

Nexus 7000 インテリジェント トラフィック デイレクタの設定例

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ITD とのトラフィック フロー](#)

[設定](#)

[ステップ 1: ITD デバイス グループの設定](#)

[プローブの設定](#)

[ノード レベルのスタンバイ](#)

[ステップ 2: ITD サービスの設定](#)

[ITD サービスの設定](#)

[デバイス グループの定義](#)

[入カインターフェイスの設定](#)

[ITD の仮想 IP アドレスの設定](#)

[ITD のロード バランス メソッドの定義](#)

[ステップ 3: フェールオーバー動作の定義](#)

[ステップ 4: ノード サーバでのループバック インターフェイスとしての ITD VIP の設定](#)

[その他の設定オプション](#)

[ノードへのウェイトの割り当て](#)

[失敗アクションの設定](#)

[確認](#)

[ITD サービスの確認](#)

[動的に作成されたアクセス リストとルート マップの確認](#)

[入カインターフェイス設定の確認](#)

[プローブ設定の確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Nexus 7000 で Intelligent Traffic Director (ITD) をトラブルシューティングして確認する基本的な手順について説明します。このドキュメントでは、ITD に関連する概念を説明するために、サーバのロードバランシングの導入を使用します。

ITD に関する詳細については、以下の参考資料を参照してください。

- [Cisco Intelligent Traffic Director の概要](#)
- [Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director コマンド リファレンス](#)

前提条件

要件

ITD について十分に理解しておくことをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Nexus 7000 シリーズ スイッチ
- Cisco NX-OS バージョン 6.2(10)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

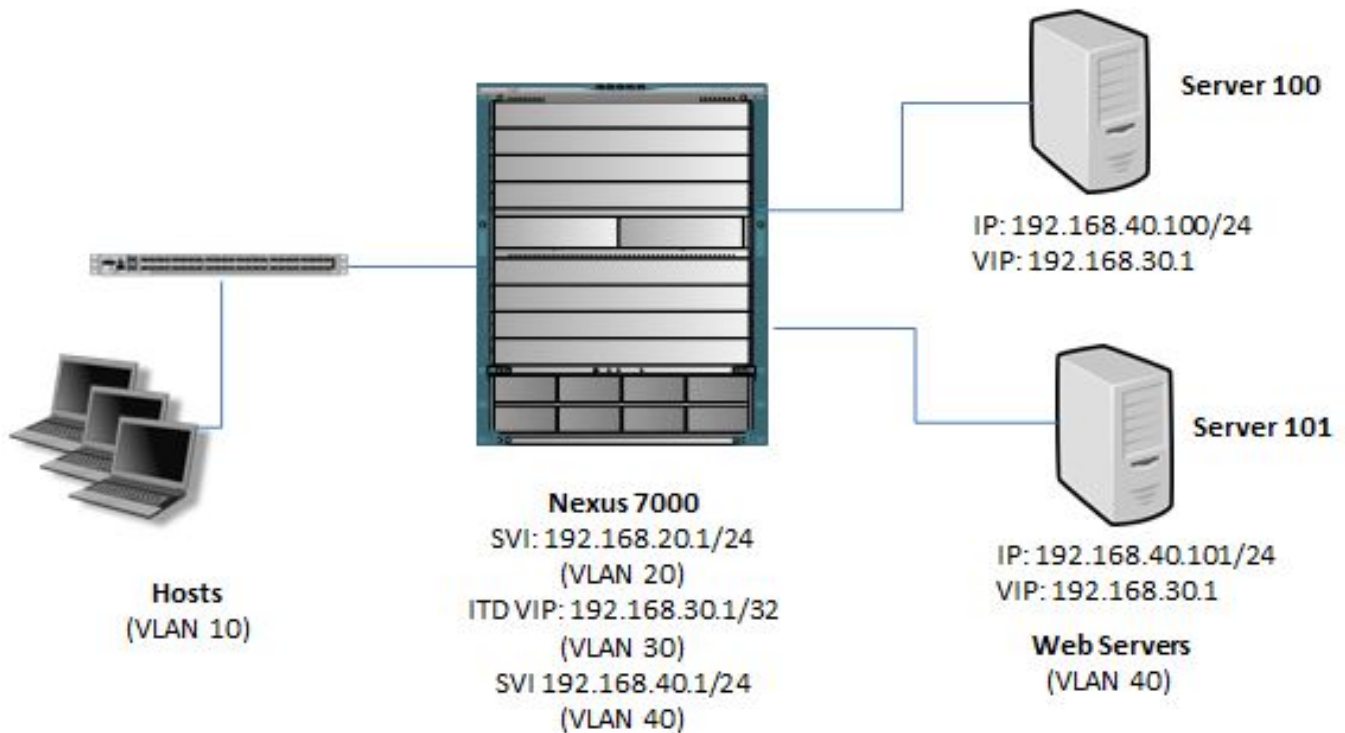
背景説明

ITD は、ITD ノードとして設定されている多数のデバイスの中で、特定のレイヤ 3 インターフェイスで入力するトラフィックのロード バランスに使用されます。

- ITD は、NX-OS バージョン 6.2(8) 以降の Nexus 7000 でサポートされ、バージョン 6.2(10) には重要な新機能があります。
- ITD は、ハードウェア コンポーネント（ラインカードのタイプ、シャーシのタイプなど）に関係なく実装できます。
- ITD によってスーパーバイザ モジュールの CPU の負荷が増えることはありません。

ITD とのトラフィック フロー

このドキュメントの情報は、次のトポロジに基づくものです。このシナリオで意図している望ましい影響は、VLAN 40 の Web サーバにアドレス指定されている VLAN 10 のホストからのトラフィックが、サーバ 100 とサーバ 101 の間でロード バランシングが行われている状態です。



- ITD は、Nexus 7000 のハードウェアでロード バランシングを実装するために、ポリシーベース ルーティングを使用します。ITD を設定すると、ITD で定義されるロード バランシング ポリシーに基づいてトラフィックを転送するために、アクセス リストとルート マップが動的に作成されます。
- これらのアクセス リストは、ITD の設定で構成された入インターフェイスに対して作成および適用されます。この場合、VLAN 20 で入力されるトラフィックは、アクセス リスト マスクで定義された最後のオクテットの有効ビットに基づき、「bucket_1」または「bucket_2」のいずれかに到達します。

```
N7k-2(config)# show ip access-lists
```

```
IP access list TEST_itd_vip_1_bucket_1
10 permit ip 1.1.1.0 255.255.255.127 192.168.30.1/32
IP access list TEST_itd_vip_1_bucket_2
10 permit ip 1.1.1.128 255.255.255.127 192.168.30.1/32
```

- その後、ルート マップにより、入力しているトラフィックが一致する節に基づいてトラフィックが転送されます。この例では、「bucket_1」に到達するトラフィックが 192.168.40.100 ノードに転送され、「bucket_2」に到達するトラフィックが 192.168.40.101 ノードに転送されているのを示しています。

```
N7k-1(config)# show route-map TEST_itd_pool
route-map TEST_itd_pool, permit, sequence 0
Description: auto generated route-map for ITD service TEST
Match clauses:
ip address (access-lists): TEST_itd_vip_1_bucket_1
Set clauses:
ip next-hop verify-availability 192.168.40.100 track 2 [ UP ]
route-map TEST_itd_pool, permit, sequence 1
Description: auto generated route-map for ITD service TEST
Match clauses:
ip address (access-lists): TEST_itd_vip_1_bucket_2
Set clauses:
ip next-hop verify-availability 192.168.40.101 track 2 [ UP ]
```

- IP アドレスは、ITD によって変換されません。Nexus 7000 から出力されてノードに向かうトラフィックは、宛先アドレス 192.168.30.1 を持ち、元の送信元 IP アドレスを保持してい

ます。

- リターン トラフィックはユニキャストで、ITD VIP 192.168.30.1 の発信元アドレスを持つ元の送信者に戻ります。

ヒント： 入カインターフェイスごとに1つのアドレス ファミリに対して、ポリシーベースルーティング (PBR) の1つのインスタンスのみがサポートされます。 インターフェイスをITD 入カインターフェイスとして定義した場合、ITD はロードバランシング アルゴリズムを実装するためにPBRを使用するため、そのインターフェイスでは追加のPBR インスタンスを設定できません。

設定

これらの機能は、ITD を設定する仮想デバイス コンテキスト (VDC) で有効にする必要があります。

```
N7k-1(config-itd)# show run | i feature
feature pbr
feature sla sender
feature sla responder
feature itd
```

ステップ 1： ITD デバイス グループの設定

ITD デバイス グループは、Web サーバ、ファイアウォールなど、トラフィックのロード バランスが行われるノードで構成されます。 デバイス グループは次のように設定されています。

```
N7k-1(config)# itd device-group TAC-device-group
N7k-1(config-device-group)# node ip 192.168.40.100
N7k-1(config-device-group)# node ip 192.168.40.101
N7k-1(config-device-group)# probe icmp
```

プローブの設定

プローブの設定では、次のプローブの種類を定義できます。

- icmp** Internet Control Message Protocol (ICMP) エコー要求を送信し、応答を待機します。サーバが応答すると、ITD はそのサーバに [passed] のマークを付けます。
- dns** ドメイン ネーム サーバ (DNS) に要求を送信し、設定済みのドメインをサーバに渡します。サーバがそのドメインの設定済みの IP アドレスを使用して応答した場合、ITD はそのアドレスに [up] のマークを付けます。
- udp** サーバに UDP パケットを送信し、サーバから ICMP Port Unreachable メッセージが返された場合、サーバに [failed] のマークを付けます。
- tcp** TCP の 3 方向ハンドシェイクを開始して、サーバから応答が送信されるまで待機します。ハンドシェイクが成功すると、ITD はセッションを終了するために FIN を送信します。応答が無効な場合、または応答がない場合、ITD はそのサーバに [failed] のマークを付けます。

一般的に、DNS、UDP、および TCP プローブは、ノード サーバ上で実行される特定のサービスの可用性を評価するために使用されます。

プローブの設定では、次のパラメータも定義できます。

- frequency : ITD が x 秒ごとにノードに ping を送信します。
- timeout : ITD は y 秒以内にノードからの応答があると想定します。
- retry-down-count : [Probe Fail] のマークが付き、失敗アクションが実行される前にノードをプローブする回数です。
- retry-up-count : [OK] のマークが付き、プールにもう一度追加される前にノードをプローブする回数です。

たとえば、次の設定を考えてみます (これは、probe icmp を設定するときのデフォルト設定です)。

```
probe icmp frequency 10 timeout 5 retry-down-count 3 retry-up-count 3
```

1 2 3 4

1. 10 秒ごとにノードに ping を送信します。
2. ノードの応答に 5 秒かかります。
3. ノードが 3 回応答に失敗すると、ノードに [Probe Fail] のマークを付けます。
4. ノードが続けて 3 回応答した後で、ノードに [OK] のマークを付けます。

このように設定すると、ITD は 35 秒 (3 × 頻度 + タイムアウト) 以上経過した後で到達不能になったノードに対応します。

ノードレベルのスタンバイ

ノードレベルまたはデバイスグループレベルでノードを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が失敗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、アクティブノードが失敗した場合にトラフィックを受信します。

デバイスレベルのスタンバイの設定は次のとおりです。

```
7k-1(config-device-group)# node ip 192.168.40.100 standby 192.168.40.103
```

デバイスグループレベルのスタンバイの設定は次のとおりです。

```
7k-1(config-device-group)# node ip 192.168.40.106 mode hot-standby
```

ステップ 2 : ITD サービスの設定

この手順では ITD サービス、つまりロード バランスを行うトラフィックとその方法が定義されません。

ITD サービスの設定

```
N7k-1(config)# itd TAC-ITD-service
```

デバイス グループの定義

以前設定したデバイス グループを参照します。

```
N7k-1(config-itd)# device-group TAC-device-group
```

入インターフェイスの設定

このインターフェイスで入力するトラフィックは、ITD によってロード バランシングが行われます。入インターフェイスは、レイヤ 3 インターフェイス (物理インターフェイス、PortChannel、またはスイッチ仮想インターフェイス (SVI)) にする必要があります。

```
N7k-1(config-itd)# ingress interface vlan 20
```

レイヤ 3 インターフェイスは、ITD の 1 つのインスタンスの入インターフェイスとしてのみ割り当てることができます。

注意： ITD 入インターフェイスは、レイヤ 3 インターフェイスにする必要があります。

ITD の仮想 IP アドレスの設定

ITD の仮想 IP アドレス (VIP) は、ホストおよびノードとは違うサブネット上に存在している必要があります。

```
N7k-1(config-itd)# virtual ip 192.168.30.1 255.255.255.255 advertise enable
```

ITD VIP は、本質的には Nexus 7000 の側から見るとダミー インターフェイスです。たとえば、スイッチが VIP にアドレス指定された ping 要求に応答しません。自動的に作成されて ITD 入インターフェイスに適用されるルート マップに対してトラフィックを一致させるために使用されます。

ヒント： 終了ノードに VIP のアドレスが設定されるまで、ITD VIP への ping の送信に成功することはできません。

ITD のロード バランス メソッドの定義

```
N7k-1(config-itd)# virtual ip 192.168.30.1 255.255.255.255 advertise enable
```

ロード バランス メソッドにより、ロードバランシングのハッシュ機構を定義できます。次のオプションを使用できます。

```
src ip          送信元 IP
src ip-l4port   送信元 IP および L4 ポート
dst ip          宛先 IP
dst ip-l4port   宛先 IP および L4 ポート
```

ヒント： ITD サービスまたはデバイス グループの設定を変更するために、ITD サービスは

、**shut** 状態になっている必要があります。

ステップ3：フェールオーバー動作の定義

ITD がノード障害に反応しないようにフェールオーバー動作を定義する必要があります。

```
N7k-1(config-itd)# failaction node reassign
```

ITD 関連の設定を表示するには、**show run services** コマンドを入力します。

```
N7k-2# show run services
```

```
!Command: show running-config services
!Time: Wed Apr 22 00:15:11 2015
```

```
version 6.2(10)
feature itd
```

```
itd device-group TAC
node ip 192.168.40.100
node ip 192.168.40.101
probe icmp frequency 10 timeout 5 retry-down-count 1 retry-up-count 1
```

```
itd TEST
device-group TAC
virtual ip 192.168.30.1 255.255.255.255 advertise enable
ingress interface Vlan20
failaction node reassign
load-balance method src ip buckets 2
no shut
```

ステップ4：ノードサーバでのループバック インターフェイスとしての ITD VIP の設定

サーバが ITD VIP にアドレス指定されたトラフィックに対応するために、サーバ上のループバック インターフェイスで IP エイリアスとして設定する必要があります。サーバは VIP の宛先アドレスの要求を受け入れ、ITD VIP アドレスからの応答を取得します。

[Linux の仮想ネットワーク インターフェイスの設定](#)

[Windows で Microsoft ループバック アダプタをインストールする方法](#)

注: サーバの IDT VIP 設定は Direct Server Return (DSR) の場合にだけ必要です。アプライアンスのロードバランシング (Cisco 適応型セキュリティ アプライアンス (ASA) のロードバランシングなど) の場合は、VIP の設定は必要ありません。

その他の設定オプション

ノードへのウェイトの割り当て

ロード バランス メソッドにより、トラフィックを分割するバケット数を定義できます。バケットの設定は任意です。デフォルトでは、バケットの数は設定されたノードの数に等しいです。バケットの数を設定する場合は、値を2の累乗(2、4、8、16、32など)にする必要があります。設定は次のようになります。

```
N7k-2(config-itd)# load-balance method src ip buckets 16
```

デフォルトでは、バケットはラウンド ロビン パターンでのアクティブ ノードに割り当てられています。ただし、多くのバケットを持つ特定のノードを評価することができます。これは実際には、1つ以上のデバイスを優先するようトラフィックを評価します。評価はデバイスグループの設定で割り当てます。このコンフィギュレーション サーバ 101 は、サーバ 100 の2倍の量のトラフィックを受信します。

```
N7k-2(config-itd)# load-balance method src ip buckets 16
```

show itd コマンドの出力を使用して、バケットの割り当てを確認できます。

```
N7k-2(config-itd)# show itd
```

```
Name Probe LB Scheme Status Buckets
```

```
-----  
TEST TCP src-ip ACTIVE 16
```

```
Device Group VRF-Name
```

```
-----  
TAC
```

```
Pool Interface Status Track_id
```

```
-----  
TEST_itd_pool Vlan20 UP 3
```

```
Virtual IP Netmask/Prefix Protocol Port
```

```
-----  
192.168.20.1 / 255.255.255.255 IP 0
```

```
Node IP Config-State Weight Status Track_id Sla_id
```

```
-----  
1 192.168.40.100 Active 33 OK 1 10001
```

```
Bucket List
```

```
-----  
TEST_itd_vip_1_bucket_1
```

```
TEST_itd_vip_1_bucket_3
```

```
TEST_itd_vip_1_bucket_5
```

```
TEST_itd_vip_1_bucket_7
```

```
TEST_itd_vip_1_bucket_9
```

```
TEST_itd_vip_1_bucket_16
```

```
Node IP Config-State Weight Status Track_id Sla_id
```

```
-----  
2 192.168.40.101 Active 66 OK 2 10002
```

```
Bucket List
```

```
-----  
TEST_itd_vip_1_bucket_2
```

```
TEST_itd_vip_1_bucket_4
```



```
TEST_itd_vip_1_bucket_6
TEST_itd_vip_1_bucket_8
TEST_itd_vip_1_bucket_10
TEST_itd_vip_1_bucket_11
TEST_itd_vip_1_bucket_12
TEST_itd_vip_1_bucket_13
TEST_itd_vip_1_bucket_14
TEST_itd_vip_1_bucket_15
```

失敗アクションの設定

ノードが失敗したら、プローブが検出して [Probe Fail] 状態にします。デフォルトでは、ITD は失敗したノードにトラフィックを転送し続けます。ITD がトラフィックを失敗したノードから他の場所へ移動するには、次のように設定する必要があります。

```
itd TEST
```

```
failaction node reassign
```

ノードが到達不能になると、どうなりますか。

- **failaction node reassign** が設定されている場合、ITD は到達不能なノードを [Probe Fail] モードにして、デバイスグループのほかのノードにトラフィックをルーティングします。
- **failaction node reassign** が設定されていない場合：シナリオ 1：プローブが設定済み、スタンバイノードが設定済み：トラフィックは最初に利用できるスタンバイノードに転送されます。シナリオ 2：プローブが設定済み、スタンバイノードの設定なし：トラフィックは再び割り当てられず、ルーティングされます。シナリオ 3：プローブの設定なし：ITD は失敗を検出できず、トラフィックは利用できないノードに引き続き転送されます。
- すべてのノードが到達不能になると、トラフィックがルーティングされます。

確認

ここでは、基本的な ITD の設定と運用を確認する方法について説明します。

ITD サービスの確認

ITD のステータスを表示するには、**show itd** コマンドを入力します。

- サービスが **ACTIVE** 状態になっていることを確認します。
- デバイスプールが **UP** 状態になっていることを確認します。
- ノードが **OK** 状態になっていることを確認します。

```
N7k-2(config-itd)# show itd
```

```
Name Probe LB Scheme Status Buckets
```

```
-----  
TEST TCP src-ip ACTIVE 16
```

```
Device Group VRF-Name
```

```
-----  
TAC
```

```
Pool Interface Status Track_id
```

```

-----
TEST_itd_pool Vlan20 UP          3

Virtual IP Netmask/Prefix Protocol Port
-----
192.168.20.1 / 255.255.255.255 IP 0

Node IP Config-State Weight Status Track_id Sla_id
-----
1 192.168.40.100 Active 33 OK          1          10001

Bucket List
-----
TEST_itd_vip_1_bucket_1
TEST_itd_vip_1_bucket_3
TEST_itd_vip_1_bucket_5
TEST_itd_vip_1_bucket_7
TEST_itd_vip_1_bucket_9
TEST_itd_vip_1_bucket_16

Node IP Config-State Weight Status Track_id Sla_id
-----
2 192.168.40.101 Active 66 OK          2          10002

Bucket List
-----
TEST_itd_vip_1_bucket_2
TEST_itd_vip_1_bucket_4
TEST_itd_vip_1_bucket_6
TEST_itd_vip_1_bucket_8
TEST_itd_vip_1_bucket_10
TEST_itd_vip_1_bucket_11
TEST_itd_vip_1_bucket_12
TEST_itd_vip_1_bucket_13
TEST_itd_vip_1_bucket_14
TEST_itd_vip_1_bucket_15

```

動的に作成されたアクセスリストとルートマップの確認

この設定は、ITD を設定するときに動的に作成されます。

- 設定済みのバケットごとに、1つのアクセスリストとルートマップがあります。
- ルートマップとアクセスリストは、ITD のサービス名をプレフィックスとして使用して作成されます (<service name>_itd_vip_1_bucket_1 など)。

```

N7k-2(config)# show ip access-lists

IP access list TEST_itd_vip_1_bucket_1
10 permit ip 1.1.1.0 255.255.255.127 192.168.20.1/32
IP access list TEST_itd_vip_1_bucket_2
10 permit ip 1.1.1.128 255.255.255.127 192.168.20.1/32

N7k-2(config)# sho route-map TEST_itd_pool
route-map TEST_itd_pool, permit, sequence 0
Description: auto generated route-map for ITD service TEST
Match clauses:
ip address (access-lists): TEST_itd_vip_1_bucket_1
Set clauses:
ip next-hop verify-availability 192.168.30.2 track 2 [ UP ]
route-map TEST_itd_pool, permit, sequence 1

```

```
Description: auto generated route-map for ITD service TEST
Match clauses:
ip address (access-lists): TEST_itd_vip_1_bucket_2
Set clauses:
ip next-hop verify-availability 192.168.30.2 track 2 [ UP ]
```

入カインターフェイス設定の確認

ルート マップが ITD 入カインターフェイスに適用されることを確認します。

```
N7k-2(config-itd)# show run int vlan 20
!Command: show running-config interface Vlan20
!Time: Thu Apr 23 00:42:41 2015
version 6.2(10)
interface Vlan20no shutdown
ip address 192.168.20.1/24
ip policy route-map TEST_itd_pool
```

プローブ設定の確認

次のコマンドからの以下の出力で、プローブの頻度がプログラミングされたことを確認します。

```
N7k-2# show run | i probe
probe icmp frequency 5
```

```
N7k-2# show run sla sender
```

```
!Command: show running-config sla sender
!Time: Tue Apr 28 18:04:02 2015
```

```
version 6.2(10)
feature sla sender
```

```
ip sla 10001
icmp-echo 192.168.40.100
frequency 5
ip sla schedule 10001 life forever start-time now
ip sla 10002
icmp-echo 192.168.40.101
frequency 5
ip sla schedule 10002 life forever start-time now
```

インターネット プロトコルのサービス レベル契約 (IPSLA) オブジェクトは、ITD が設定される
ときに動的に作成されます。これらのオブジェクトは、ITD のルート マップで参照されます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director コマンド リファレンス](#)

- [Cisco Nexus 7000 Series NX-OS Intelligent Traffic Director コンフィギュレーション ガイド、リリース 6.x](#)
- [Cisco Intelligent Traffic Director の概要](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)