


Node      IP                                  Cluster-id C-S WGT Probe Port    Probe-IP
  STS
----------------------------------------- ---------- --- --- ---- ----- ---------------
 --
1                                  2009::2            A   1 ICMP
  OK
2                                  2008::2            A   1 ICMP
  OK


switch-1#
```

この例は、ユーザー定義のアクセス リストを使用して ITD サービスのトラフィックをフィルタリングする方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# ip access-list acl4
switch-1(config-acl)#                  10 permit ip 7.7.1.0/24 6.6.1.0/24
switch-1(config-acl)#                  20 permit ip 7.7.2.0/26 6.6.2.0/26
```

```
switch-1(config-acl)#                ipv6 access-list acl6
switch-1(config-ipv6-acl)#                 10 permit ipv6 2004::5/120 2005::5/120
switch-1(config-ipv6-acl)#                 20 permit ipv6 2004::100/122 2005::100/122
switch-1(config-ipv6-acl)#
switch-1(config-ipv6-acl)#
switch-1(config-ipv6-acl)#  itd SER1
switch-1(config-itd)#                  shut
switch-1(config-itd)#                  access-list acl4
switch-1(config-itd)#                  no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#                 itd SER2
switch-1(config-itd)#                   shut
switch-1(config-itd)#                   access-list ipv6 acl6
switch-1(config-itd)#                   no shut
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 22:57:25 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  access-list acl4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  access-list ipv6 acl6
  no shut

switch-1#
```

この例は、ユーザー定義のアクセス リストを使用して ITD サービスからトラフィックを除外する方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)# shut
```

```
switch-1(config-itd)# no access-list acl4
switch-1(config-itd)# exclude access-list acl4
switch-1(config-itd)# no sh
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)# itd SER2
switch-1(config-itd)# sh
switch-1(config-itd)# no access-list ipv6 acl6
switch-1(config-itd)# exclude access-list acl6
switch-1(config-itd)# no sh
switch-1(config-itd)# end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:01:38 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  exclude access-list acl4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  exclude access-list acl6
  no shut

switch-1#
```

この例は、ユーザー定義のアクセス リストのルールを更新し、そのようなユーザー ACLS を使用して ITD サービスの変更を有効にする方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# ip access-list acl5
switch-1(config-acl)#                    10 permit ip 7.7.1.0/24 6.6.1.0/24
switch-1(config-acl)#                itd SER1
switch-1(config-itd)#                    shut
switch-1(config-itd)#                    access-list acl5
switch-1(config-itd)#                    no shut
Note: Configure buckets equal to or more than the total number of nodes.
```

```
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#  ip access-list acl5
switch-1(config-acl)#                    20 permit ip 7.7.2.0/26 6.6.2.0/26
switch-1(config-acl)#                 itd session access-list acl5 refresh
switch-1(config)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:07:42 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  ingress interface Eth1/17
  failaction node reassign
  load-balance method src ip buckets 4
  access-list acl5
  exclude access-list acl4
  no shut

itd SER2
  device-group DG2
  ingress interface Eth1/18
  failaction node least-bucket
  load-balance method src ip
  exclude access-list acl6
  no shut

switch-1#
```

この例は、定義された ITD 仮想 IP アドレス宛てのトラフィックに特に ITD サービスを使用する方法を示しています。

```
switch-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch-1(config)# itd SER1
switch-1(config-itd)#                              shut
switch-1(config-itd)#                              no access-list acl5
switch-1(config-itd)#                              load-balance method src ip buckets 64
switch-1(config-itd)#                              virtual ip 6.6.1.1 255.255.255.192
switch-1(config-itd)#                              virtual ip 6.6.1.64 255.255.255.192
switch-1(config-itd)#                              failaction node per-bucket
switch-1(config-itd)#                              no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.
```

```
switch-1(config-itd)#                           itd SER2
switch-1(config-itd)#                             shut
switch-1(config-itd)#                             load-balance method src ip buckets 64
switch-1(config-itd)#                             virtual ipv6 2005::100 121
switch-1(config-itd)#                             virtual ipv6 2005:: 121
switch-1(config-itd)#                             failaction bucket distribute
switch-1(config-itd)#                             no shut
Note: Configure buckets equal to or more than the total number of nodes.
 The mask position that exceeds the available bits based on the number of buckets and
load-balance mode will internally default to 0.

switch-1(config-itd)#  end
switch-1#
switch-1# sh run services

!Command: show running-config services
!No configuration change since last restart
!Time: Tue Jan  5 23:17:20 2021

version 10.1(1) Bios:version 01.14
feature itd

itd device-group DG1
  probe icmp frequency 2 timeout 1 retry-down-count 2 retry-up-count 1
  node ip 10.200.3.2
  node ip 10.200.2.2
  node ip 10.200.4.2

itd device-group DG2
  probe icmp
  node ipv6 2009::2
  node ipv6 2008::2

itd SER1
  device-group DG1
  virtual ip 6.6.1.1 255.255.255.192
  virtual ip 6.6.1.64 255.255.255.192
  ingress interface Eth1/17
  failaction node per-bucket
  load-balance method src ip buckets 64
  exclude access-list acl4
  no shut

itd SER2
  device-group DG2
  virtual ipv6 2005::100 121
  virtual ipv6 2005:: 121
  ingress interface Eth1/18
  failaction bucket distribute
  load-balance method src ip buckets 64
  exclude access-list acl6
  no shut

switch-1#
switch-1# 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   64         Eth1/17
```

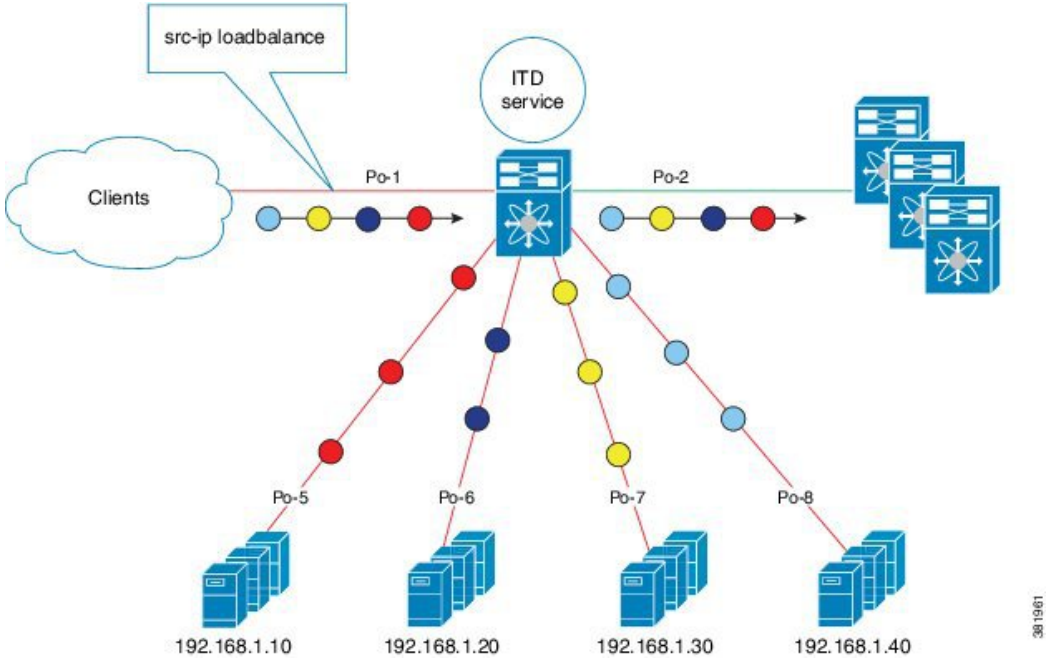
```
Source Interface
----------------


Exclude ACL
-------------------------------
 acl4

Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG1                                                ICMP

Virtual IP                                Netmask/Prefix Protocol     Port
------------------------------------------------- ------------ ----------
6.6.1.1 / 255.255.255.192                            IP           0


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ----- ----- --------------- --
1              10.200.3.2             A   1 ICMP                        OK
2              10.200.2.2             A   1 ICMP                        OK
3              10.200.4.2             A   1 ICMP                        OK

Virtual IP                                Netmask/Prefix Protocol     Port
------------------------------------------------- ------------ ----------
6.6.1.64 / 255.255.255.192                           IP           0


Node  IP                  Cluster-id C-S WGT Probe Port     Probe-IP   STS
------------------------- ---------- -- --- ----- ----- --------------- --
1              10.200.3.2             A   1 ICMP                        OK
2              10.200.2.2             A   1 ICMP                        OK
3              10.200.4.2             A   1 ICMP                        OK

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
-------------- ---------- -------- ---------  --------------
SER2           src-ip     ACTIVE   64         Eth1/18

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


Exclude ACL
-------------------------------
 acl6

Device Group                                          Probe  Port
------------------------------------------------- ----- ------
DG2                                                ICMP

Virtual IP                                Netmask/Prefix Protocol     Port
------------------------------------------------- ------------ ----------
2005::100 / 121                                      IP           0


Node      IP                                  Cluster-id C-S WGT Probe Port    Probe-IP
  STS
----------------------------------------- ---------- --- --- ---- ----- ---------------
 --
1                                  2009::2             A   1 ICMP
```

```
  OK
2                                   2008::2             A   1 ICMP
  OK

Virtual IP                                  Netmask/Prefix Protocol     Port
------------------------------------------------------- ------------ ----------
2005:: / 121                                            IP           0


Node      IP                                Cluster-id C-S WGT Probe Port    Probe-IP
  STS
----------------------------------------- ---------- --- --- ---- ----- ---------------
 --
1                                   2009::2             A   1 ICMP
  OK
2                                   2008::2             A   1 ICMP
  OK

switch-1#
```

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 *4:* 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
```

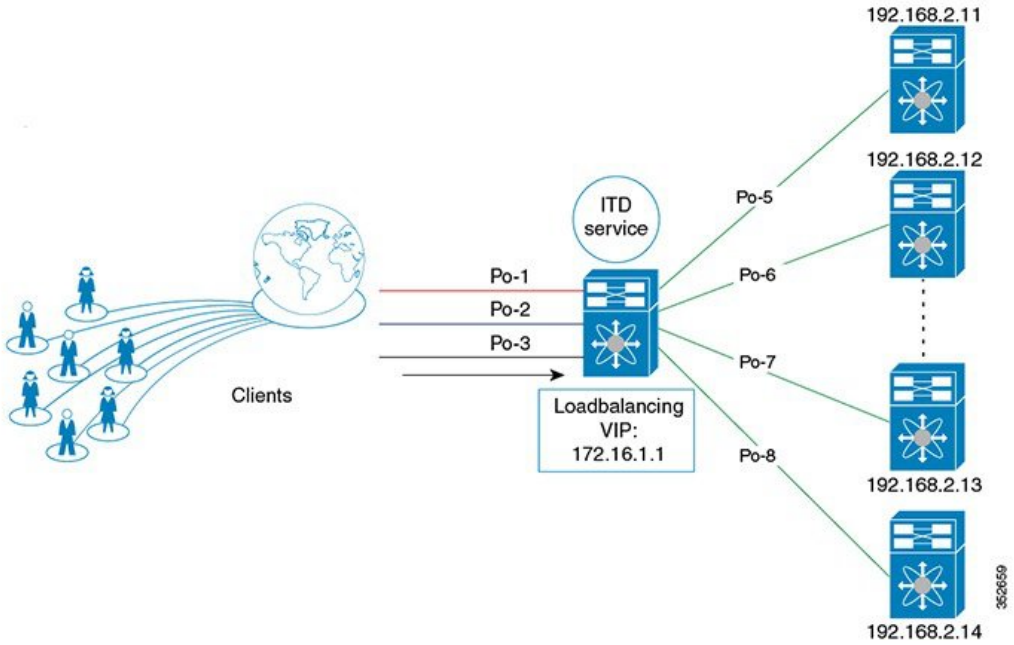
ステップ 2：ITD サービスを定義します。

```
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：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 *5: 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。

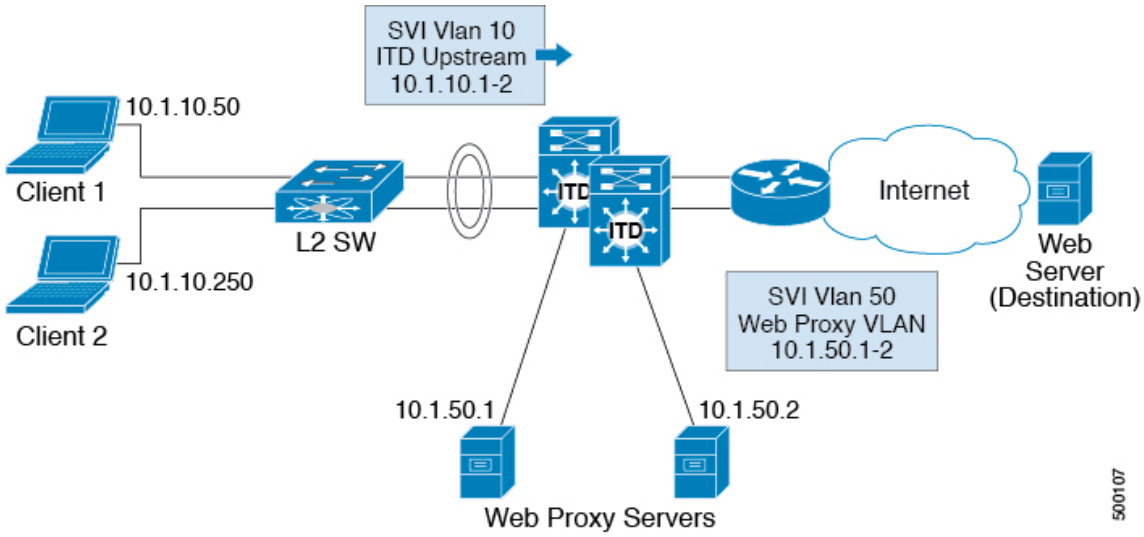
ITD を使用した Web プロキシ展開では、スイッチはインターネットに向かう Web トラフィックを照合し、プロキシサーバーに向けて負荷を分散します。プロキシサーバーは自律モード（WCCP から独立してアクティブ-アクティブ）で動作し、プロキシサーバーにリダイレクトされるトラフィックを処理します。ITD を介して実行されるノード ヘルス プローブは、ノードの状態を追跡し、可用性に基づいて適切にノードを削除または追加するという目的を果たします。スタンバイ サーバーは、冗長性のためにグループ レベルまたはノード レベルで構成することもできます。

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 *6 : 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：スティックのファイアーウォール

ITD サービス

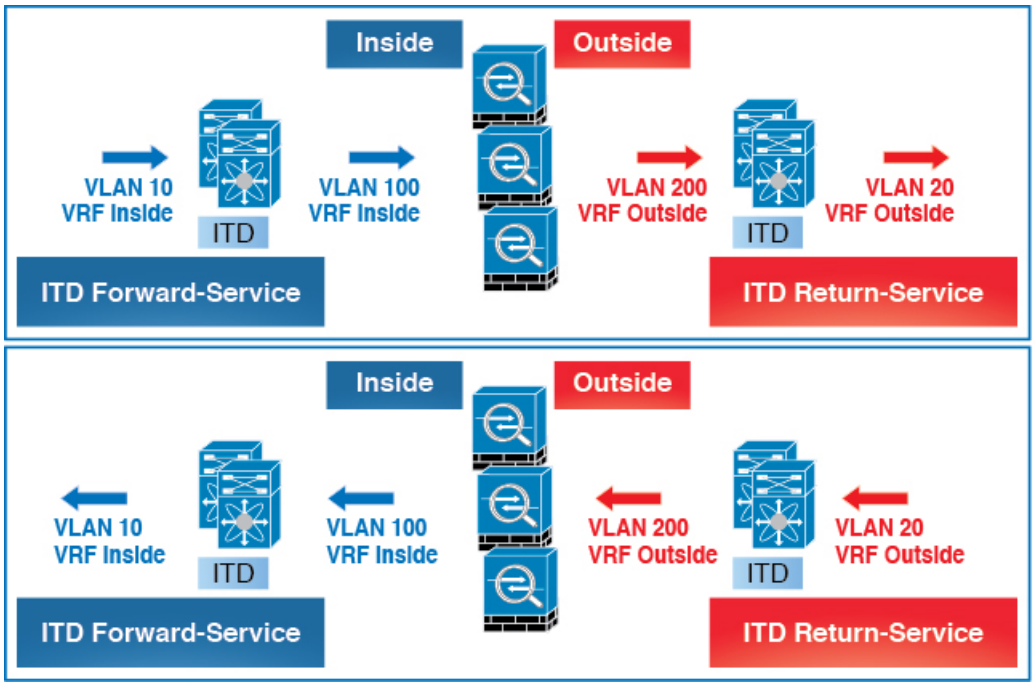
ITD サービス構成は、トラフィック フローの特定の方向に対する ITD トラフィック分散を定義します。フローの両方向をリダイレクトする必要がある場合は、2 つの ITD サービスを設定する必要があります。1 つは転送トラフィック フロー用、もう 1 つはリターン トラフィック フロー用です。ASA には異なる内部インターフェイスと外部インターフェイスの IP アドレスがあるため、2 つの異なるデバイス グループも、対応する内部および外部 IP アドレスを指すように構成する必要があります。

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 *7: ITD ASA* の展開



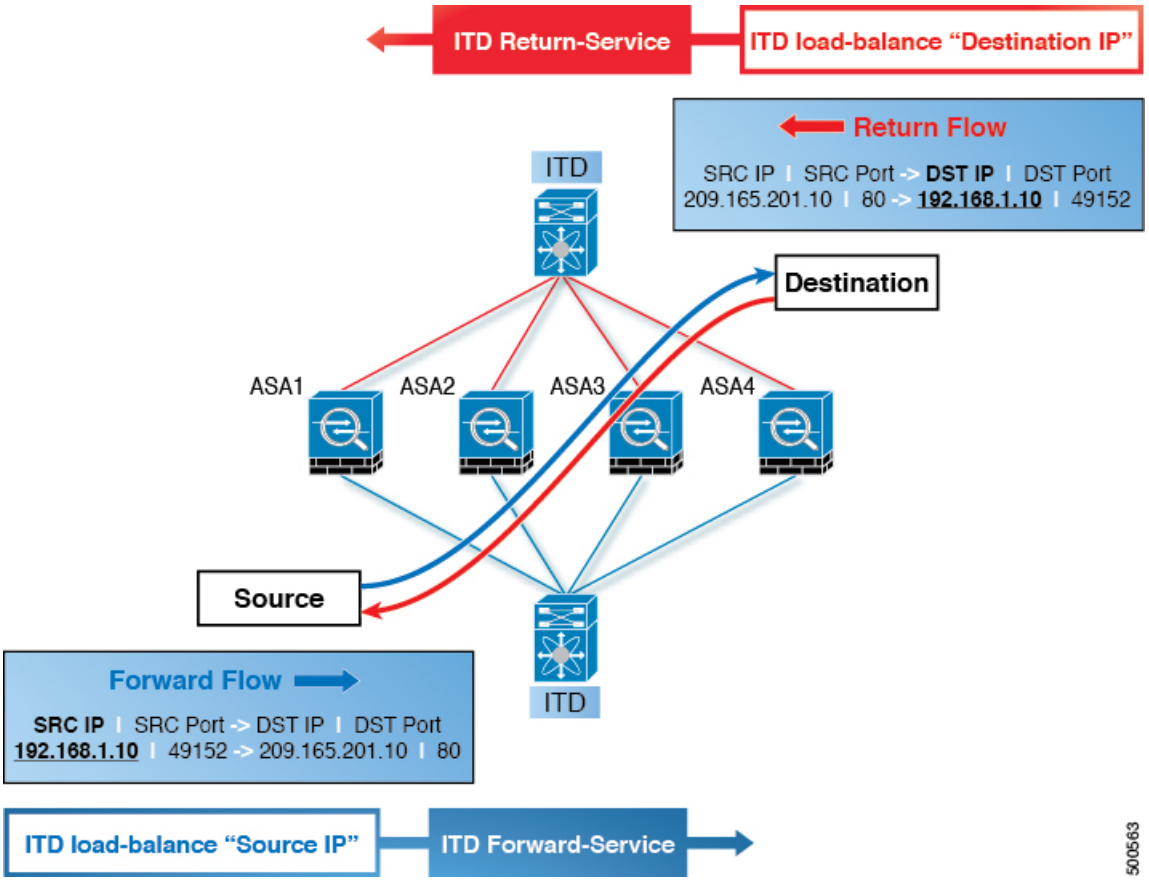
この図は、VLAN 10 および 20 を、ネットワーク上の送信元および接続先への内部および外部インターフェイスとして示しています。VLAN 100 および 200 は、ループのないトラフィックを確保するために ASA に対して使用されます。

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 *8 : ITD ASA* 展開におけるフローの対称性

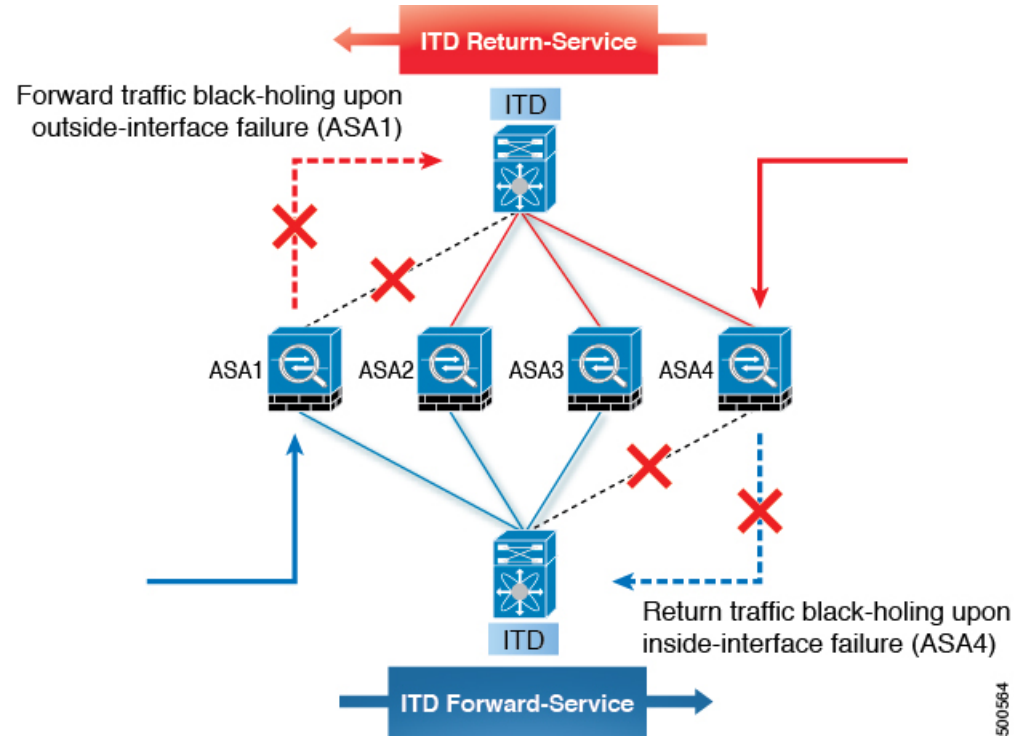


この図は、順方向フローの送信元 IP アドレスと逆方向フローの宛先 IP アドレスがどのように一定であるかを示しています。各 ITD サービスに適切なパラメータを選択すると、ITD IP の永続性によるフローの対称性が保証されます。

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 *9*: *ASA* 障害シナリオ

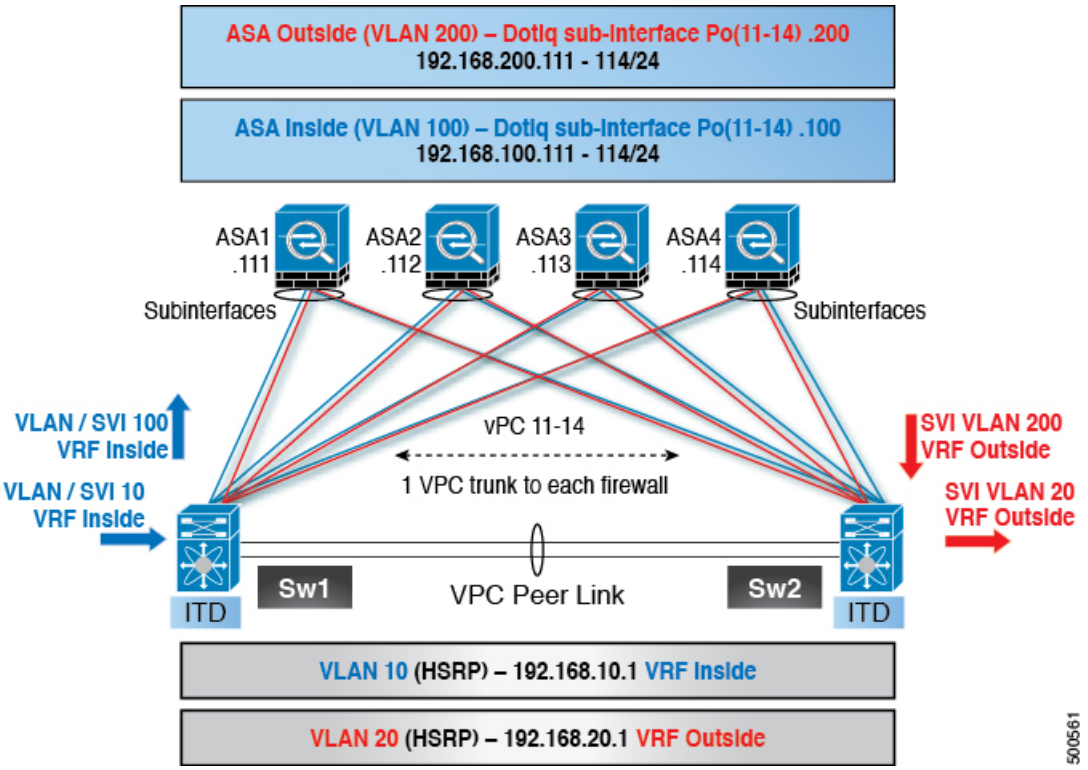


ITD ピア スイッチ ノード状態同期機能は、デュアル スイッチの非 vPC（またはシングル スイッチ）トポロジでのみサポートされます。ASA クラスタリングは、このような障害が発生した場合に ASA が完全に停止することを保証するため、この問題も解決します。ファイアウォール オン スティックの実装（シングル リンクまたは vPC）では、この問題に対処できません。これは、ASA の内部インターフェイスと外部インターフェイスが同じ物理（または仮想）インターフェイスに属しているためです。

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 *10* : 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。

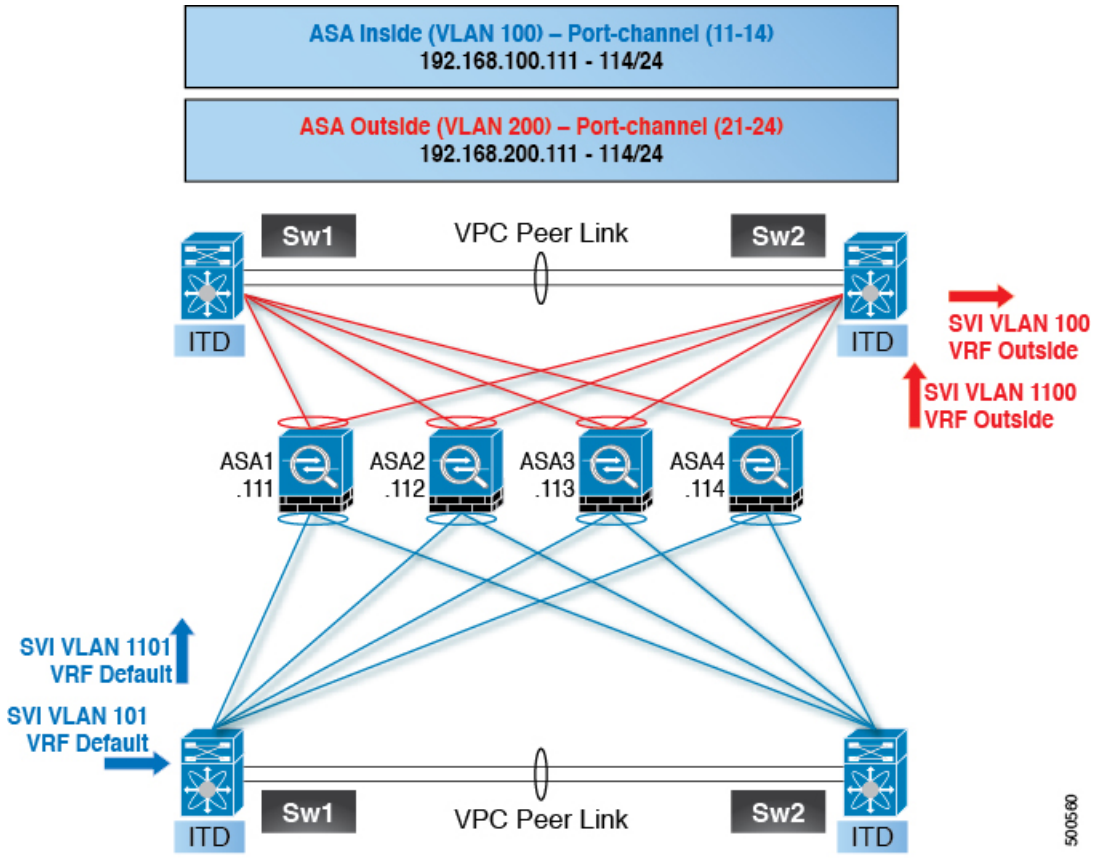
- VLAN 10、20、100、および 200 とそれらの SVI は、適切な VRF にマッピングされます。
- この例では、ITD ロードバランシング設定を使用してフローの対称性を実現しています。
- vPC シナリオでは、vPC の 1 つのメンバーが稼働している限り、ITD に変更はありません。vPC レッグに障害が発生したスイッチの ITD リダイレクションは、通常の vPC 配置の場合と同様に、ピア リンクを介してピア スイッチを通過します。

- 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 *11 : 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。

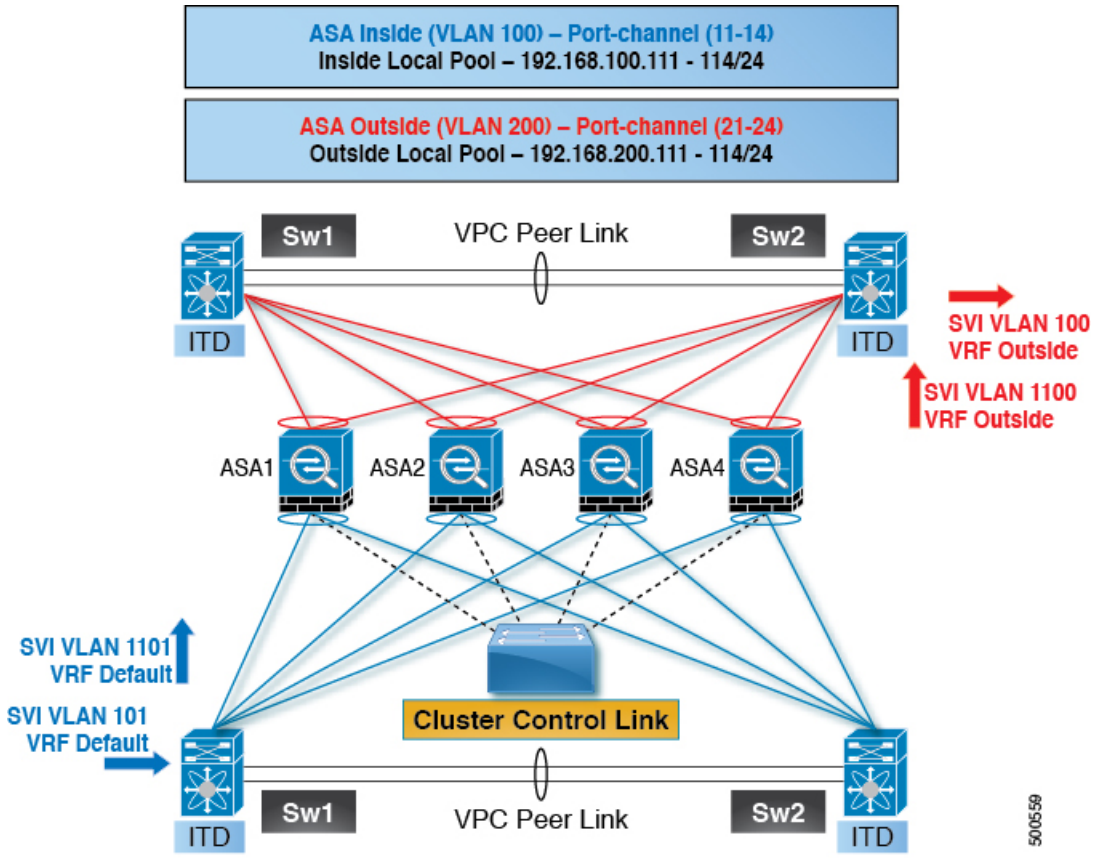
ITD で ASA クラスタリングを使用する場合の潜在的な欠点は、バックアップ フローおよびその他のクラスタ テーブル操作が、非クラスタ化ファイアウォールでは消費されないメモリと CPU リソースを消費することです。したがって、非クラスター化ファイアウォールを使用すると、ファイアウォールのパフォーマンスが向上する場合があります。

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。
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 *12 : 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。

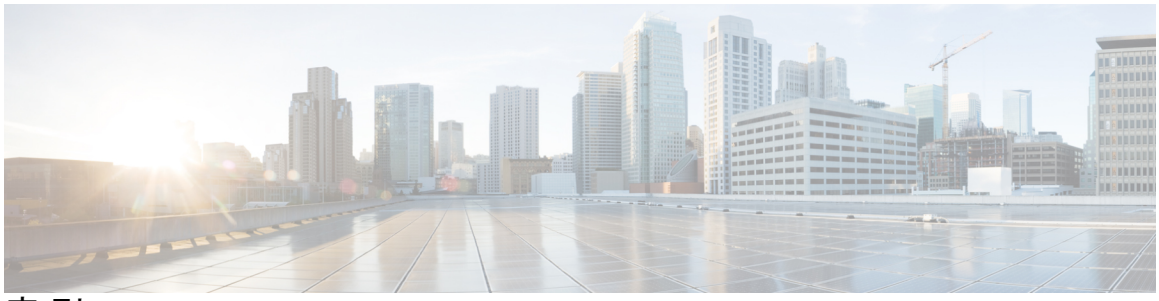
```
cluster group ASA-CLUSTER-L3
  local-unit ASA1
  cluster-interface port-channel 31
  ip address 192.168.250.100 255.255.255.0
  piority 1
  health-check holdtime 1.5
  clacp system-mac auto system-priority 1
  enable

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。

関連資料

関連資料



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。