Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director コンフィギュレーション ガイド

初版：2015 年 07 月 30 日

最終更新：2016 年 02 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/

Text Part Number: OL-32044-01-J

【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

ここでは、『*Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director* コンフィギュレーション ガイド』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

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。

表記法	説明
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、角カッコ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、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコ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。角カッコ内の波カッコと縦棒は、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、screen 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。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

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。
ciscodfa-docfeedback@cisco.com

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

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

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *1*：新規および変更された *ITD* 機能

機能	説明	変更されたリリース
許可 ACL	この機能が導入されました。	7.3(0)D1(1)
最適化されたノード挿入/削除	この機能が導入されました。	7.3(0)D1(1)
宛先 NAT	この機能が導入されました。	7.2(1)D1(1)
ITD サービス内の複数のデバイスグループ	この機能が導入されました。	7.2(1)D1(1)

新機能および変更された機能に関する情報

機能	説明	変更されたリリース
Intelligent Traffic Director	次の拡張機能が追加されました。 • ノードごとのプローブ。 • IPv6 データ ノードに対する IPv4 制御プローブ。 • リダイレクションからトラフィックを除外する除外 ACL。	7.2(0)D1(1)
Intelligent Traffic Director	次の拡張機能が追加されました。 • 重み付けロードバランシング。 • ノードレベルのスタンバイ。 • レイヤ 4 ポートのロードバランシング。 • 同じデバイス上の 2 つの VDC 間でのサンドイッチ モード ノード状態同期。 • DNS プローブ。 • ITD 統計情報収集の開始/停止/クリア。 • ITD サービスとプローブに対する VRF サポート。	6.2(10)
Intelligent Traffic Director	この機能が導入されました。	6.2(8)

第 2 章

ITD の設定

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

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ITD の概要

Intelligent Traffic Director（ITD）は、テラビット規模のスイッチとギガビット規模のサーバやアプライアンスとの間のパフォーマンス ギャップに対処する、インテリジェントでスケーラブルなクラスタリングおよびロード バランシング エンジンです。ITD アーキテクチャは、レイヤ 2 およびレイヤ 3 スイッチングに、レイヤ 4 からレイヤ 7 のアプライアンスを統合して規模と容量を拡大し、高帯域幅アプリケーションに対処します。

ITD では適応型ロード バランシングを行って、トラフィックをアプリケーション クラスタに分散します。Cisco Nexus 7000 シリーズ スイッチに備わったこの機能により、ネットワークやトポロジをアップグレードすることなく、あらゆるベンダーのサーバおよびアプライアンスを配置できます。

ITD 機能の概要

Intelligent Traffic Director は簡易性、柔軟性、および拡張性を提供します。これにより、お客様は外部ハードウェアを使用せずに、さまざまな使用例でトラフィック分散ソリューションを簡単に導入できます。一般的な導入シナリオをいくつかご紹介します。

- ファイアウォール クラスタの最適化
- 侵入防御システムや侵入検知システムなどのセキュリティ サービスの予測可能な冗長化と拡張
- 企業およびサービス プロバイダー向けの大規模な DNS ソリューション
- SSL アクセラレータや HTTP 圧縮などの特殊な Web サービスの拡張
- ネットワークのデータ プレーンを使用した高帯域幅アプリケーションの配信

Cisco ITD 機能は次の使用例に対応しています。

- それぞれが 10 Gbps の 256 台のサーバに対するトラフィックのロードバランシング。
- ファイアウォール クラスタへのロードバランシング。ITD はポリシーベース ルーティング（PBR）よりも優れています。
- スタンドアロン デバイスへのロードバランシングによる NG IPS および WAF の拡張。

- WAAS/WAE ソリューションの拡張。
- VDS-TC（ビデオキャッシュ）ソリューションの拡張。
- ECMP またはポートチャネルの置き換えによる再ハッシュの回避。ITD は復元力を備えています。

ITD の利点

Cisco NX-OS スイッチ上の ITD は、次の利点をもたらします。

高い拡張性

- レイヤ 3 および 4 サービスとアプリケーションのロード バランシングおよびトラフィック リダイレクトに対するハードウェア ベースのマルチテラビット規模の拡張性
- ラインレート 1、10、40、および 100 ギガビット イーサネット（GE）のパフォーマンスが高いトラフィック分散接続

運用の簡素化

- アプライアンスとサーバ クラスタリングの透過的な接続
- 最適化された迅速かつ簡単なプロビジョニング

投資保護

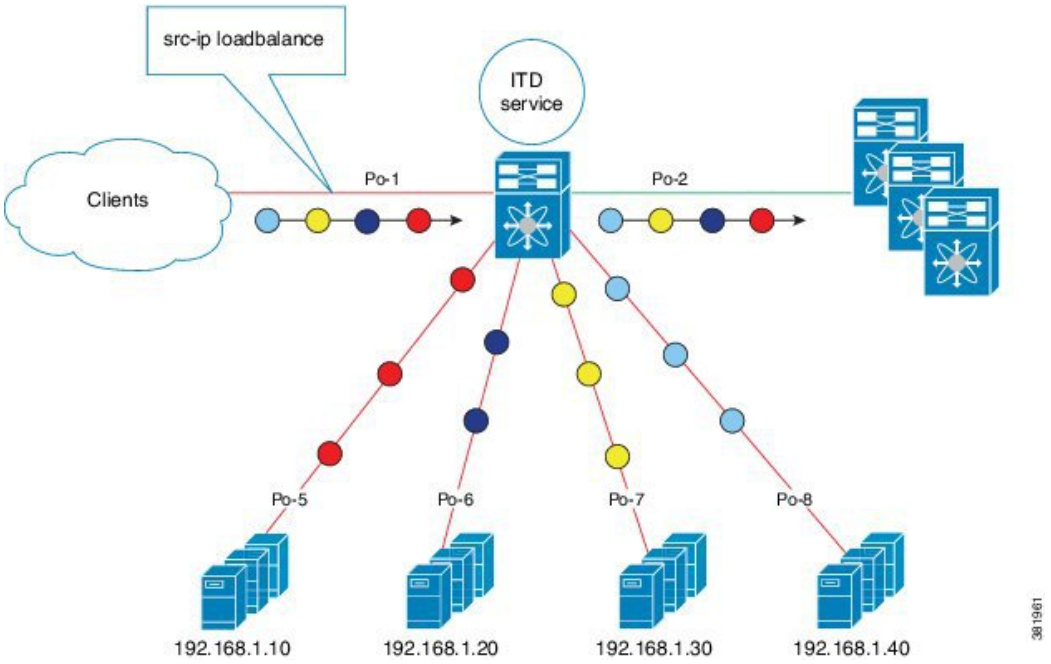
- すべての Cisco Nexus 5000、6000、7000、および 9000 スイッチング プラットフォームでサポートされます。新しいハードウェアは必要ありません。
- エンド デバイスを選びません。すべてのサーバおよびサービス アプライアンスがサポートされます。

展開モード

ワンアーム展開モード

サーバをワンアーム展開モードでCisco NX-OSデバイスに接続できます。このトポロジでは、サーバはクライアントトラフィックまたはサーバ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。

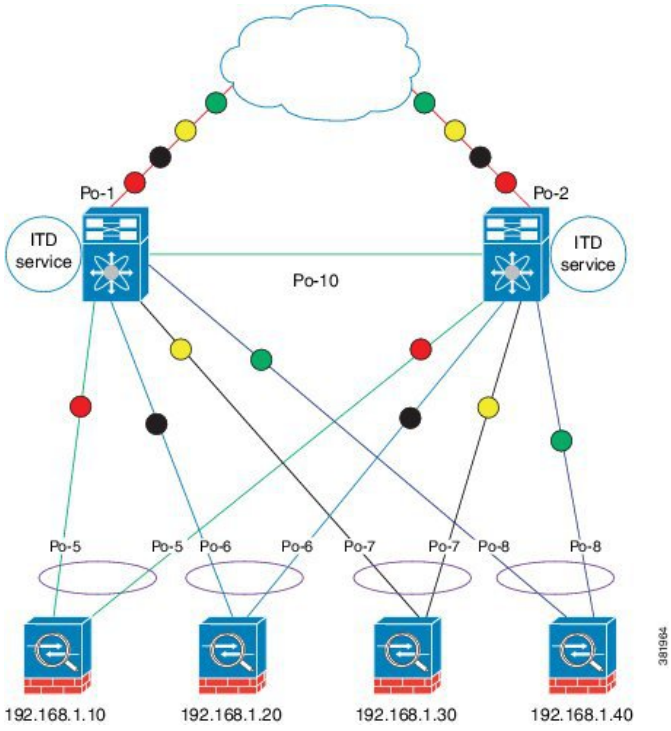
図 *1*：ワンアーム展開モード



VPC でのワンアーム展開モード

ITD 機能は、仮想ポート チャネル（vPC）に接続されたアプライアンス クラスタをサポートします。ITD サービスは各 Cisco NX-OS 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。

図 *2*：*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 Cisco NX-OS 7000 シリーズ 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。

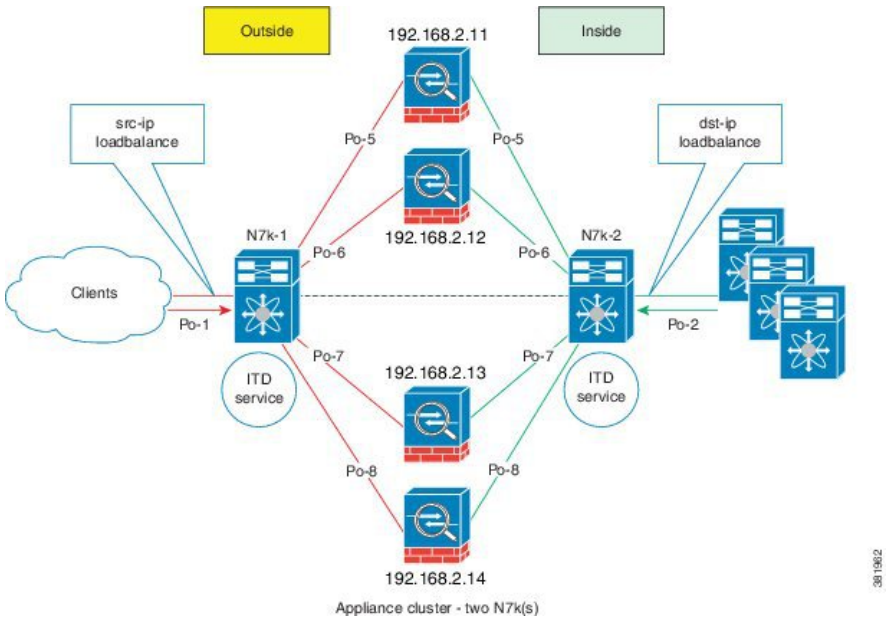
このモードの主な要件は、フローのフォワードトラフィックとリバーストラフィックの両方が同じアプライアンスを通過しなければならないことです。サンドイッチ展開の例としては、クライアントとサーバ間のトラフィックが同じアプライアンスを通過する必要があるファイアウォールおよびロード バランサの展開があります。

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）。
- 送信元 IP ロードバランシング スキーム（ITD サービスは外部に接続する入力方向のインターフェイス上で動作します）。

- 宛先 IP ロードバランシング スキーム（ITD サービスはサーバに接続する入力方向のインターフェイス上で動作します）。

図 *3*：サンドイッチ展開モード

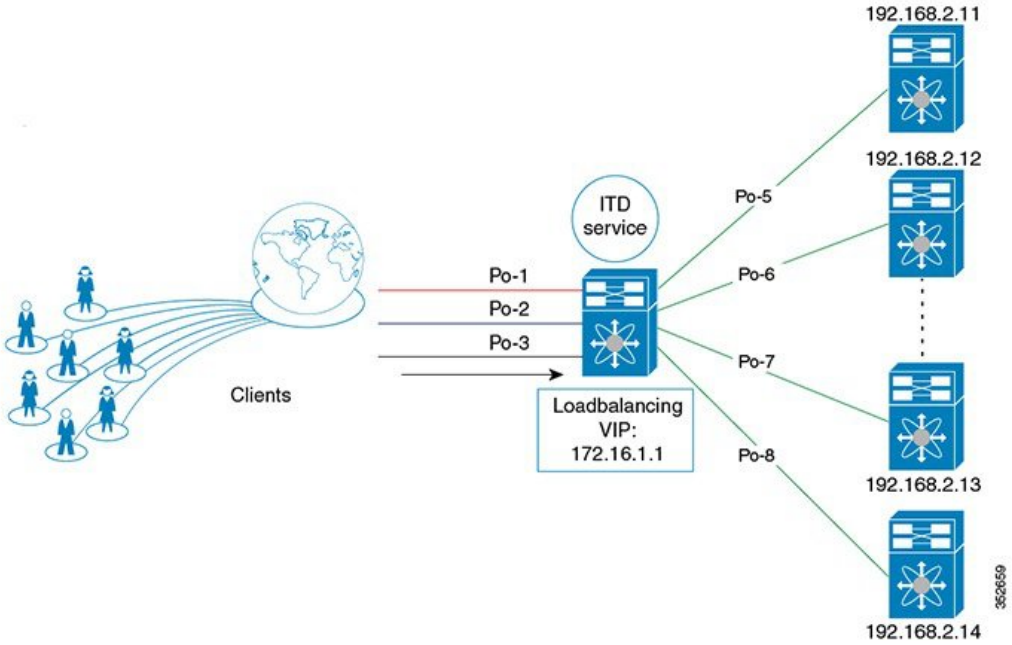


サーバ ロード バランシング展開モード

ITD サービスは、Cisco NX-OS 7000 シリーズ スイッチ上の仮想 IP（VIP）をホストするように設定できます。VIP を宛先とするインターネット トラフィックの負荷は、アクティブ ノードに分散されます。従来のサーバ ロード バランサとは違い、ITD サービスはステートフル ロード バランサではないため、送信元 NAT は不要です。

（注） 各 Cisco NX-OS 7000 シリーズ スイッチで、ITD サービスを同じように設定する必要があります。この ITD サービスの設定は、スイッチごとに手動で行う必要があります。

図 *4*：*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）とは、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る機能です。宛先 NAT はロード バランシングに使用される NAT タイプの 1 つです。

宛先 NAT の利点

ITD 展開で NAT を使用した場合の利点は次のとおりです。

- サーバ プール内のすべてのサーバで仮想 IP アドレスをホストする必要がありません。
- サーバ IP を認識する必要がないクライアントは、トラフィックを常に仮想 IP アドレスに送信します。
- ロードバランサによってサーバ障害が検出され、クライアントがプライマリ サーバのステータスを認識していなくても、トラフィックは適切なサーバにリダイレクトされます。
- NAT は実サーバの IP をクライアントに対して隠すことでセキュリティを確保します。

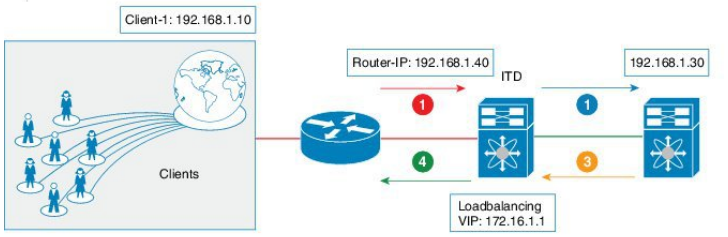
- NAT により、異なるサーバ プール間で実サーバを移動する際の柔軟性が向上します。

NAT には異なるタイプがありますが、一般には次の利点が得られるため宛先 NAT がロード バランシングに導入されます。

- 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、書き換えられてサーバにリダイレクトされる。
- 送信元またはクライアントから宛先またはサーバへのトラフィック（フォワードパス）の処理では、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が変換されて、送信元から宛先またはサーバへのトラフィックとしてリダイレクトされる。
- 宛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 アドレスによって送信元 IP アドレスに再変換される。つまり、サーバまたは送信元からクライアントまたは宛先へのトラフィックが、クライアントまたは送信元からクライアントまたは宛先へのトラフィックに変換される。

次の図は、仮想 IP アドレスを使った NAT を示しています。

図 *5*： 仮想 *IP* アドレスによる *NAT*



Step	dst-mac	src-mac	src-ip	dst-ip
1	N7K MAC	Router MAC	192.168.1.10	192.168.1.20
2	Server MAC	N7K MAC	192.168.1.10	192.168.1.30
3	N7K MAC	Server MAC	192.168.1.30	192.168.1.10
4	Router MAC	N7K MAC	192.168.1.20	192.168.1.10

354187

デバイス グループ

ITD 機能は、デバイス グループをサポートしています。デバイス グループを設定する際に、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

ITD サービス内の複数のデバイスグループ

この機能を使って同じインターフェイス上のサービスごとに複数のデバイスグループを設定できるので、ITD の拡張が可能です。

1つの入力インターフェイスからのトラフィックは、VIP とデバイスグループの両方に基づいて分散されます。

ITD サービスは、異なるデバイスグループのノードを指定するネクスト ホップを含むルートマップを 1 つ生成します。

最適化されたノード挿入またはノード削除

この機能を使用すると、ユーザは既存のトラフィックの中断を最小限に抑えながら、ノードを動的に追加または削除することができます。ITD では、アクティブなサービスでノードが削除または追加されたときにノードの断続的な状態が維持されるようになりました。また、サービスの中断を最小限に抑えてノードを追加または削除すると、ITD は自動的にバケットを再プログラムします。この機能は、次でサポートされます。

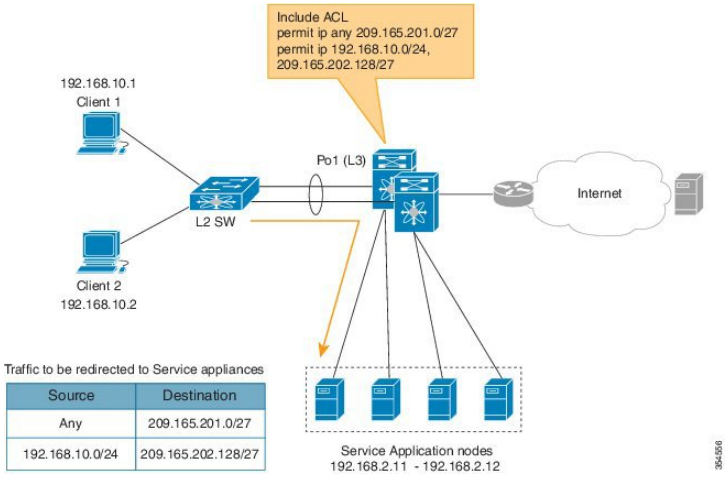
- デバイスグループ レベル
- 仮想 IP アドレス（VIP）、さらに VIP なしでも可
- 複数の VIP デバイスグループ機能

許可 ACL

許可 ACL 機能を使用すると、ITD で許可する IP アドレスを定義することで ITD のロードバランシングの対象となるトラフィックを選択できます。この機能で設定された ACL では、ロードバランシング用にトラフィックを照合する許可 ACE を定義します。ACL で一致しないアドレスは ITD をバイパスします。許可 ACL および除外 ACL 機能を併用して、ITD 内でトラフィックを詳細に選択することができます。この両方の ACL には許可 ACE のみを含めることができます。拒否 ACE は使用できません。サービス アプライアンスが特定のインターネット トラフィックにのみ

対応する状況では、ITD はトラフィックを選択してロードバランシングまたはリダイレクトを実行します。残りのトラフィックは RIB によって通常どおりルーティングされます。

図 *6*：許可 *ACL*



許可 ACL 機能は、ITD 内でトラフィックを選択してトラフィック フィルタリングを実行するために使用されます。VIP 機能で照合できるのは宛先フィールドのみですが、許可 ACL 機能では、送信元と宛先の両方のフィールドを照合できます。

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 でも設定できます。

ITD サービスでトラフィックをリダイレクトするには、入力インターフェイスおよびデバイス グループ ノードのすべてが同じ VRF に属している必要があります。設定済み VRF で、関連するデバイス グループのすべての入力インターフェイスおよびノードメンバーが到達可能であることを確認する必要があります。

ロード バランシング

ITD 機能では、**loadbalance** コマンドを使用して特定のロードバランシング オプションを設定することができます。

loadbalance コマンドのオプションのキーワードは次のとおりです。

- **buckets**：作成するバケットの数を指定します。バケットは 2 のべき乗数で設定する必要があります。1 つ以上のバケットが、クラスタ内の 1 つのノードにマッピングされます。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**：ロードバランシングのマスク位置を指定します。このキーワードは、IP アドレスの特定のオクテットまたはビットに基づいてパケット分類を行わなければならない場合

に役立ちます。デフォルトでは、システムは最後のオクテットまたは最下位ビット（LSB）をバケットに使用します。デフォルト以外のビット/オクテットを使用する場合、**mask-position** キーワードを使用して、トラフィック分類の開始点を指定できます。たとえば、IPアドレスの第 2 オクテットの 8 番目のビットと第 3 オクテットの 16 番目のビットで開始することができます。

- **src** または **dst ip**：送信元または宛先IPアドレスに基づくロードバランシングを指定します。
- **src ip** または **src ip-l4port**：送信元 IP アドレス、または送信元 IP アドレスと送信元 L4 ポートに基づくロード バランシングを指定します。
- **dst ip** または **dst ip-l4port**：宛先 IP アドレス、または宛先 IP アドレスと宛先 L4 ポートに基づくロード バランシングを指定します。

ホット スタンバイ

ITD は、N+1 冗長性をサポートしています。N+1 冗長性では、M ノードが N アクティブ ノードのスタンバイ ノードとして機能できます。

アクティブ ノードに障害が発生すると、ITD は運用可能なスタンバイ ノードを検索し、最初に使用可能なスタンバイ ノードを選択して、障害が発生したノードに置き換えます。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、新しくアクティブになった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、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運用可能になると、そのノードはアクティブ ノードとして復帰します。この場合、アクティブ ノードとして機能していたスタンバイ 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、スタンバイ ノードはスタンバイ ノードのプールに戻されます。

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、最初に使用可能なスタンバイ ノードにリダイレクトされます。

ノードは、ノードレベルまたはデバイス グループレベルでスタンバイとして設定できます。ノードレベルのスタンバイは、関連付けられたアクティブ ノードで障害が発生した場合にのみトラフィックを受信します。デバイス グループレベルのスタンバイは、いずれかのアクティブ ノードで障害が発生した場合にトラフィックを受信します。

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 サービスを設定できます。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。**ingress interface** コマンドを使用して、複数の入力インターフェイスを設定できます。

同じ入力インターフェイスを 2 つの ITD サービスに設定できるので、1 つの IPv4 ITD サービスと 1 つの IPv6 ITD サービスをそれぞれ使用することができます。

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設定すると、IPv4 および IPv6 トラフィックをどちらも同じ入力インターフェイスで受信できます。IPv4 トラフィックのリダイレクトには IPv4 ITD ポリシーが適用され、IPv6 トラフィックのリダイレクトには IPv6 ITD ポリシーが適用されます。

（注） 入力インターフェイスを複数の IPv4 ITD サービスや複数の IPv6 ITD サービスに設定しないでください。この設定は自動的にチェックされません。

システム ヘルス モニタリング

ITD は、次を目的としたヘルス モニタリング機能をサポートしています。

- ITD チャネルとピア ITD サービスを監視する。
- 各ノードに接続されているインターフェイスの状態を監視する。
- 設定済みプローブを使用して、ノードの正常性を監視する。
- 入力インターフェイスの状態を監視する。

ヘルス モニタリングにより、次の重大なエラーが検出および修正されます。

- ITD サービスが shut/no shut または削除されている。
- iSCM プロセスのクラッシュ。
- iSCM プロセスの再起動。
- スイッチのリブート。
- スーパーバイザ スイッチオーバー。
- インサービス ソフトウェア アップグレード（ISSU）。
- ITD サービス ノード障害。
- ITD サービス ノード ポートまたはインターフェイスのダウン。
- 入力インターフェイスのダウン。

ノードの監視

ITD ヘルス モニタリング モジュールは、障害の検出および障害シナリオの処理を目的に、定期的にノードを監視します。

ヘルス モニタリング用に各ノードを定期的にプローブで検査するため、ICMP、TCP、UDP、および DNS プローブがサポートされています。プローブはデバイス グループ レベルまたはノード レベルで設定できます。デバイス グループ レベルで設定したプローブは、デバイス グループの各ノード メンバーに送信されます。ノード レベルで設定したプローブは、関連付けられているノー

ドのみに送信されます。ノード固有のプローブを設定すると、そのプローブのみが当該ノードに送信されます。ノード固有のプローブが設定されていないすべてのノードには、デバイス グループ レベルのプローブ（設定されている場合）が送信されます。

IPv6 データ ノードの IPv4 制御プローブ

IPv6 デバイス グループの IPv6 ノードについては、ノードがデュアルホーム ノード（IPv4 および IPv6 ネットワーク インターフェイスをサポートする）である場合、IPv4 プローブを設定して正常性を監視できます。IPv6 プローブはサポートされていないため、この方法で IPv4 プローブを使用して IPv6 データ ノードの正常性を監視できます。

（注） IPv6 プローブはサポートされません。

ノードに接続されたインターフェイスの正常性

ITD は IP サービス レベル契約（IP SLA）機能を活用して、定期的に各ノードをプローブで検査します。プローブは 1 秒の頻度ですべてのノードに同時に送信されます。クラスタ グループ設定の一部としてプローブを設定できます。プローブは、3 回再試行した後に障害が発生したと宣言されます。

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 ノードが設定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。

ピア ITD サービスのモニタ

サンドイッチ モード クラスタ展開の場合、ITD サービスは各 Cisco NX-OS 7000 シリーズ スイッチで実行されます。両方向でフローがクラスタ ノードを通過する一貫したトラフィックを確立するためには、ITD チャネルの正常性が重要です。

各 ITD サービスはピア ITD サービスを定期的にプローブで検査して、障害を検出します。ping はピア ITD サービスに毎秒送信されます。応答がない場合は 3 回再試行されます。頻度と再試行回数は設定できません。

（注） ワンアーム展開モードのスイッチで実行される ITD サービスのインスタンスは 1 つのみなので、ピア ITD のモニタリングは適用されません。

ITD チャネル障害の処理

ハートビート信号の未送信が 3 回続くと、ITD チャネルはダウンしていると見なされます。

ITD チャネルがダウンしている間も、トラフィックはクラスタ ノードを通過します。ただし、各スイッチの ITD サービスがクラスタ グループのビューに関する情報を交換できないため、この状態に迅速に対処する必要があります。ITD チャネルがダウンしていると、ノード障害が発生したときにトラフィックの損失につながる可能性があります。

Failaction 再割り当て

ITD の Failaction により、障害が発生したノード上のトラフィックを、最初に使用可能なアクティブ ノードに再割り当てできます。障害が発生したノードが復旧すると、そのノードは自動的に接続の提供を再開します。この機能をイネーブルにするには、**failaction** コマンドを使用します。

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、設定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。障害が発生したノードがアクティブ状態に戻ると、トラフィックはこの新しいノードに戻され、ノードによる接続の提供が再開されます。

（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。

スタンバイ ノードを使用しない Failaction 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、設定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 バケット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。障害が発生したノードがアクティブ状態に戻ると、トラフィックはこの新しいノードに戻され、ノードによる接続の提供が開始されます。

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。

- ノードがダウンすると（プローブが失敗した場合）、トラフィックは最初に使用可能なアクティブ ノードに再割り当てされます。
- ノードが障害状態から復旧すると（プローブが成功した場合）、接続の処理を開始します。
- 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。

スタンバイ ノードを使用した Failaction 再割り当て

ノードがダウンした場合、スタンバイ ノードがアクティブであれば、トラフィックは接続に対応し、バケット割り当ての変更は行われません。アクティブ ノードとスタンバイ ノードの両方がダウンした場合、ノードに関連付けられたトラフィック バケットは、設定済みの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 バケット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。障害が発生したノードがアクティブ状態に戻ると、トラフィックはこの新しいノードに戻され、ノードによる接続の提供が開始されます。

- ノードがダウンし（プローブが失敗した場合）、有効なスタンバイ ノードがない場合、トラフィックは最初に使用可能なアクティブ ノードに送信されます。
- スタンバイ ノードを含むすべてのノードがダウンした場合、トラフィックは最初に使用可能なアクティブ ノードに再割り当てされます。
- ノードが障害状態から復旧すると（プローブが成功した場合）、接続の処理を開始します。
- 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。

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。

- シナリオ 1：プローブを設定する、かつ
  - スタンバイを設定する
  - スタンバイを設定しない
- シナリオ 2：プローブを設定しない

プローブを設定して Failaction 再割り当てを使用しない場合

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、スタンバイが設定されていれば、そのスタンバイ ノードが接続を引き継ぎます。
- ノードに障害が発生し、スタンバイが設定されていない場合、Failactionが設定されていないと、トラフィックはルーティングされます。この場合、トラフィックの再割り当ては行われません。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。

プローブを設定せずに Failaction 再割り当てを使用しない場合

プローブが設定されていないと、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。

除外 ACL

除外 ACL を設定して、ITD リダイレクションから除外するトラフィックを指定することができます。除外 ACL に一致するトラフィックは ITD リダイレクションから除外され、除外 ACL に一致しないトラフィックは ITD ポリシーによってリダイレクトされます。

ITD のライセンス要件

ITD には、拡張レイヤ 2 パッケージ ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ITD の前提条件

ITD には、次の前提条件があります。

- **feature itd** コマンドを使用して、ITD 機能をイネーブルにする必要があります。
- **feature itd** コマンドを入力する前に、次のコマンドを設定する必要があります。
  - **feature pbr**
  - **feature sla sender**
  - **feature sla responder**
  - **ip sla responder**

ITD の注意事項と制約事項

ITD 設定時の注意事項と制約事項は次のとおりです。

- 仮想 IP タイプおよび ITD デバイス グループ ノード タイプは IPv4 または IPv6 のいずれか一方でなければなりません。両方を混在させることはできません。
- コンフィギュレーション ロールバックは、ITD サービスがターゲットとソースの両方の設定で shut モードになっている場合にのみサポートされます。
- IPv6 プローブは IPv6 ノードのデバイス グループではサポートされていません。ただしノードがデュアルホーム接続されている（つまり IPv6 と IPv4 の両方のネットワーク インターフェイスがある）場合は、IPv6 データ ノードを監視するように IPv4 プローブを設定できます。
- **failaction** コマンドは、IPv4 に対してのみサポートされています。
- ITD では SNMP はサポートされていません。

最適化されたノード挿入/削除機能のサポートについては、次のとおりです。

- スタンバイ ノードおよびバックアップ ノードがない場合はサポートされます。
- 重み付けではサポートされません。
- NAT ではサポートされません（Cisco NX-OS 7000 シリーズ スイッチ）。
- 許可 ACL 機能が設定されている場合はサポートされません。
- ノード レベルのプローブではサポートされません。

Cisco NX-OS Release 7.3(0)D1(1) では、許可 ACL 機能は IPv4 でのみサポートされます。

ITD の設定

サーバはスイッチにルーテッド インターフェイスまたはポートチャネルを介して接続することも、SVI を設定したスイッチポート経由で接続することもできます。

ITD のイネーブル化

はじめる前に

feature itd コマンドを設定する前に、**feature pbr** および **feature ipsla** コマンドを入力する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **feature itd**	ITD 機能をイネーブルにします。

デバイス グループの設定

はじめる前に

ITD 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **itd device-group***name*	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。
ステップ 3	switch(config-device-group)# **node ip***ipv4-address*	ITD のノードを指定します。この手順を繰り返して、すべてのノードを指定します。 IPv6 ノードを設定するには、**node ipv6***ipv6-address* を使用します。 （注） ITD デバイス グループは、IPv4 または IPv6 ノードのいずれか一方で構成する必要があります。両方を混在させることはできません。
ステップ 4	switch(config_dg_node)# [**mode hot-standby**] [**standby***ipv4-address*] [**weight** *value*] [**probe**{**icmp**| **tcp** **port***port-number*| **udp** **port***port-number*| **dns** {*hostname*| *target-address*}}] [**frequency***seconds*] [[**retry-down-count**| **retry-up-count**] *number*] [**timeout***seconds*]	ITD のデバイス グループ ノードを指定します。この手順を繰り返して、すべてのノードを指定します。 **weight***value* キーワードは、重み付けトラフィック分散用にノードの適切な重みを指定します。 **mode hot-standby** は、このノードをデバイスグループのスタンバイ ノードにすることを指定します。 ノードレベルのスタンバイを各ノードに関連付けることができます。**standby** 値は、このアクティブ ノードのスタンバイ ノード情報を指定します。 ノードレベルのプローブを設定してノードの正常性を監視できます。**Probe** 値は、このアクティブ ノードの正常性を監視するために使用するプローブ パラメータを指定します。 （注） IPv6 プローブはサポートされません。
ステップ 5	switch(config-device-group)# **probe** {**icmp** | **tcp** **port***port-number* | **udp** **port***port-number* | **dns** {*hostname* |*target-address*} } [**frequency***seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout***seconds*]	クラスタ グループのサービス プローブを設定します。 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 • DNS

	コマンドまたはアクション	目的
		キーワードは次のとおりです。 • **retry-down-count**：ノードをダウン状態としてマークする条件となるプローブの連続失敗回数を指定します。 • **retry-up-count**：ノードをアップ状態としてマークする条件となるプローブの連続成功回数を指定します。 • **timeout**：プローブ応答を待機する秒数を指定します。 • **frequency**：ノードに連続して送信されるプローブの間隔を秒単位で指定します。 （注） IPv6 プローブはサポートされません。

ITD サービスの設定

はじめる前に

- ITD 機能をイネーブルにします。
- ITD サービスに追加するデバイスグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **itd***service-name*	ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
ステップ 3	switch(config-itd)# **device-group***device-group-name*	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。

	コマンドまたはアクション	目的
ステップ 4	switch(config-itd)# **ingress interface***interface*	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。
ステップ 5	switch(config-itd)# **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***position*}	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。キーワードは次のとおりです。 • **buckets**：作成するバケットの数を指定します。バケットは 2 のべき乗数で設定する必要があります。 • **mask-position**：ロードバランシングのマスク位置を指定します。 • **method**：送信元 IP アドレスまたは宛先 IP アドレス ベースのロード バランシング、または送信元 IP アドレスと送信元ポート ベースのロード バランシング、または宛先 IP アドレスと宛先ポート ベースのロード バランシング指定します。
ステップ 6	switch(config-itd)# **virtual ip***ipv4-addressipv4-network-mask* [**tcp** | **udp** {*port-number* | **any**}] [**advertise** {**enable** | **disable**}]	ITD サービスの仮想 IPv4 アドレスを設定します。 （注） 仮想 IPv6 アドレスを設定するには、**virtual ipv6** *ipv6-address ipv6-network-mask* | *ipv6-prefix/length*} [**ip** | **tcp** {*port-number* | **any**} | **udp** {*port-number* | **any**}] [**advertise** {**enable** | **disable**}] を使用します。 **advertise enable** キーワードは、仮想 IP ルートをネイバー デバイスにアドバタイズすることを指定します。 **tcp**、**udp**、**ip** キーワードは、仮想 IP アドレスが指定のプロトコルによるフローを受け入れることを指定します。
ステップ 7	switch(config-itd)# **failaction node reassign**	ノードで障害が発生した後のトラフィック再割り当てを有効にします。障害が発生したノードへのトラフィックは、最初に使用可能なアクティブ ノードに再割り当てされます。

	コマンドまたはアクション	目的
ステップ 8	switch(config-itd)# **vrf***vrf-name*	ITD サービスの VRF を指定します。
ステップ 9	switch(config-itd)# **no shutdown**	ITD サービスをイネーブルにします。
ステップ 10	switch(config-itd)# **exclude access-list***acl-name*	リダイレクションからトラフィックを除外します。**acl-name** は、ITD リダイレクションから除外する一致トラフィックを指定します。

宛先 NAT の設定

NAT 宛先を指定した任意の仮想 IP アドレスの設定

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`	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***service-name* 例： `switch (config) # itd nat1`	ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
ステップ 3	**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	**virtual ip***ipv4-address ipv4-network-mask* 例： `switch(config-itd)# virtual ip 172.16.1.10 255.255.255.255`	ITD サービスの仮想 IPv4 アドレスを設定します。
ステップ 5	**nat destination** 例： `switch(config-itd)# nat destination`	宛先 NAT を設定します。

	コマンドまたはアクション	目的
ステップ 6	**ingress interface interface next-hop** *ip-address* 例： `switch(config-itd)# ingress interface ethernet 3/1 next-hop 203.0.113.254`	1 つ以上の入力インターフェイスを ITD サービスに追加し、ネクストホップ IP アドレス（設定する入力インターフェイスに直接接続されたインターフェイスの IP アドレス）を設定します。
ステップ 7	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。

NAT 宛先とポートを指定した仮想 IP アドレスの設定

はじめる前に

ITD 機能をイネーブルにします。

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`	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***service-name* 例： `switch (config) # itd nat1`	ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
ステップ 3	**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	**virtual ip***ipv4-address ipv4-network-mask* **80** *80* 例： `switch(config-itd)# virtual ip 172.16.1.10 255.255.255.255`	ITD サービスの TCP ポートと仮想 IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**nat destination** 例： `switch(config-itd)# nat destination`	宛先 NAT を設定します。
ステップ 6	**ingress interface interface next-hop** *ip-address* 例： `switch(config-itd)# ingress interface ethernet  3/1 next-hop 192.168.1.70`	1 つ以上の入力インターフェイスを ITD サービスに追加し、ネクストホップ IP アドレス（設定する入力インターフェイスに直接接続されたインターフェイスの IP アドレス）を設定します。
ステップ 7	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。

NAT 宛先およびポート変換を指定した複数の仮想 IP の設定

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`	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 device-group***name* 例： `switch(config)# itd device-group dg`	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 3	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.20`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 4	**exit** 例： `switch# exit`	ITD デバイス グループ コンフィギュレーション モードを終了して、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。

	コマンドまたはアクション	目的
ステップ 5	**itd***service-name* 例： `switch (config) # itd nat1`	ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
ステップ 6	**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 7	**virtual ip***ipv4-address ipv4-network-mask* 例： `switch(config-itd)# virtual ip 172.16.1.10 255.255.255.255`	ITD サービスの仮想 IPv4 アドレスを設定します。
ステップ 8	**virtual ip***ipv4-address ipv4-network-mask* 例： `switch(config-itd)# virtual ip 172.16.1.20 255.255.255.255`	ITD サービスの仮想 IPv4 アドレスを設定します。
ステップ 9	**nat destination** 例： `switch(config-itd)# nat destination`	宛先 NAT を設定します。
ステップ 10	**ingress interface***interface slot/port* 例： `switch(config-itd)# ingress interface ethernet 3/1`	入力インターフェイスを ITD サービスに追加します。

最適化されたノード挿入またはノード削除の設定

最適化されたノード挿入の設定

ITD サービスの設定

はじめる前に

- 包含 ACL 機能を設定するには、loadbalance コマンドを設定する必要があります。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 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。
switch(config)# **itd device-group***name*

ステップ 3 ITD のノードを指定します。

- 3 つのノードを指定するには、この手順を 3 回繰り返して次の IP アドレスを毎回 1 つずつ使用します。
  - 10.2.1.10
  - 10.2.1.20
  - 10.2.1.30
- IPv6 ノードを設定するには、**node ipv6***ipv6-address* を使用します。

switch(config-device-group)# **node ip***ipv4-address*

ステップ 4 ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
switch(config-device-group) #**itd service-name**

ステップ 5 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。
switch(config-itd)# **device-group***device-group-name*

ステップ 6 入力インターフェイスを ITD サービスに追加します。
switch(config-itd)# **ingress interface***interfaceslot/port*

ステップ 7 ITD デバイスをイネーブルにします。
switch(config-itd)# **no shutdown**

ノードを挿入する ITD セッションの作成

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 ITD セッションを作成します。
switch# **itd session device-groupwebservers**

ステップ 3 ITD のノードを指定します。この手順を繰り返して、すべてのノードを指定します。
switch(config-device-group)# **node ip**

ステップ 4 設定をピア スイッチと同期させ、設定をローカルに適用するには、**commit** コマンドを使用します。設定は、**commit** コマンドが発行されるまでバッファ内に格納されます。
switch(config-device-group)#**commit**

最適化されたノード挿入の例

以下に示すのは、最適化された挿入を設定するシナリオでのノード分散です。

デバイス グループに 3 つのノードがあり、デフォルト バケットは次のように分散されています。

Node1 = バケット 1 および 4

Node2 = バケット 2

Node3 = バケット 3

4 つ目のバケットが追加されると、新しく追加されたノード（Node4）に 4 つ目のバケットが再分散されるので、次のような分散になります。

デバイス グループに 3 つのノードがあり、デフォルト バケットは次のように分散されています。

Node1 = バケット 1

Node2 = バケット 2

Node3 = バケット 3

Node4 = バケット 4

別のノードを追加する場合は、新しいバケットが必要です。これは常に次の 2 のべき乗数になります。したがって、5つ目のノードを追加すると、8個のバケットがデフォルトで作成されます。

その場合の分散は次のとおりです。

Node1 = バケット 1 および 6

Node2 = バケット 2 および 7

Node3 = バケット 3 および 8

Node4 = バケット 4

Node5 = バケット 5

設定例：最適化されたノード挿入の設定

次に、実行コンフィギュレーションの例を示します。

```
configure terminal
 itd device-group webservers
  node ip 10.2.1.10
  node ip 10.2.1.20
  node ip 10.2.1.30
  itd http_service
   device-group webservers
   ingress interface Ethernet 3/1
   no shutdown
   exit
 itd session device-group webservers
  node ip 10.2.1.40
  commit
```

最適化されたノード削除の設定

ノードを削除する ITD セッションの作成

はじめる前に

ITD サービスを設定します。デバイス グループ *webservers* にノードが 4 つある ITD サービス *http_service* については、前のタスクの設定を参照してください。他のノードへのサービスに影響を与えずにサービスを削除するには、次の手順を使用します。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 ITD セッションを作成します。
switch(config)#**itd session device-group***name*

ステップ 3 削除するノードを指定します。これは設定済みのデバイスグループにすでに含まれているノードです。
switch(config)# **no node ip***ipv4-address*

ステップ 4 ITD のノードを指定します。
switch(config-device-group)# **node ip***ipv4-address*

ステップ 5 設定をピア スイッチと同期させ、設定をローカルに適用するには、**commit** コマンドを使用します。設定は、**commit** コマンドが発行されるまでバッファ内に格納されます。

switch(config-device-group)# **commit**

最適化されたノード削除の例

ノードを削除すると、これに関連付けられていたバケットは、デバイス グループ内の最初のノードから順にバケットの割り当てが最も少ないノードに再分散されます。

Node1 = バケット 1

Node2 = バケット 2

Node3 = バケット 3

Node4 = バケット 4

ここで Node2 が削除されると、バケット分散は次のようになります。

デバイス グループに 3 つのノードがあり、デフォルト バケットは次のように分散されています。

Node1 = バケット 1 および 2

Node2（削除）

Node3 = バケット 3

Node4 = バケット 4

設定例：最適化されたノード削除の設定

次に、実行コンフィギュレーションの例を示します。

```
configure terminal
 itd device-group webservers
  node ip 10.2.1.10
  node ip 10.2.1.20
  node ip 10.2.1.30
  itd http_service
  device-group webservers
  ingress interface Ethernet 3/1
  no shutdown
  exit
 itd session device-group webservers
  no node ip 10.2.1.20
```

最適化されたノード置換の設定

ノードを置換する ITD セッションの作成

はじめる前に

ITD サービスを設定します。デバイス グループ *webservers* にノードが 4 つある ITD サービス *http_service* については、前のタスクの設定を参照してください。他のノードへのサービスに影響を与えずにサービスを置換するには、次の手順を使用します。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 ITD セッションを作成します。
switch(config)# **itd session device-group***name*

ステップ 3 削除するノードを指定します。
switch(config-device-group)# **no node ip***ipv4-address*

ステップ 4 追加するノードを指定します。
switch(config-device-group)# **node ip***ipv4-address*

ステップ 5 設定をピア スイッチと同期させ、設定をローカルに適用するには、**commit** コマンドを使用します。設定は、**commit** コマンドが発行されるまでバッファ内に格納されます。
switch(config-device-group)# **commit**

最適化されたノード置換の例

ノードを削除すると、これに関連付けられていたバケットは、デバイス グループ内の最初のノードから順にバケットの割り当てが最も少ないノードに再分散されます。

Node1 = バケット 1

Node2 = バケット 2

Node3 = バケット 3

Node4 = バケット 4

ここで Node2 が削除されると、バケット分散は次のようになります。

デバイス グループに 3 つのノードがあり、デフォルト バケットは次のように分散されています。

Node1 = バケット 1 および 2

Node2（削除）

Node3 = バケット 3

Node4 = バケット 4

設定例：最適化されたノード置換の設定

次に、実行コンフィギュレーションの例を示します。

```
configure terminal
 itd device-group webservers
  node ip 10.2.1.10
  node ip 10.2.1.20
  node ip 10.2.1.30
  itd http_service
  device-group webservers
  ingress interface Ethernet 3/1
  no shutdown
  exit
 itd session device-group webservers
  no node ip 10.2.1.30
  node ip 10.2.1.50
 commit
```

デバイス グループの設定

はじめる前に

ITD 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **itd device-group***name*	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。
ステップ 3	switch(config-device-group)# **node ip***ipv4-address*	ITD のノードを指定します。この手順を繰り返して、すべてのノードを指定します。 IPv6 ノードを設定するには、**node ipv6***ipv6-address* を使用します。 （注） ITD デバイス グループは、IPv4 または IPv6 ノードのいずれか一方で構成する必要があります。両方を混在させることはできません。
ステップ 4	switch(config_dg_node)# [**mode hot-standby**] [**standby***ipv4-address*] [**weight**	ITD のデバイス グループ ノードを指定します。この手順を繰り返して、すべてのノードを指定します。

	コマンドまたはアクション	目的
	value] [**probe** {**icmp**| **tcp** **port***port-number*| **udp** **port***port-number*| **dns** {*hostname*| *target-address*}} [**frequency***seconds*] [[**retry-down-count**| **retry-up-count**] *number*] [**timeout***seconds*]	**weight***value* キーワードは、重み付けトラフィック分散用にノードの適切な重みを指定します。 **mode hot-standby** は、このノードをデバイスグループのスタンバイ ノードにすることを指定します。 ノードレベルのスタンバイを各ノードに関連付けることができます。**standby** 値は、このアクティブ ノードのスタンバイ ノード情報を指定します。 ノードレベルのプローブを設定してノードの正常性を監視できます。**Probe** 値は、このアクティブ ノードの正常性を監視するために使用するプローブ パラメータを指定します。 （注） IPv6 プローブはサポートされません。
ステップ 5	switch(config-device-group)# **probe** {**icmp** | **tcp** **port***port-number* | **udp** **port***port-number* | **dns** {*hostname* |*target-address*} } [**frequency***seconds*] [[**retry-down-count** | **retry-up-count**] *number*] [**timeout***seconds*]	クラスタ グループのサービス プローブを設定します。 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 • DNS キーワードは次のとおりです。 • **retry-down-count**：ノードをダウン状態としてマークする条件となるプローブの連続失敗回数を指定します。 • **retry-up-count**：ノードをアップ状態としてマークする条件となるプローブの連続成功回数を指定します。 • **timeout**：プローブ応答を待機する秒数を指定します。 • **frequency**：ノードに連続して送信されるプローブの間隔を秒単位で指定します。 （注） IPv6 プローブはサポートされません。

ITD 設定の確認

ITD 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show itd [*itd-name*] [**brief**]	すべてまたは特定の ITD インスタンスのステータスおよび設定を表示します。 • 特定のインスタンスのステータスおよび設定を表示するには、*itd-name* 引数を使用します。 • ステータスおよび設定の要約情報を表示するには、**brief** キーワードを使用します。
show itd [*itd-name* | **all**] {**src** | **dst**} *ip-address*] **statistics** [**brief**]	ITD インスタンスの統計情報を表示します。 • 特定のインスタンスの統計情報を表示するには、*itd-name* 引数を使用します。 • 要約情報を表示するには、**brief** キーワードを使用します。 （注） **show itd statistics** コマンドを使用する前に、**itd statistics** コマンドを使用して ITD 統計情報をイネーブルにする必要があります。
show running-config services	設定された ITD デバイスグループおよびサービスを表示します。
show itd session device-group	設定されているすべてのセッションを一覧表示します。
show itd session device-group*device-group-name*	デバイスグループの名前と一致する ITD セッションを一覧表示します。

以下に、ITD 設定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

Exclude ACL
------------------------------
 exclude-smtp-traffic
```

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

Pool                          Interface    Status Track_id
----------------------------- ------------ ------ ---------
WEB_itd_pool                  Po-1       UP       3

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

  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  1     10.10.10.11       Active       1      OK          1         10001

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


  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  2     10.10.10.12       Active       1      OK          2         10002

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

switch# show itd brief

Name           Probe LB Scheme  Interface  Status   Buckets
-------------- ----- ---------- ---------- -------- --------
WEB            ICMP  src-ip     Eth3/3     ACTIVE   2

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


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

  Node  IP                Config-State Weight Status     Track_id  Sla_id
  ----------------------- ------------ ------ ---------- --------- ---------
  1     10.10.10.11       Active       1      OK          1         10001
  2     10.10.10.12       Active       1      OK          2         10002

switch(config)# show itd statistics

Service        Device Group             VIP/mask               #Packets
-------------------------------------------------------------------------------
test            dev              9.9.9.10 / 255.255.255.0       114611  (100.00%)

Traffic Bucket        Assigned to      Mode       Original Node   #Packets
-------------------------------------------------------------------------------
test_itd_vip_0_acl_0  10.10.10.9       Redirect    10.10.10.9      57106  (49.83%)

Traffic Bucket        Assigned to      Mode       Original Node   #Packets
-------------------------------------------------------------------------------
test_itd_vip_0_acl_1  12.12.12.9       Redirect    12.12.12.9      57505  (50.17%)

switch (config)# show running-config services

version 6.2(10)
feature itd

itd device-group WEB-SERVERS
probe icmp
node ip 10.10.10.11
```

```
node ip 10.10.10.12

itd WEB
device-group WEB-SERVERS
virtual ip 10.10.10.100 255.255.255.255
ingress interface po-1
no shut
```

許可 ACL の設定

はじめる前に

ITD 機能をイネーブルにします。

ITD サービスをイネーブルにします。

包含 ACL 機能を設定するには、loadbalance コマンドを設定する必要があります。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 IP アクセス リストを名前で定義します。
switch(config-if)# **ip access-list***access-list-name*

ステップ 3 名前付き IP アクセス リストの条件を設定し、ITD の対象トラフィックを選択する許可 ACE を設定します。
switch(config-acl)# **permit ip any***destination-addressaddress-mask*

ステップ 4 名前付き IP アクセス リストの条件を設定し、ITD の対象トラフィックを選択する許可 ACE を設定します。

- 注：この例では、宛先ネットワーク 209.165.202.0/27 へのトラフィックと送信元ネットワーク 192.168.10.0/24 から宛先へのトラフィックをそれぞれ選択する 2 つの ACE を示します。

switch(config-acl)# **permit ip any***source-addressaddress-maskdestination-addressaddress-mask*

ステップ 5 ACL コンフィギュレーション モードを終了します。
switch(config-acl)# **exit**

ステップ 6 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* 引数は、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。

- 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。

switch(config)# **device-group***device-group-name*

ステップ 7 ITD サービスに 1 つ以上の入力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。

switch(config-itd)# **ingress interface***interface*

ステップ 8 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。

- method キーワードは、送信元 IP アドレスまたは宛先 IP アドレス ベースの負荷/トラフィック分散を指定します。

switch(config-itd)# **load-balance***methodsrcip*

ステップ 9 指定した ACL を ITD サービスまたはインターフェイスに適用します。

- method キーワードは、送信元 IP アドレスまたは宛先 IP アドレス ベースの負荷/トラフィック分散を指定します。

switch(config-itd)# **access-list***acl-name*

許可 ACL の設定

次に、実行コンフィギュレーションの例を示します。

```
configure terminal
 ip access-list includeACL
  permit ip any 209.165.201.0 255.255.255.224
  permit ip any 192.168.10.0 255.255.255.0 209.165.201.0 255.255.255.224
  exit
   device-group dg1
    ingress interface Ethernet 3/1
    load-balance method src ip
    access-list includeACL2
```

許可 ACL の確認

ITD 設定を表示して許可 ACL 機能を確認するには、次のいずれかのタスクを実行します。

コマンド	目的
show itd [*itd-name*] [**brief**]	すべてまたは特定の ITD インスタンスのステータスおよび設定を表示します。 • 特定のインスタンスのステータスおよび設定を表示するには、*itd-name* 引数を使用します。 • ステータスおよび設定の要約情報を表示するには、**brief** キーワードを使用します。

コマンド	目的
show running-config services	設定された ITD デバイスグループおよびサービスを表示します。
show ip access-lists*name*	指定した IP ACL の設定を表示します。

以下に、ITD 設定を確認する例を示します。

```
switch# show itd

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

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

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


Device Group                                        Probe  Port
--------------------------------------------------- ------ ------
WEB-SERVERS                                                ICMP

Pool                           Interface    Status Track_id
------------------------------ ------------ ------ ---------
WEB_itd_pool                   Po-1       UP       4

ACL Name/SeqNo                   IP/Netmask/Prefix            Protocol  Port
-------------------------------- ---------------------------- ---- -------
acl2/10                          192.168.1.30/24                    TCP  0

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1     192.168.1.10    Active   1  ICMP                      OK   5   10005

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

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2     192.168.1.20     Active   1 ICMP                      OK   6   10006

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

ACL Name/SeqNo                   IP/Netmask/Prefix            Protocol  Port
-------------------------------- ---------------------------- ---- -------
acl2/20                          192.168.1.40/24                    TCP  0

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  1     192.168.1.10   Active   1 ICMP                       OK   5   10005

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

  Node  IP            Cfg-S   WGT Probe Port     Probe-IP   STS Trk# Sla_id
  ------------------- ------- --- ---- ----- --------------- -- --- -------
  2    192.168.1.20   Active   1 ICMP                      OK   6   10006
```

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

以下に、許可 ACL 機能を確認する例を示します。

```
switch (config)# show running-config services

!Command: show running-config services
!Time: Wed Feb 10 15:31:53 2016

version 7.3(1)D1(1)

feature itd


itd device-group WEB-SERVERS
  probe icmp
  node ip 192.168.1.10
  node ip 192.168.1.20


itd WEB
  device-group WEB-SERVERS
  ingress interface Po-1
  failaction node reassign
  load-balance method src ip
  access-list acl2
  no shut
```

以下に、ACL リストを確認する例を示します。

```
switch(config-itd)# show ip access-lists IncludeACL


10 permit ip any 209.165.201.0 255.255.255.224
20 permit ip 192.168.10.0 255.255.255.0 209.165.202.128 255.255.255.224
```

ITD サービス内の複数のデバイスグループの設定

複数のデバイス グループの作成

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`	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。

	コマンドまたはアクション	目的
ステップ 2	**feature itd***name* 例： `switch(config)# feature itd`	ITD 機能をイネーブルにします。
ステップ 3	**itd 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	**probe icmp** 例： `switch(config-device-group)# probe icmp`	Intelligent Traffic Director にクラスタ グループのサービス プローブを設定します。
ステップ 5	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.10`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 6	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.20`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 7	**exit** 例： `switch# exit`	ITD デバイス グループ コンフィギュレーション モードを終了して、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 8	**itd device-group***name* 例： `switch(config)# itd device-group dg_server1`	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 9	**probe icmp** 例： `switch(config-device-group)# probe icmp`	Intelligent Traffic Director にクラスタ グループのサービス プローブを設定します。
ステップ 10	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.30`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。

	コマンドまたはアクション	目的
ステップ 11	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.2.40`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 12	**exit** 例： `switch# exit`	ITD デバイス グループ コンフィギュレーション モードを終了して、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 13	**itd device-group***name* 例： `switch(config)# itd device-group dg_server2`	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 14	**probe icmp** 例： `switch(config-device-group)# probe icmp`	Intelligent Traffic Director にクラスタ グループのサービス プローブを設定します。
ステップ 15	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.50`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 16	**node ip***ipv4-address* 例： `switch(config-device-group)# node ip 192.168.1.60`	Intelligent Traffic Director の IPv4 クラスタ ノードを作成します。
ステップ 17	**exit** 例： `switch# exit`	ITD デバイス グループ コンフィギュレーション モードを終了して、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。

サービス内の複数のデバイス グループの関連付け

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`	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***service-name* 例： `switch (config) # itd multi-dg`	ITD サービスを設定し、ITD コンフィギュレーション モードを開始します。
ステップ 3	**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	**virtual ip***ipv4-address ipv4-network-mask***tcp***port-number***device-group***device-group-name* 例： `switch(config-itd)# virtual ip 172.16.1.10 255.255.255.255 tcp 23 device-group dg1_servers`	ITD サービスの仮想 IPv4 アドレスを設定します。
ステップ 5	**virtual ip***ipv4-address ipv4-network-mask***tcp***port-number***device-group***device-group-name* 例： `switch(config-itd)# virtual ip 172.16.1.20 255.255.255.255 tcp 23 device-group dg2_servers`	ITD サービスの仮想 IPv4 アドレスを設定します。
ステップ 6	**ingress interface interface***namenumber* 例： `switch(config-itd)# ingress interface ethernet  3/1`	1 つ以上の入力インターフェイスを ITD サービスに追加し、ネクスト ホップ IP アドレス（設定する入力インターフェイスに直接接続されたインターフェイスの IP アドレス）を設定します。

	コマンドまたはアクション	目的
ステップ 7	**no shutdown** 例： `switch(config-itd)# no shutdown`	ITD サービスをイネーブルにします。

ITD の設定例

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)# probe icmp
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
```

以下に、仮想 IPv4 アドレスを設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd test
switch(config-itd)# device-group dg
switch(config-itd)# ingress interface Po-1
switch(config-itd)# virtual ip  172.16.1.10 255.255.255.255 advertise enable tcp any
```

以下に、仮想 IPv6 アドレスを設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd test
switch(config-itd)# device-group dg
switch(config-itd)# ingress interface Po-1
switch(config-itd)# virtual ipv6 ffff:eeee::cccc:eeee dddd:efef::fefe:dddd tcp 10 advertise
 enable
```

次に、デバイス グループレベルのスタンバイ ノードを設定する例を示します。ノード 192.168.2.15 をデバイス グループ全体のスタンバイとして設定します。アクティブ ノードのいずれかに障害が発生すると、障害のあるノードに送信されるトラフィックは 192.168.2.15 にリダイレクトされます。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# probe icmp
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)# node ip 192.168.2.15
switch(config-dg-node)# mode hot standby
switch(config-dg-node)# exit
```

次に、ノードレベルのスタンバイ ノードを設定する例を示します。ノード 192.168.2.15 をノード 192.168.2.11 専用のスタンバイとして設定します。ノード 192.168.2.11 に障害が発生した場合にのみ、ノード 192.168.2.11 に送信されるトラフィックが 192.168.2.15 にリダイレクトされます。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# probe icmp
switch(config-device-group)# node ip 192.168.2.11
switch(config-dg-node)# standby ip 192.168.2.15
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-dg-node)# exit
```

次に、トラフィックを適切に分散するための重み付けを設定する例を示します。ノード 1 および 2 はノード 3 および 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 192.168.2.11
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 192.168.2.12
switch(config-dg-node)# weight 3
switch(config-device-group)# node ip 192.168.2.13
switch(config-device-group)# node ip 192.168.2.14
switch(config-dg-node)# exit
```

次に、ノードレベルのプローブを設定する例を示します。ノード 192.168.2.14 に TCP プローブを設定して、ICMP プローブをデバイスグループに設定します。TCP プローブはノード 192.168.2.14 に送信され、ICMP プローブはノード 192.168.2.11、192.168.2.12、および 192.168.2.13 に送信されます。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-device-group)# probe icmp
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-dg-node)# probe tcp port 80
switch(config-dg-node)# exit
```

次に、スタンバイ モード用のプローブを設定する例を示します。ノード 192.168.2.15 をノード 192.168.2.11 専用のスタンバイとして設定します。ICMP プローブはデバイスグループに設定しますが、TCP プローブはスタンバイ ノード 192.168.2.15 に設定します。ICMP プローブはノード 192.168.2.11、192.168.2.12、192.168.2.13、および 192.168.2.14 に送信されます。TCP プローブはノード 192.168.2.15 に送信されます。

```
switch(config)# feature itd
switch(config)# itd device-group dg
switch(config-dg-node)# probe icmp
switch(config-device-group)# node ip 192.168.2.11
switch(config-device-group)# standby ip 192.168.2.15
switch(config-dg-node-standby)# probe tcp port 80
switch(config-dg-node)# 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-dg-node)# exit
```

次に、IPv6 ノードに IPv4 プローブを設定する例を示します。dg-v6 は IPv6 のデバイス グループであり、IPv6 プローブはサポートされていません。ノード 210::10:10:14 がデュアルホーム接続されている場合（つまり IPv6 および IPv4 ネットワーク インターフェイスがどちらもサポートされ、IPv4 ノード アドレスは 210.10.10.1 です）、IPv4 プローブを設定してノードの正常性を監視できます。次に示す例では、IPv6 データ ノード 210::10:10:14: の正常性を監視するために、IPv4 アドレス 192.168.2.11 に TCP プローブが送信されるように設定します。

```
switch(config)# feature itd
switch(config)# itd device-group dg-v6
switch(config-device-group)#  node ipv6 210::10:10:11
switch(config-device-group)#  node ipv6 210::10:10:12
switch(config-device-group)# node ipv6 210::10:10:13
switch(config-device-group)# node ipv6 210::10:10:14
switch(config-dg-node)# probe tcp port 80 ip 192.168.2.11
switch(config-dg-node)# exit
```

次に、ITD サービスに除外 ACL を設定する例を示します。次の例では、ITD リダイレクションから SMTP トラフィックを除外する除外 ACL「exclude-SMTP-traffic」が設定されます。

```
switch(config)# feature itd
switch(config)# itd test
switch(config-device-group)# device-group dg
switch(config-itd)# ingress interface Po-1
switch(config-itd)# vrf RED
switch(config-itd)# exclude access-list exclude-SMTP-traffic
switch(config-idt)# no shut
```

次に、ITD サービスに VRF を設定する例を示します。

```
switch(config)# feature itd
switch(config)# itd test
switch(config-itd)# device-group dg
switch(config-itd)# ingress interface Po-1
switch(config-itd)# vrf RED
switch(config-idt)# no shut
```

次に、ITD サービスの統計情報収集をイネーブルにする例を示します。

（注） パケット カウンタを表示するには、「show itd statistics」に対して統計情報収集をイネーブルにする必要があります。

```
switch(config)# itd statistics test
```

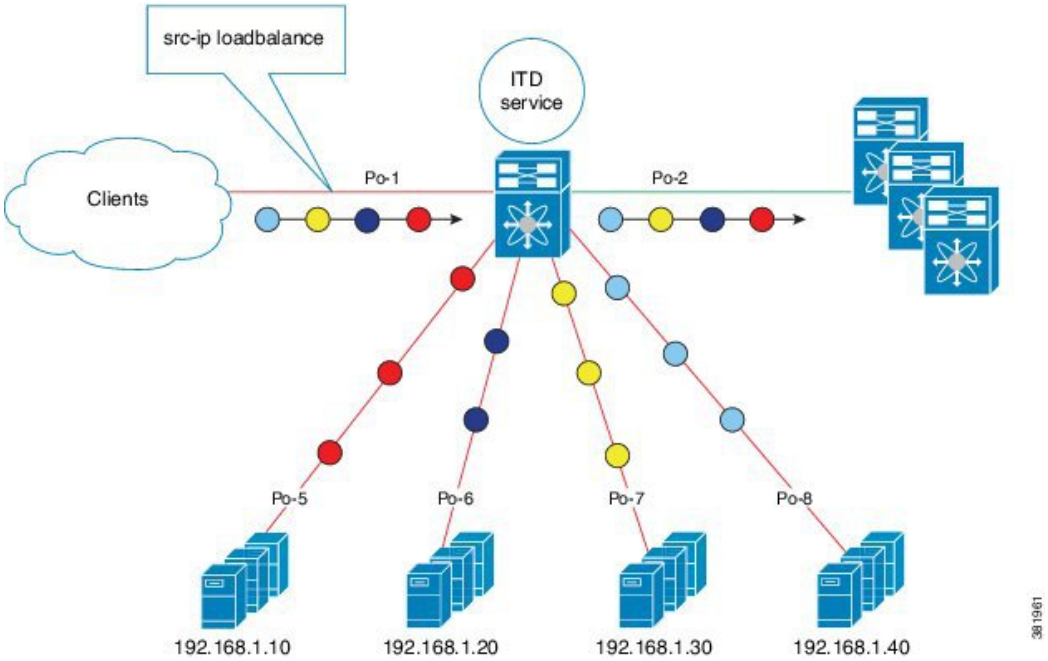
次に、ITD サービスの統計情報収集をディセーブルにする例を示します。

```
switch(config)# no itd statistics test
```

設定例：ワンアーム展開モード

以下の設定では、次の図に示すトポロジを使用します。

図 7：ワンアーム展開モード



手順 1：デバイス グループを定義する。

```
switch(config)# itd device-group DG
switch(config-device-group)# probe icmp
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
```

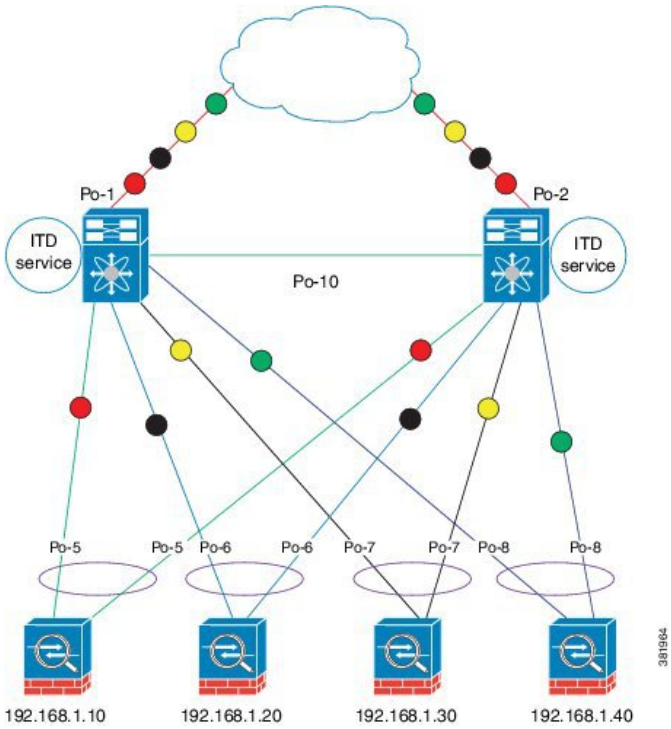
手順 2：ITD サービスを定義する。

```
switch(config)# itd Service1
switch(config-itd)# ingress interface port-channel 1
switch(config-itd)# device-group DG
switch(config-itd)# no shutdown
```

設定例：VPC でのワンアーム展開モード

以下の設定では、次の図に示すトポロジを使用します。

図 *8*：*VPC* でのワンアーム展開モード



デバイス 1

手順 1：デバイス グループを定義する。

```
N7k-1(config)# itd device-group DG
N7k-1s(config-device-group)# probe icmp
N7k-1(config-device-group)# node ip 192.168.2.11
N7k-1(config-device-group)# node ip 192.168.2.12
N7k-1(config-device-group)# node ip 192.168.2.13
N7k-1(config-device-group)# node ip 192.168.2.14
```

手順 2：ITD サービスを定義する。

```
N7k-1(config)# itd Service1
N7k-1(config-itd)# ingress interface port-channel 1
N7k-1(config-itd)# device-group DG
N7k-1(config-itd)# no shutdown
```

デバイス 2

手順 1：デバイス グループを定義する。

```
N7k-2(config)# itd device-group DG
```

```
N7k-2(config-device-group)# probe icmp
N7k-2(config-device-group)# node ip 192.168.2.11
N7k-2(config-device-group)# node ip 192.168.2.12
N7k-2(config-device-group)# node ip 192.168.2.13
N7k-2(config-device-group)# node ip 192.168.2.14
```

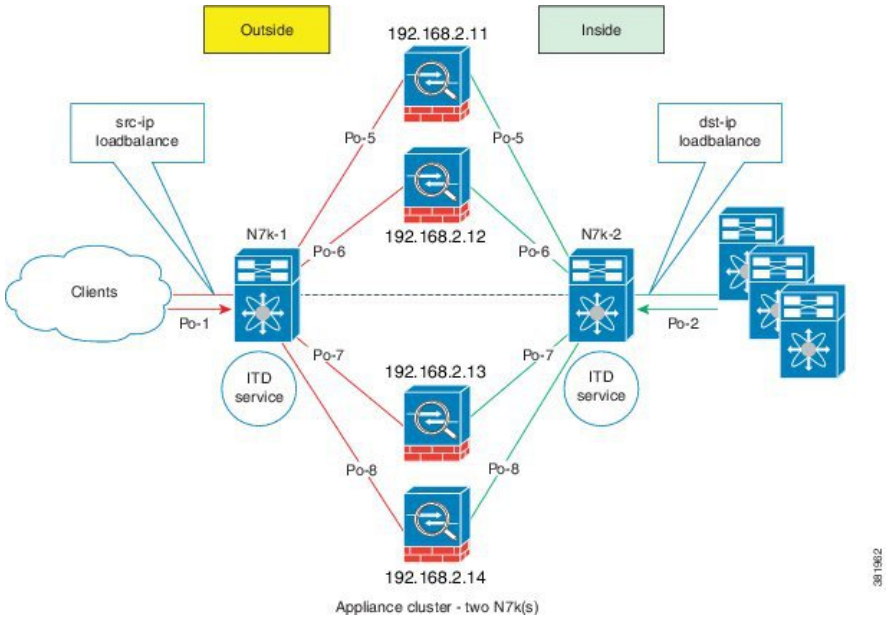
手順 2：ITD サービスを定義する。

```
N7k-2(config)# itd Service1
N7k-2(config-itd)# ingress interface port-channel 2
N7k-2(config-itd)# device-group DG
N7k-2(config-itd)# no shutdown
```

設定例：サンドイッチ展開モード

以下の設定では次の図に示すトポロジを使用します。

図 *9*：サンドイッチ展開モード



デバイス 1

手順 1：デバイス グループを定義する。

```
N7k-1(config)# itd device-group DG
N7k-1s(config-device-group)# probe icmp
N7k-1(config-device-group)# node ip 192.168.2.11
N7k-1(config-device-group)# node ip 192.168.2.12
N7k-1(config-device-group)# node ip 192.168.2.13
N7k-1(config-device-group)# node ip 192.168.2.11
```

手順 2：ITD サービスを定義する。

```
N7k-1(config)# itd HTTP
N7k-1(config-itd)# ingress interface port-channel 1
N7k-1(config-itd)# device-group DG
```

```
N7k-1(config-itd)# load-balance method src ip
N7k-1(config-itd)# no shutdown
```

デバイス 2

手順 1：デバイス グループを定義する。

```
N7k-2(config)# itd device-group DG
N7k-2(config-device-group)# probe icmp
N7k-2(config-device-group)# node ip 192.168.2.11
N7k-2(config-device-group)# node ip 192.168.2.12
N7k-2(config-device-group)# node ip 192.168.2.13
N7k-2(config-device-group)# node ip 192.168.2.14
```

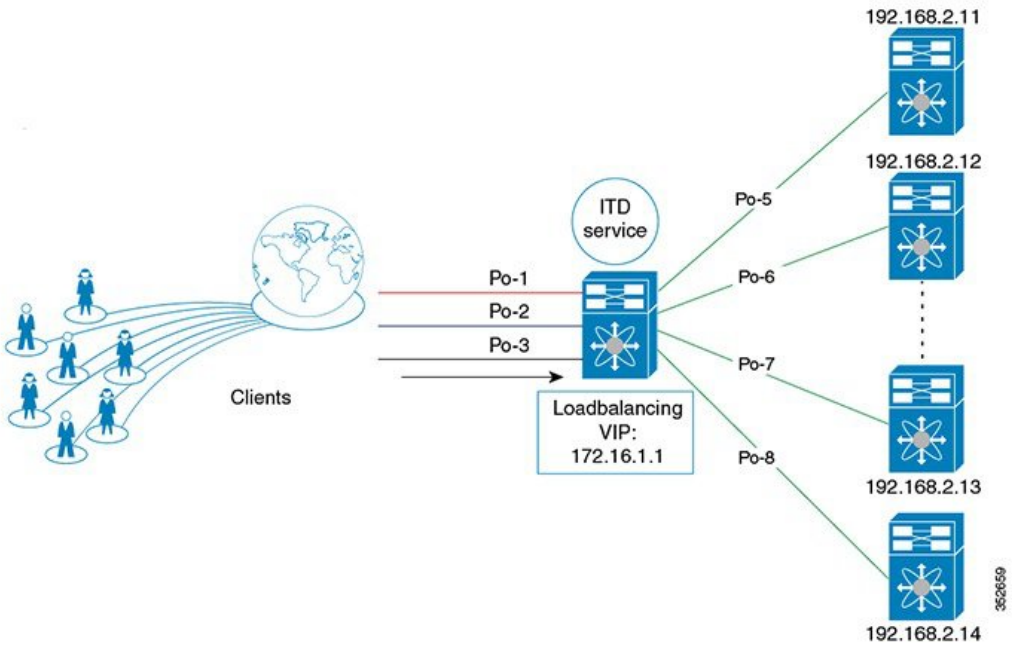
手順 2：ITD サービスを定義する。

```
N7k-2(config)# itd HTTP
N7k-2(config-itd)# ingress interface port-channel 2
N7k-2(config-itd)# device-group DG
N7k-2(config-itd)# load-balance method dst ip
N7k-2(config-itd)# no shutdown
```

設定例：サーバ ロードバランシング展開モード

以下の設定では、次の図に示すトポロジを使用します。

図 *10*：*VIP* を使用した *ITD* 負荷分散



手順 1：デバイス グループを定義する。

```
switch(config)# itd device-group DG
switch(config-device-group)# probe icmp
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
```

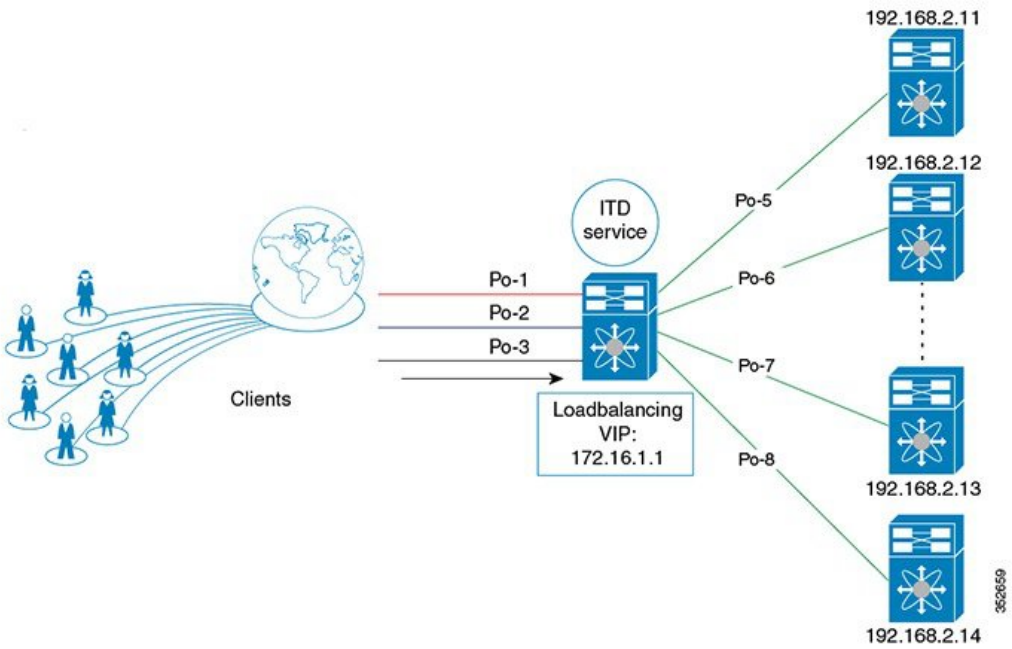
手順 2：ITD サービスを定義する。

```
switch(config)# itd Service2
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  172.16.1.20 255.255.255.255
switch(config-itd)# no shutdown
```

設定例：サーバ ロードバランシング展開モード

以下の設定では、次の図に示すトポロジを使用します。

図 *11*：*VIP* を使用した *ITD* 負荷分散



手順 1：デバイス グループを定義する。

```
switch(config)# itd device-group DG
switch(config-device-group)# probe icmp
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
```

手順 2：ITD サービスを定義する。

```
switch(config)# itd Service2
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  172.16.1.20 255.255.255.255
switch(config-itd)# no shutdown
```

ITD の関連資料

関連項目	マニュアル タイトル
Intelligent Traffic Director コマンド	『*Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director Command Reference*』

ITD の標準規格

この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。

ITD の機能履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
許可 ACL	7.3(0)D1(1)	この機能が導入されました。
最適化されたノード挿入/削除	7.3(0)D1(1)	この機能が導入されました。
宛先 NAT	7.2(1)D1(1)	この機能が導入されました。
ITD サービス内の複数のデバイスグループ	7.2(1)D1(1)	この機能が導入されました。
ITD	7.2(0)D1(1)	次の拡張機能が追加されました。 • ノードレベルのプローブ。 • IPv6 データ ノードに対する IPv4 制御プローブ。 • リダイレクションからトラフィックを除外する除外 ACL。

機能名	リリース	機能情報
ITD	6.2(10)	次の拡張機能が追加されました。 • 重み付けロードバランシング。 • ノードレベルのスタンバイ。 • レイヤ4ポートのロードバランシング。 • 同じデバイス上の 2 つの VDC 間でのサンドイッチ モード ノード状態同期。 • DNS プローブ。 • ITD 統計情報収集の開始/停止/クリア。 • ITD サービスとプローブに対する VRF サポート。
Intelligent Traffic Director（ITD）	6.2(8)	この機能が導入されました。

第 3 章

導入とベスト プラクティス

設計および導入の考慮事項

ここでは、ITD の設計および導入に関する考慮事項について説明します。

ITD サービスの数

ITD サービスの設定では、トラフィック フローの特定の方向の ITD トラフィック分散を定義します。フローの両方向でリダイレクトが必要な場合は、次のように 2 つの ITD サービスを設定する必要があります。フォワード トラフィック フローに 1 つ、リターン トラフィック フローに 1 つ。ASA には別々の内部および外部インターフェイス IP アドレスがあるため、2 つの異なるデバイス グループを設定して、対応する内部および外部 IP アドレスを指定する必要があります。

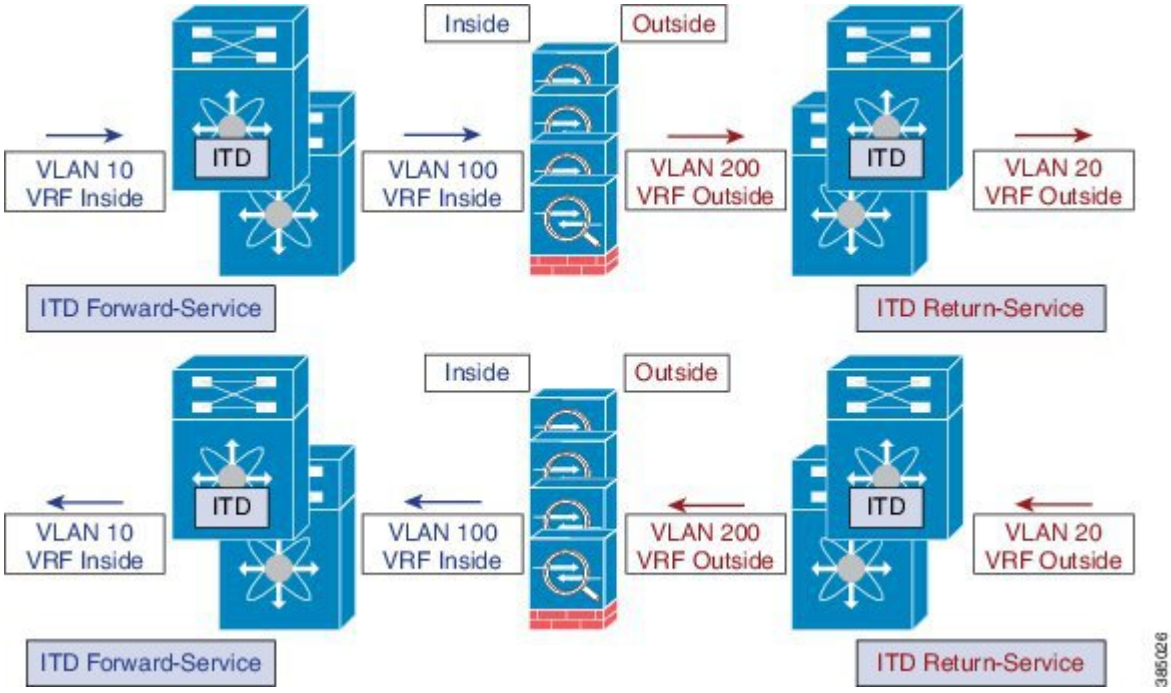
追加 ASA VLAN

ITD のフォワードおよびリターン サービスは Nexus スイッチ上の内部および外部 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 アプリケーションをイネーブルにすると、すべてのトラフィックを調査する必要があり、サービスでトラフィック フィルタリングは設定しません。その結果として、SVI にヒットするトラフィックは、いずれも対応する 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場合と同じ VLAN に設定されている場合、そのスイッチ上の別の VLAN に ITD サービスが存在するため、ファイアウォールからスイッチに戻るトラフィック

は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スイッチの間でトラフィックがループしないように個別のVLANのペアを使用する必要があります。

図 *12*： *ITD-ASA* 展開の論理ビュー



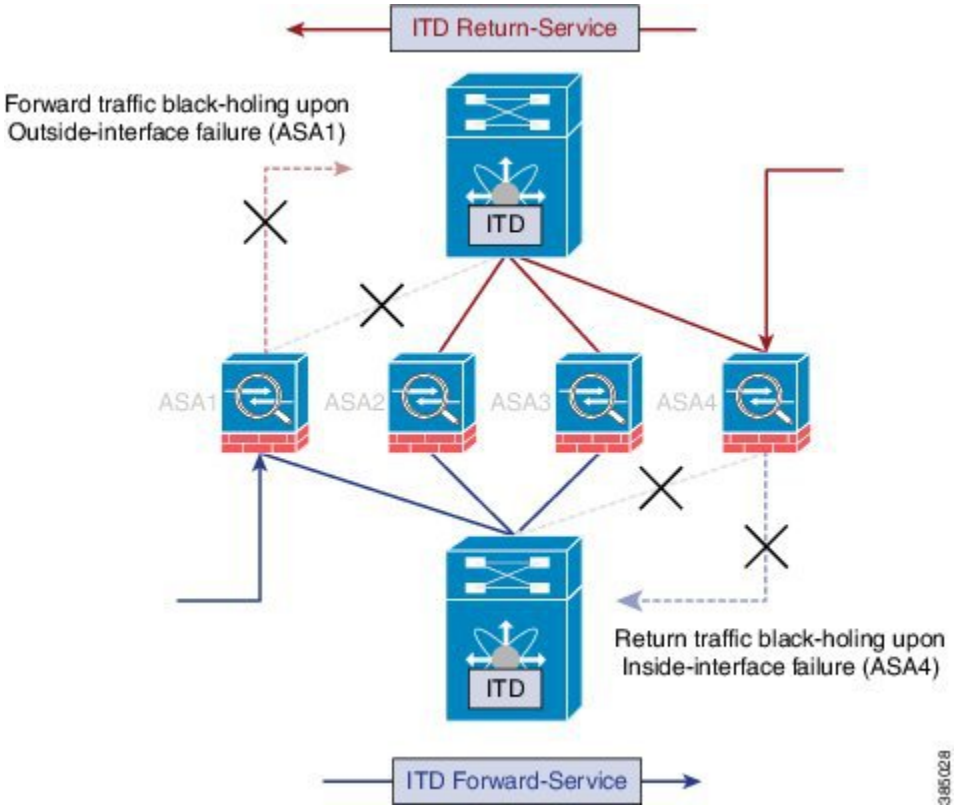
上記の例では、VLAN 10およびVLAN 20がネットワーク上の送信元と宛先への内部および外部インターフェイスの役目を担っており、VLAN 100およびVLAN 200はループフリー トラフィックを可能にするためにASAに対して使用されています。

リンク障害のシナリオ

ASAの内部または外部インターフェイスのいずれか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するため、そのASAの反対側に着信するトラフィックはブラックホール

化されます。ITD ピア VDC ノード状態同期機能は、VDC 間でノード状態を同期することで ITD から ASA のリモート側を削除するという方法によりこの問題を解決します。

図 *13*：ピア *VDC* 同期を使用しない場合の *ASA* 障害のシナリオ



ITD ピア VDC ノード状態同期機能は、デュアル VDC 非 vPC 単一スイッチ トポロジでのみ現在サポートされています。このような障害が発生した場合にクラスタリングではASA を完全にダウンさせるので、ASA クラスタリングでもこの問題は解決されます。Firewall on a Stick 実装（単一のリンクまたは vPC）では、ASA の内部および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、この問題は発生しません。

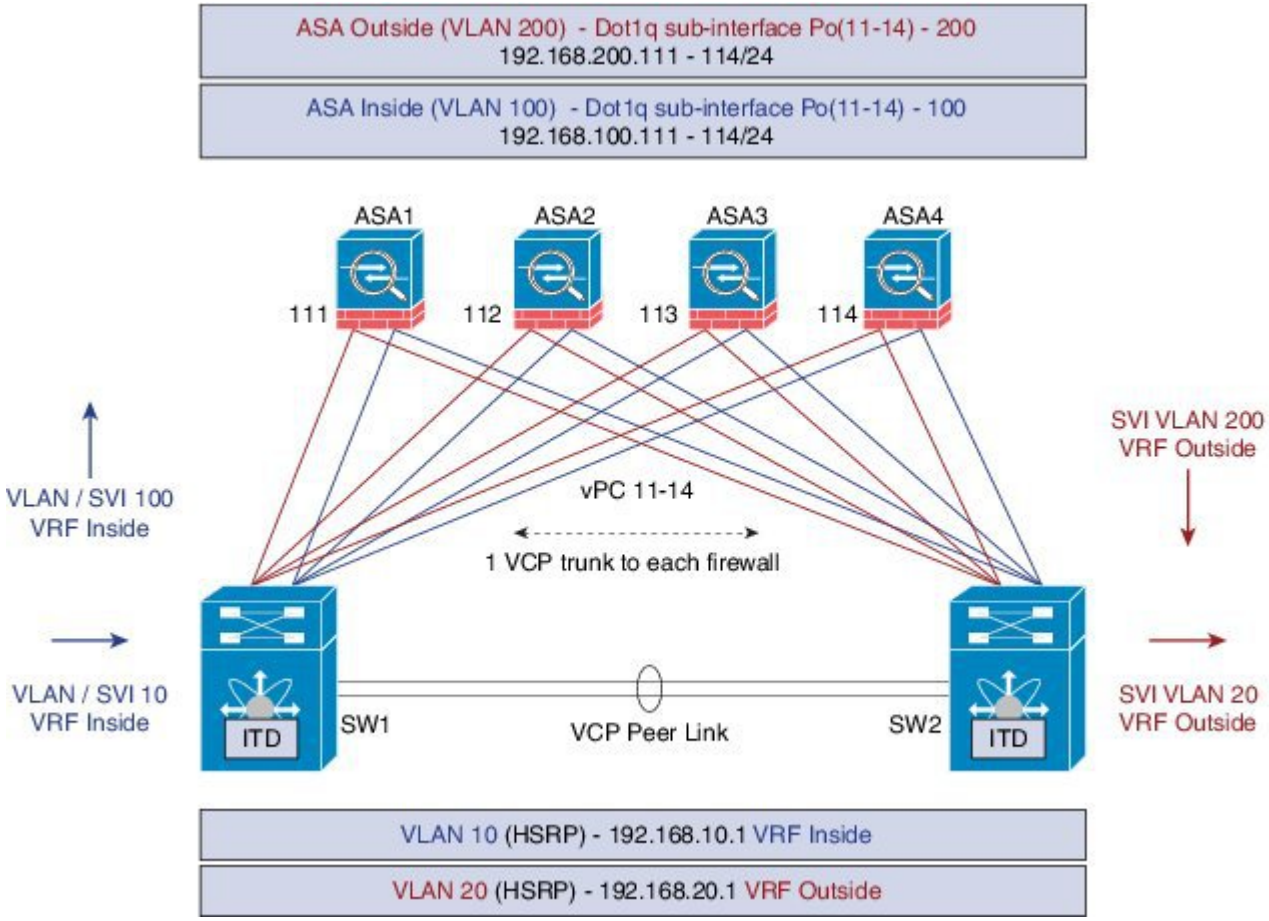
ITD ASA の展開

設定例：Firewall on a Stick

Firewall on a Stick 展開では、ASA とスイッチの接続に VPC ポートチャネル（または単一ポート）トランクが使用されます。次の図を参照してください。この設定では、内部および外部インターフェイスは dot1q サブインターフェイス（VLAN 100、200）です。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、インターフェイス間で物理ポートを分割しません。

図 *14*： *vPC* を使用した *Firewall on a Stick*



以下は Nexus 7000 の設定例の抜粋です。この例ではスイッチ（sw1）の設定の一部を示します。設定は、適切な方法ですべてのASAに対して同様に拡張する必要があります。他の機能はすでに設定されていると仮定します。

```
interface vlan 10
description Inside_Vlan_to_Network
vrf member INSIDE
ip address 192.168.10.10/24
hsrp 10
ip 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 192.168.20.1

interface vlan100
description Inside_Vlan_to_ASA
```

```
vrf member INSIDE
ip address 192.168.100.10/24
hsrp 100
ip 192.168.100.1

interface vlan200
description Outside_Vlan_to_ASA
vrf member OUTSIDE
ip address 192.168.200.10/24
hsrp 200
ip 192.168.200.1

.............................

interface Port-Channel111
 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-Channel41
 description Downstream_vPC_to_Network
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 vpc 41
 no shutdown

interface Port-Channel 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 192.168.100.111
   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 INSIDE
 vrf INSIDE
  #applies ITD service to VRF "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 a 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 Dst-IP
no shutdown

itd OUTSIDE
 vrf OUTSIDE
  #applies ITD service to VRF "OUTSIDE"
device-group FW_OUTSIDE
ingress interface Vlan 10
failaction node reassign
load-balance method dst ip buckets 16
#distributes traffic into 16 buckets
#load balances traffic based on Destination-IP.
#OUTSIDE service uses Dst-IP
no shutdown
```

以下は ASA の設定の抜粋です。次に示す ASA 側の設定は 1 つの ASA（ASA-1）の設定です。同様の設定を他のすべての ASA に拡張する必要があります。

```
interface Port-Channel11
 nameif aggregate
 security-level 100
 no ip address
!
interface Port-Channel11.100
 description INSIDE
 vlan 100
 nameif inside
 security-level 100
 ip address 192.168.100.111 255.255.255.0
!
interface Port-Channel11.200
 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 TenGigabitEthernet0/6
 description CONNECTED_TO_SWITCH_A_VPC
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/7
 description CONNECTED_TO_SWITCH_B_VPC
 channel-group 11 mode active
 no nameif
 no security-level
!
```

上記の設定とトポロジでは次の点に注意してください。

- VLAN 10、20、100、200、およびそれぞれの SVI の適切な VRF へのマッピング。
- ASA（内部および外部）に対する ITD デバイスグループの設定。
- フローの対称性を実現する ITD ロードバランシング設定。
- vPC のシナリオでは、vPC メンバーのいずれかが動作している限り、ITD は変更されません。vPC レッグに障害が発生したスイッチ上の ITD リダイレクションは、一般的な vPC の場合と同様にピアリンク経由でピアスイッチを通過します。

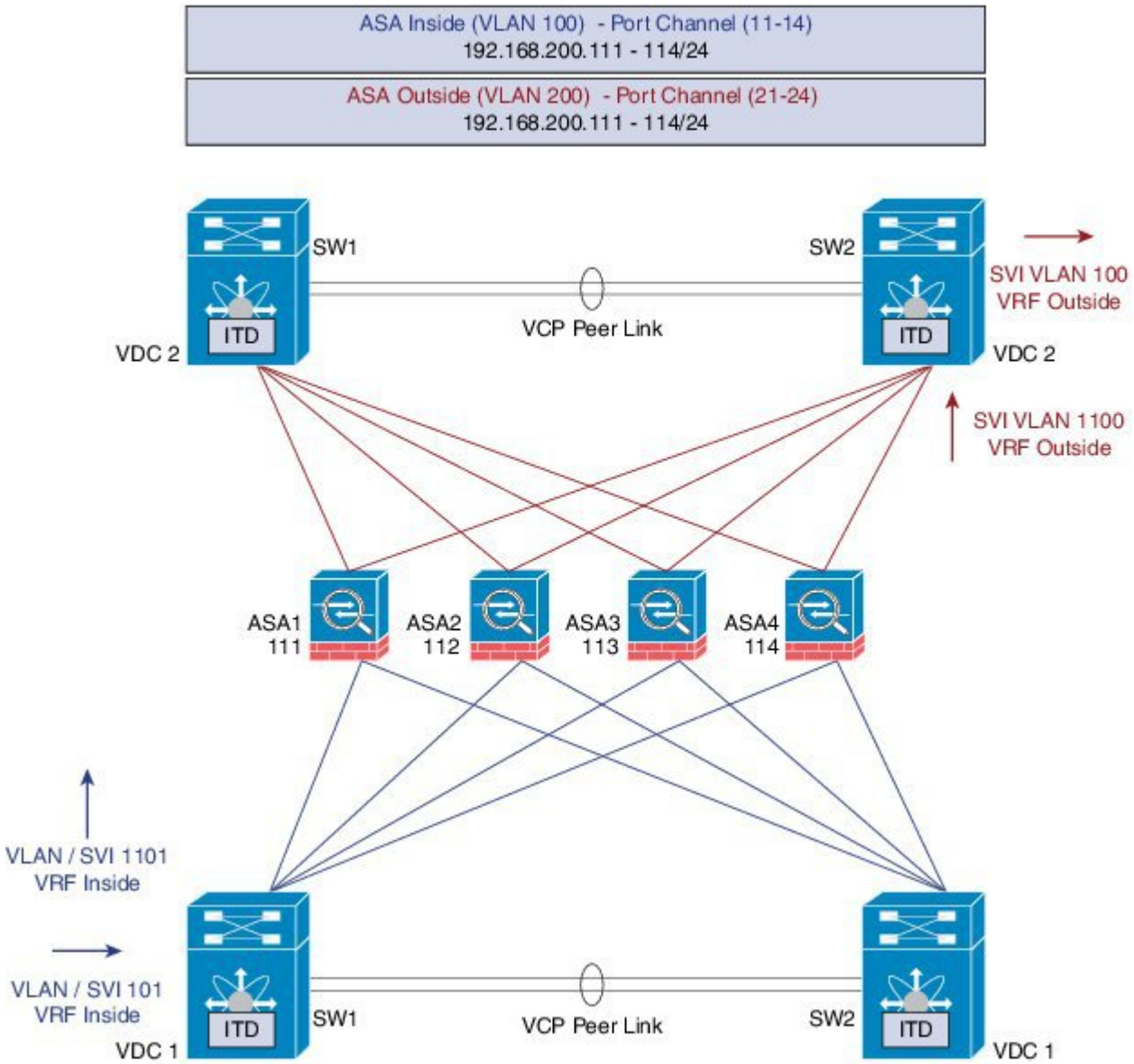
- このトポロジおよび展開方式では、内部および外部インターフェイスが ASA 上の同じ物理または仮想インターフェイス（dot1q サブインターフェイス）に関連付けられているため、物理リンク障害が発生してもトラフィックはブラックホール化されません。
- vPC を介したルーティング プロトコル ネイバーシップをサポートするには（Cisco NX-OS 7.2(0)D1(1) 以降のリリース）、vPC ドメイン内で **layer3 peer-router** コマンドを設定する必要があります。
- 内部と外部の両方のファイアウォール インターフェイスへの接続にレイヤ 3 インターフェイスが使用されるため、VRF が必要です。特定の状況でトラフィックがファイアウォールを迂回してルーティング（VLAN 間）しないように、VRF を設定します。
- トラフィックは PBR を介して ASA に転送されるので、ルートは必要ありません。

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

vPC を使用するサンドイッチ モードでは、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。次の図にこのトポロジを示します。なお、Nexus 7000 は現時点でノード状態同期機能をサポートしていません。vPC を使用することで、1 つのリ

ンクに障害が発生してもトラフィックフローは妨げられません。vPC を使用した他のシナリオと同様に、ITD はピアスイッチのリンクを介して ASA への転送を続行します。

図 *15*：*vPC* を使用したデュアル *VDC 2* スイッチ サンドイッチ モードのファイアウォール



Nexus 7000 での設定手順

単一スイッチ トポロジとこのトポロジの主な違いは、Nexus スイッチと ASA の間に単一リンクではなく vPC ポートチャネルが存在する点です。さらに、前述の例と同じく、スイッチの内部および外部インターフェイスは別の VDC に設定されます。

以下は VDC1 の設定です。

```
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-Channel11
 description To_ASA-1-INSIDE
 switchport mode access
 switchport access vlan 100
 vpc 11

interface Ethernet4/1
 description To_ASA-1-INSIDE
 switchport mode access
 switchport access vlan 100
 channel-group 11 mode active
```

以下は VDC2 の設定です。

```
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-Channel21
 description To_ASA-1-OUTSIDE
 switchport mode access
 switchport access vlan 200
 vpc 11

interface Ethernet4/25
 description To_ASA-1-OUTSIDE
 switchport mode access
 switchport access vlan 200
 channel-group 21 mode active
```

ASA での設定手順

以下は ASA の設定の抜粋です。

```
interface Port-Channel11
 description INSIDE
 vlan 100
 nameif inside
 security-level 100
 ip address 192.168.100.111 255.255.255.0

interface Port-Channel21
 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 TenGigabitEthernet0/6
 description CONNECTED_TO_SWITCH0-A-VPC
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/7
 description CONNECTED_TO_SWITCH-B-VPC
```

```
 channel-group 11 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/8
 description CONNECTED_TO_SWITCH-A-VPC
 channel-group 21 mode active
 no nameif
 no security-level

interface TenGigabitEthernet0/9
 description CONNECTED_TO_SWITCH-B-VPC
 channel-group 21 mode active
 no nameif
 no security-level
```

上記の設定とトポロジでは次の点に注意してください。

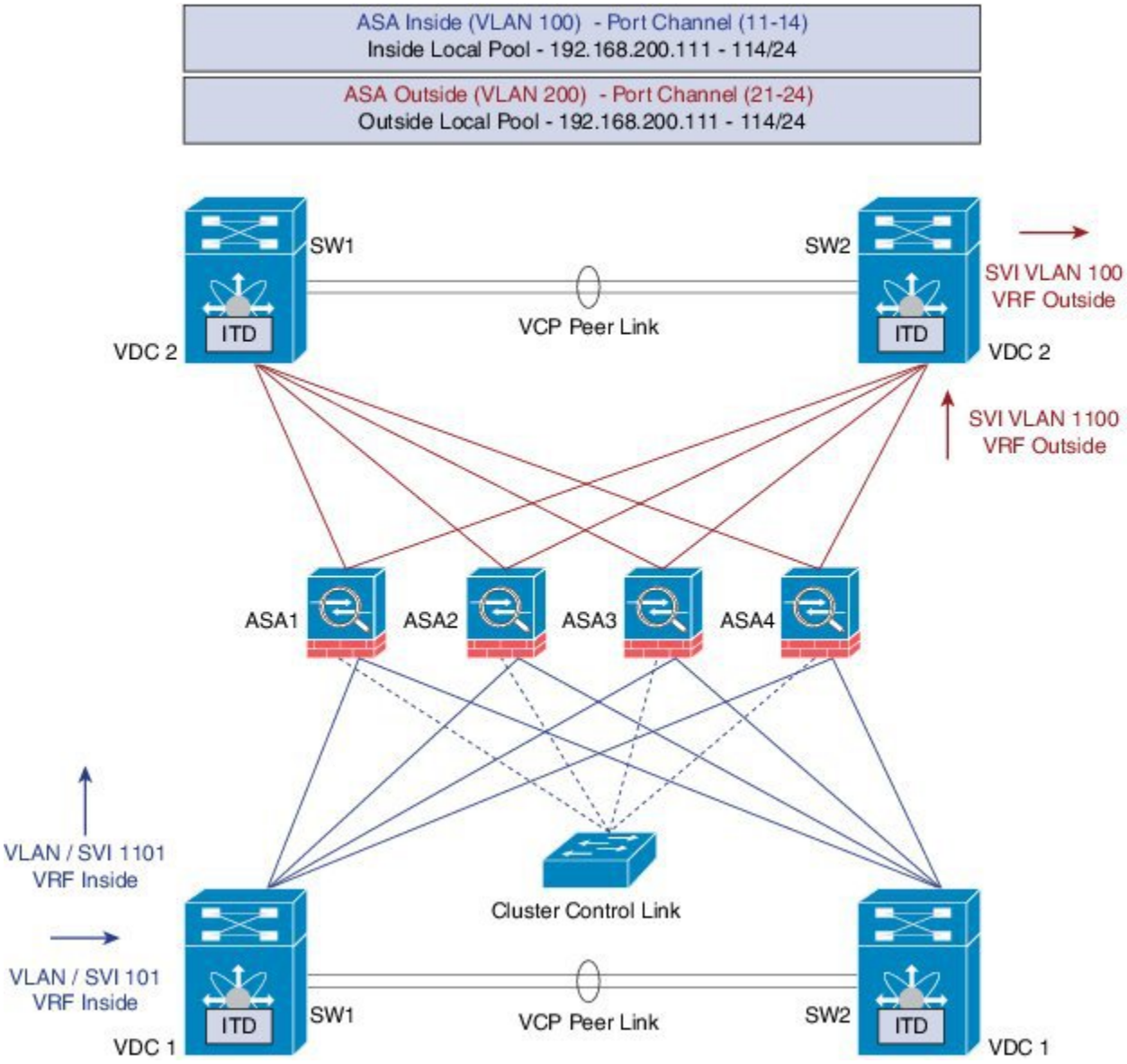
- フローの対称性を実現する ITD ロードバランシング設定。
- vPC のシナリオでは、vPC メンバーのいずれかが動作している限り、ITD は変更されません。vPC レッグに障害が発生したスイッチ上の ITD リダイレクションは、一般的な vPC の場合と同様にピアリンク経由でピアスイッチを通過します。
- このトポロジまたは展開方式では、ASA 上のいずれかのポート チャネルまたは非 VPC での単一の物理リンクに障害が発生すると、トラフィックのブラックホール化が発生する可能性があります。
- Cisco NX-OS 7.2(0)D1(1) 以降のリリースで、vPC を介したルーティング プロトコル ネイバーシップをサポートするには、vPC ドメイン内で **layer3 peer-router** コマンドを設定する必要があります。
- トラフィックは PBR を介して ASA に転送されるため、ルートは必要ありません。

設定例：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 を単一の論理デバイスとしてグループ化すると、管理およびネットワークへの統合という点で単一

のデバイスの利便性を得られる上に、複数デバイスによる高いスループットおよび冗長性が実現します。次の図を参照してください。

図 *16*： ***vPC*** を使用したデュアル ***VDC*** サンドイッチによる ***ASA*** クラスタ



ACL クラスタリング

次の表は、ASA デバイスのステータスが変化したときに、ECMP で発生した CCL に対する影響と ITD で発生した影響の比較結果です。

ASA ステータス	ITD	ECMP
安定状態	CCL 上の最小トラフィック。想定されているトラフィック タイプ。 ライン カードとスイッチのタイプに関係なく、全く同じ負荷分散。	すべての場所で同じライン カード タイプとスイッチ モデルが使用されている場合の CCL 上の最小トラフィック。異なるハードウェアが使用されている場合は、非対称のレベルが高くなって CCL ネットワーク上に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ハッシュ関数が異なります。2 台のスイッチ（vPC 環境内など）が同じフローを別々の ASA デバイスに送信すると、CCL トラフィックが発生します。
単一 ASA 障害	CCL 上で追加のトラフィックは発生しません。ITD は IP スティッキ性とレジリエント ハッシングを提供します。	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 上で発生します。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。
単一 ASA リカバリ	クラスタ内の 2 台の ASA（バケットを受信するリカバリされた ASA とそのバケットが優先的に提供される ASA）間の CCL 上でトラフィック リダイレクションが発生する可能性があります。	追加のトラフィック リダイレクションが CCL 上で発生する可能性があります。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。
ASA の追加	CCL 上の最小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 上で発生します。これにより、クラスタ内のすべての ASA へのある程度のトラフィックが発生することになります。

ITD は個々のモード レイヤ 3（L3）ASA クラスタを対象にロード バランスを実行できます。ITD は各ファイアウォールによって処理されるフローの予測を実現するので、クラスタリングを補完

します。OSPF ECMP およびポートチャネル ハッシュ アルゴリズムを利用する代わりに、ITD バケットによってフローを特定します。

L3 クラスタを使用すると、バケットの割り当てに基づいてフロー オーナーを事前に特定できます。通常、ITD および L3 クラスタリングを利用せずに最初のオーナー選択を予測することは不可能ですが、ITD を使用すれば事前に特定できます。

ASA クラスタリングでもバックアップ フロー オーナーの実装が使用されます。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対して、別のファイアウォールはそのフローの状態とオーナー ASA を保存します。実際のアクティブなフロー オーナーに障害が発生すると、ITD の Failaction 再割り当てによって、障害のあるオーナー ASA からのバケットに含まれるすべてのフローはデバイス グループにリストされている次のアクティブ ノードに転送されます。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フローの適切なバックアップ オーナーではない場合、このファイアウォールはバックアップ オーナーからフロー状態の情報を受け取って、トラフィックをシームレスに処理する必要があります。詳細については、『Cisco ASA Series CLI Configuration Guide, 9.0』を参照してください。

ITD で ASA クラスタリングを使用する際の潜在的な欠点は、バックアップ フローおよび他のクラスタ テーブルの動作により、非クラスタ化ファイアウォールでは消費しないメモリと CPU リソースが消費されることです。したがって、非クラスタ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可能性があります。ただし、ASA クラスタ メンバーに障害が発生しても既存の接続がタイムアウトしないという確証は、お客様にとって非常に価値があると考えられます。

Nexus 7000 での設定手順

クラスタリングを導入しても ITD 設定は変わりません。ITD Nexus 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、vPC トポロジを使用したデュアル VDC サンドイッチでのファイアウォールと同じ設定です。

ITD 設定は、ノード状態同期が削除されたことを除いて以前の方法とほとんど同じです。

ASA での設定手順

ASA クラスタリングは、PBR 展開シナリオと同様に、次のマニュアルで説明されている L3 クラスタとして設定されます。ASA クラスタの設定に関する詳細情報は、次のリンクで確認できます。次に、レイヤ 3 クラスタリング トポロジのファイアウォールに対する ASA での設定例を示します。詳細については、『Cisco ASA Series CLI Configuration Guide, 9.0』を参照してください。

```
cluster group ASA-CLUSTER-L3
local-unit ASA1
cluster-interface port-channel1 ip 192.168.250.100 255.255.255.0
priority 1
health-check holdtime 1.5
clacp system-mac auto system-priority 1
enable

mac-address pool MAC-INSIDE aaaa.0101.0001 - aaa.0101.0008
mac-address pool MAC-OUTSIDE aaaa.0100.0001 - aaa.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-Channel11
 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-Channel21
 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-Channel31
 description Clustering Interface
 lacp max-bundle 8


interface TenGigabitEthernet0/6
 channel-group 11 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/7
 channel-group 11 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/8
 channel-group 21 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet0/9
channel-group 21 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet1/0
channel-group 31 mode active
 no nameif
 no security-level
 no ip address

interface TenGigabitEthernet1/1
channel-group 31 mode active
 no nameif
 no security-level
 no ip address
```

上記の設定に示すように、ポートチャネル 11 と 21 は前述の例の内部または外部インターフェイスに使用されます。ただし、クラスタリング インターフェイス用のポートチャネル 31 が追加されています。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、常に現在のマスター ユニットに属します。同様に MAC アドレス プールも設定され、対応する内部または外部ポートチャネルで使用されます。

設定例：WCCP タイプの ITD シナリオ

Web プロキシを使用した設計

ITD を使用した Web プロキシ導入では、Nexus スイッチがインターネット宛ての Web トラフィックの照合とプロキシ サーバに対するそのロード バランシングを担当します。

プロキシ サーバは、Autonomous モードで動作（WCCP から独立してアクティブ-アクティブとして動作）し、リダイレクトされてきたトラフィックを処理します。ITD が実行するノードの正常性のプローブには、ノードの状態を追跡し、その可用性に基づいて適切にノードを削除または追加する目的があります。冗長性を確保するために、スタンバイ サーバをグループ レベルまたはノード レベルで設定することもできます。

サービスの数

パケット フローのスライドに示すように、通常は、ITD リダイレクションが VLAN に対向するクライアントの順方向にのみ必要です。以降は、ITD リダイレクションまたは分散を使用せずにパケットがルーティングまたは転送されます。このような Web プロキシ導入を伴う ITD は、1 つの ITD サービスのみが必要で、これが順方向に設定されます。ただし、逆トラフィック リダイレクションの要件がある場合は、トラフィック選択を送信元 L4 ポートに基づく必要があります。LB パラメータの反転によってフローの対称性も維持する必要があります。

プロキシ ヘルス モニタリングのプローブ

Web プロキシ導入に ITD を使用する場合は、Web プロキシ サーバの可用性を確認するために、ITD プローブが使用されます。このことは、障害が発生したプロキシ サーバに送信されたトラフィックがブラックホール化する可能性があるため重要です。プラットフォームごとの最新リリースで現在使用可能なプローブは次のとおりです。

- Nexus 7000（7.2(1)D1(1)）：ICMP、TCP/UDP、DNS
- Nexus 5000：ICMP
- Nexus 9000：ICMP

ロードマップ：プラットフォーム全体のプローブ パリティが今後リリースされる予定です。追加の HTTP プローブについては調査中です。

（注） これらは確定されていませんが、ロードマップ項目になっています。

トラフィック選択要件

ITD のトラフィック フィルタリングまたはトラフィック選択に対して現在サポートされている方式を以下に示します。

- **仮想 IP（Nexus 5000、Nexus 6000、Nexus 7000、および Nexus 9000 でサポートされる）**：

  宛先フィールド専用のトラフィック選択（フィルタリング）に使用される IP+サブネット マスクの組み合わせ。

- **除外 ACL**：

  ITD をバイパスするトラフィックを指定するために使用される ACL。

  この ACL で許可されなかったトラフィックが ITD を通過します。

  除外 ACL は、送信元と宛先の両方のフィールドに基づいてフィルタリングできます。除外 ACL は VIP より優先されます。

除外 ACL は許可 ACE エントリのみをサポートします。拒否 ACE は除外 ACL 上でサポートされません。

- **ポート数ベースのフィルタリング**

  "Port 80 needs ITD service" のように L4 ポートに基づいてトラフィックを選択する場合は、以下を使用して実行できるようになりました。

  - 一致する宛先ポート：VIP – 0.0.0.0 0.0.0.0 tcp 80（任意の送信元または宛先 IP、一致する宛先ポート 80）
  - 一致する送信元ポート："permit tcp any neq 80 any"（80 以外の任意のポートが ITD をバイパスし、ポート 80 はリダイレクトされる）を含む除外 ACL。
  - 一致する複数のポート番号：ITD 内の複数の VIP 回線をポートごとに 1 つずつ設定できます。

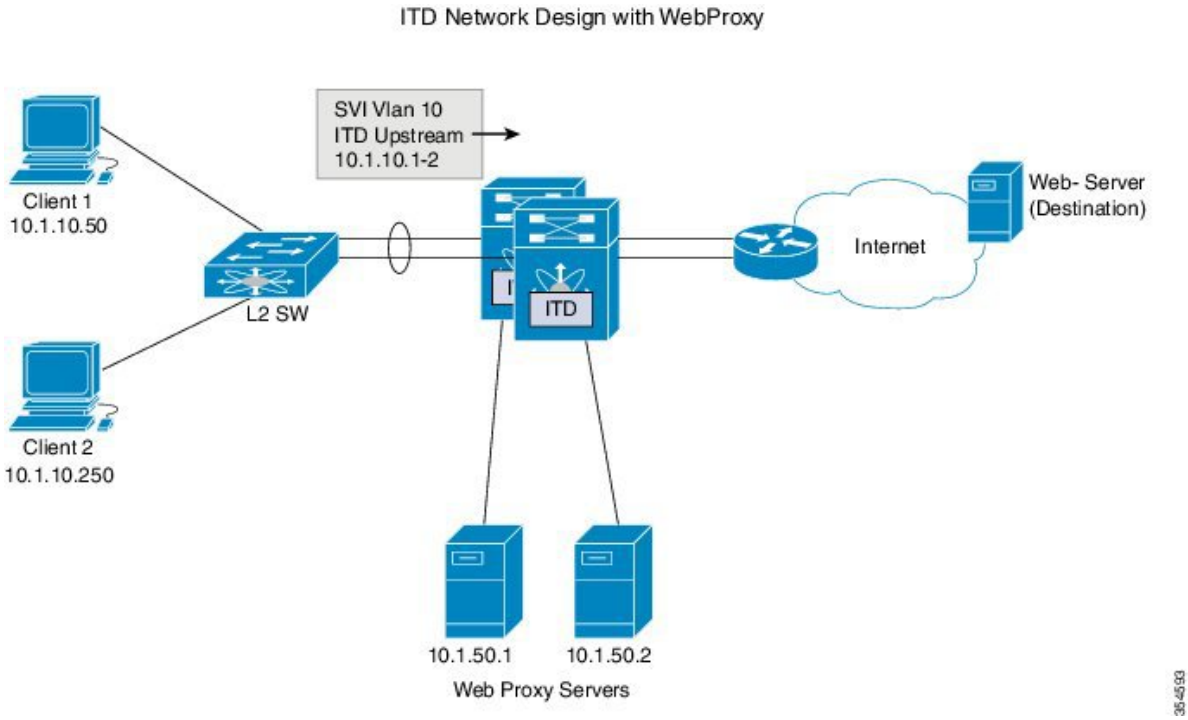
- **包含 ACL**：ロードマップ項目 - Cisco Nexus 7000 リリース 7.3(0)D1(1)、Cisco Nexus 9000 リリース 7.0(3)I3(1)

  "Port 80 needs ITD service" のように L4 ポートに基づいてトラフィックを選択する場合は、以下を使用して実行できるようになりました。

  - ITD が提供する必要のあるトラフィックを許可するために使用される包含 ACL。両方の SRCand DST フィールドを照合することができます。
  - Permit 行だけが許可されます 。一度に使用できるのは VIP と包含 ACL のどちらかで、両方を使用することはできません。
  - ロードバランシング パラメータによって、包含 ACL 内で使用可能な一致の最大長が決定されます。たとえば、発信元ベースの LB と 8 つのバケットを使用した場合に、照合可能な送信元 IP アドレスの最大マスクは /29 です。宛先 LB と 8 つのバケットを使用した場合に、照合可能な宛先 IP の最大マスクは /29 です。

（注） この包含 ACL 機能は、ロードマップ項目で、現在のリリースでは使用できません。ここで提供される情報は、一時的なもので、変更される可能性があります。

図 *17*： ***WebProxy*** を使用した ***ITD*** ネットワーク設計



上の図に示すように、インターネットへの宛先ポート 80/443（ingressVLAN10）は、Web プロキシ サーバ 10.1.50.1/10.1.50.2 に分配されます。

プライベート ネットワーク（10.0.0.0/8、192.168.0.0/16、および 172.16.0.0/20）宛ての VLAN 10 上のトラフィックはプロキシ サーバに送信されません。

```
 itd device-group Web_Proxy_Servers              <<<< Configure ITD Device-group
Web_Proxy_Servers and point to server IP addresses.
  probe icmp
  node ip 10.1.50.1
  node ip 10.1.50.2

ip access-list itd_exclude_ACL                  <<<< Configure Exclude ACL to exclude all
 traffic destined to Private IP addresses.
  10 permit ip any 10.0.0.0 255.0.0.0
  20 permit ip any 192.168.0.0 255.255.0.0
  30 permit ip any 172.16.0.0 255.255.240.0

Itd Web_proxy_SERVICE
  device-group Web_Proxy_Servers                <<<< Apply Exclude ACL.
  exclude access-list itd_exclude_ACL
  virtual ip 0.0.0.0 0.0.0.0 tcp 80             <<<< Any Traffic TO DESTINATION Port-80
redirect to group  Web_Proxy_Servers
```

```
  virtual ip 0.0.0.0 0.0.0.0 tcp 443             <<<< Any Traffic TO DESTINATION Port-443
redirect to group Web_Proxy_Servers
  ingress interface Vlan 10
  failaction node reassign
  load-balance method src ip
  no shutdown
```

リターン トラフィックのリダイレクションが必要な場合は、次の追加の設定が必要になります。

（注） レイヤ 4 の range 演算子を使用することで可能なのはポート フィルタリングのみです。除外 ACL は permit エントリのみをサポートします。

```
ip access-list itd_exclude_return            <<<< Configure Exclude ACL (Return) to exclude
 all but port 80 & 443
  10 permit tcp any range 0 79 any
  20 permit tcp any range 81 442 any
  10 permit tcp any range 444 65535 any

itd Web_proxy_SERVICE                          <<<< Configure Return ITD service for return
 traffic:
  device-group Web_Proxy_Servers
  exclude access-list itd_exclude_return      <<<< Apply Exclude ACL for Return ITD service.
  ingress interface Vlan 20                     <<<<  Internet-facing ingress interface on
the Nexus Switch.
  failaction node reassign
  load-balance method dst ip                    <<<<  Flow symmetry between forward/retrun
flow achieved by flipping LB parameter.
  no shutdown
```

上記の設定に示すように、ポートチャネル 11 と 21 は前述の例の内部または外部インターフェイスに使用されます。ただし、クラスタリング インターフェイス用のポートチャネル 31 が追加されています。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、常に現在のマスター ユニットに属します。同様に MAC アドレス プールも設定され、対応する内部または外部ポートチャネルで使用されます。