

Ejemplo de configuración inteligente del Traffic Director del nexo 7000

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de tráfico con el ITD](#)

[Configurar](#)

[Paso 1: Configure al grupo de dispositivos ITD](#)

[Configuración de sonda](#)

[Recurso seguro llano del nodo](#)

[Paso 2: Servicio de la configuración ITD](#)

[Configure el servicio ITD](#)

[Defina al grupo de dispositivos](#)

[Configure la interfaz de ingreso](#)

[Configure a la dirección IP virtual ITD](#)

[Defina el método del balance de la carga ITD](#)

[Paso 3: Defina el comportamiento de la Conmutación por falla](#)

[Paso 4: Configure el ITD VIP como Loopback Interface en los servidores del nodo](#)

[Otras opciones de configuración](#)

[Asigne las ponderaciones a los Nodos](#)

[Configure Failaction](#)

[Verificación](#)

[Verifique los servicios ITD](#)

[Verifique las Listas de acceso dinámicamente creadas y el Route Map](#)

[Verifique la configuración de la interfaz de ingreso](#)

[Verifique la configuración de sonda](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos básicos para resolver problemas y para verificar al Traffic Director inteligente (ITD) en el nexo 7000. Este documento utiliza un **despliegue del Server Load Balancing** para ilustrar los conceptos relacionados con el ITD.

Para más información sobre el ITD, refiera a estos recursos:

- [Traffic Director inteligente de Cisco de un vistazo](#)
- [Referencia de comandos inteligente del Traffic Director de las 7000 Series NX-OS del nexa de Cisco](#)

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del ITD.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 7000 Series Switch del nexa de Cisco
- Versión 6.2(10) del Cisco NX-OS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

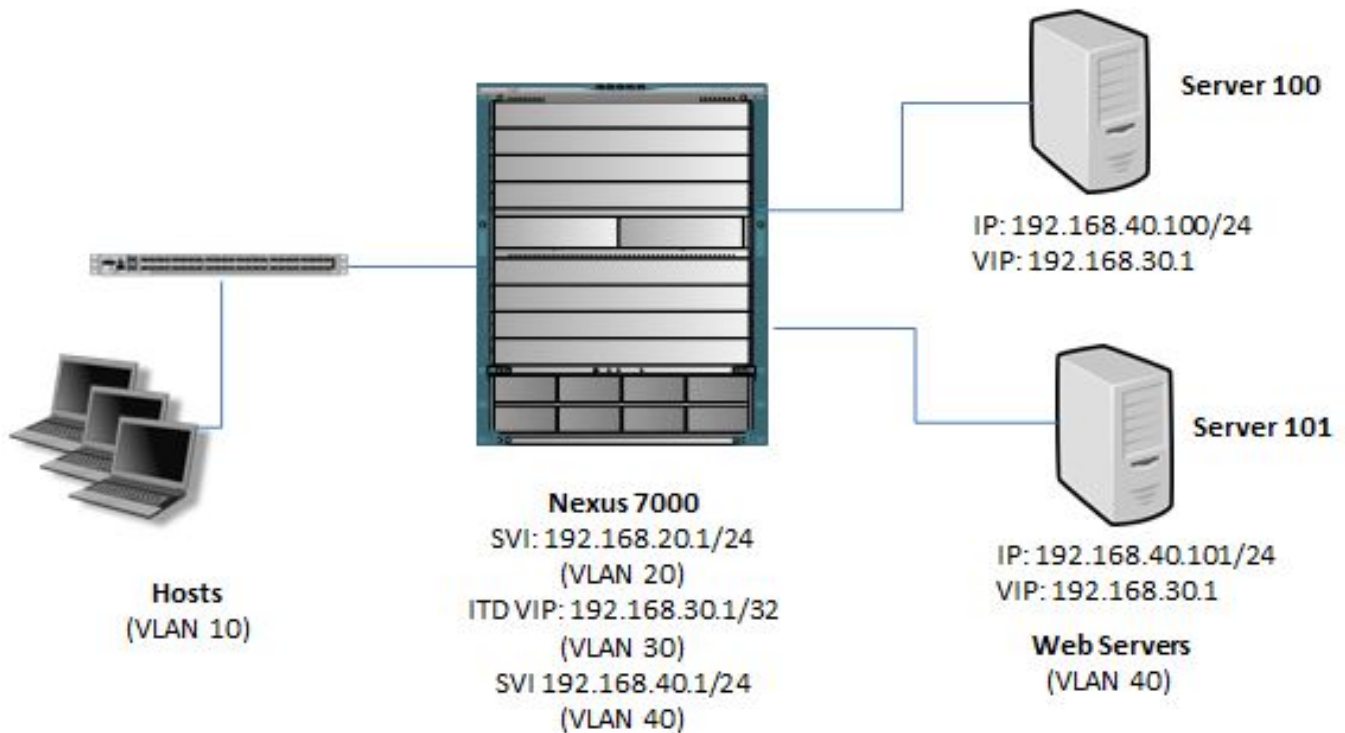
Antecedentes

El ITD se utiliza para cargar el tráfico de la balanza que los ingresos en una interfaz específica de la capa 3 entre varios dispositivos configuraron como Nodos ITD.

- El ITD se soporta en el nexa 7000 en la versión 6.2(8) y posterior NX-OS y tiene nuevas funciones significativas en la versión 6.2(10).
- El ITD puede ser componentes independientes del hardware implementados (los tipos del linecard, chasis teclean, etc).
- El ITD no agrega ninguna carga al módulo de Supervisor CPU.

Flujo de tráfico con el ITD

La información en este documento se basa en esta topología. En este escenario, el efecto deseado está para el tráfico de los host en el VLAN10 dirigido a los servidores Web en el VLA N 40 para ser carga equilibrio entre el servidor 100 y el servidor 101.



- El ITD utiliza el Policy-Based Routing para implementar el Equilibrio de carga en hardware en el nexa 7000. Cuando se configura el ITD, las Listas de acceso y un Route Map se crean dinámicamente para remitir el tráfico basado en su directiva del Equilibrio de carga definida en el ITD.
- Estas Listas de acceso se crean y se aplican a la interfaz de ingreso configurada en la configuración ITD. En este caso, tráfico que los ingresos en el VLAN20 golpean el "bucket_1" o el "bucket_2" basado en el bit significativo en el octeto más reciente definido por la máscara de la lista de acceso:

```
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
```

- El Route Map entonces adelante que el tráfico basó en contra qué cláusula hace juego el tráfico ingressing. Este ejemplo muestra ese tráfico que los golpes el "bucket_1" se remitan al nodo y al tráfico de 192.168.40.100 que los golpes el "bucket_2" se remiten al nodo de 192.168.40.101.

```
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 ]
```

- La dirección IP **no es traducida por el ITD**. El tráfico que las salidas el nexa 7000 hacia los Nodos tienen una dirección destino de 192.168.30.1 y conservan la dirección IP de la fuente

original.

- El tráfico de retorno es unicast de nuevo al emisor original con una dirección de origen del ITD VIP 192.168.30.1.

Tip: Solamente un caso del Routing basado en políticas (PBR) se soporta por la familia del direccionamiento por la interfaz de ingreso. Si usted define una interfaz como interfaz de ingreso ITD, usted no podrá configurar los casos adicionales PBR en esta interfaz puesto que el ITD utiliza el PBR para implementar el algoritmo del balanceo de carga.

Configurar

Estas características se deben habilitar en el contexto del dispositivo virtual (VDC) en el cual usted configura el ITD:

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

Paso 1: Configure al grupo de dispositivos ITD

El grupo de dispositivos ITD consiste en los Nodos entre los cuales el tráfico será carga balanceada, tal como servidores Web, los Firewall, y así sucesivamente. Configuran al grupo de dispositivos como sigue:

```
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
```

Configuración de sonda

La configuración de sonda permite que usted defina estos tipos de la sonda:

- | | |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP | Envía un pedido de eco del Internet Control Message Protocol (ICMP) y está atenta una respuesta servidor vuelve una respuesta, el ITD marca el servidor según lo pasado. |
| dns | Envía una petición a un Domain Name Server (DNS) ese los pasos un dominio configurado al servidor. Si el servidor responde con un IP Address configurado para ese dominio, el ITD marca el direccionamiento como para arriba. |
| udp | Envía un paquete UDP a un servidor y marca el servidor según lo fallado solamente si el servidor devuelve un mensaje inalcanzable del puerto ICMP. |
| tcp | Inicia un apretón de manos de tres vías TCP y espera que el servidor envíe una respuesta. Si el apretón de manos es acertado, el ITD envía un FIN para terminar la sesión. Si la respuesta es inválida o si no hay respuesta, el ITD marca el servidor según lo fallado. |

Las sondas generalmente DNS, UDP, y TCP serían utilizadas a los asnos la Disponibilidad de los servicios específicos que se ejecutan en los servidores del nodo.

La configuración de sonda también permite que usted defina estos parámetros:

- frecuencia - El ITD hace ping al nodo cada x segundos
- descanso - El ITD cuenta con una respuesta del nodo dentro de los segundos y
- comprobación-abajo-cuenta - cuántas veces de sondear el nodo antes de que se marque como "falla de la sonda" y el failaction se ejecuta
- comprobación-arriba-cuenta - cuántas veces de sondear el nodo antes de que se marque como "OK" y se agregada al pool

Por ejemplo, considere esta configuración (ésta es la configuración predeterminada cuando usted configura el **ICMP de la sonda**):

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

1 2 3 4

1. Haga ping al nodo cada 10 segundos.
2. Permita que 5 segundos para el nodo contesten.
3. Después de que el nodo no pueda contestar 3 veces, marque el nodo como "falla de la sonda".
4. Después de que el nodo conteste 3 veces en fila, marque el nodo como "OK".

Dado esta configuración, el ITD **reacciona a un nodo que llegue a ser inalcanzable después por lo menos de 35 segundos** (frecuencia + descanso 3 x).

Recurso seguro llano del nodo

Un nodo se puede configurar como recurso seguro en el nivel del nodo o el nivel de grupo de dispositivos. Un recurso seguro del nivel del nodo recibe el tráfico solamente si su nodo activo asociado falla. Un recurso seguro del nivel de grupo de dispositivos recibe el tráfico si los nodos activos uces de los fallan.

La configuración espera del dispositivo-nivel es:

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

La configuración espera del grupo de dispositivos es:

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

Paso 2: Servicio de la configuración ITD

En este paso que el ITD mantiene se define, es decir, el tráfico usted quiere cargar la balanza y cómo.

Configure el servicio ITD

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

Defina al grupo de dispositivos

Refiérase al grupo de dispositivos previamente configurado:

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

Configure la interfaz de ingreso

Trafi que los ingresos en esta interfaz son carga balanceada por el ITD. La interfaz de ingreso **debe ser una interfaz de la capa 3** (interfaz física, portchannel, o Switched Virtual Interface (SVI)).

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

Cada interfaz de la capa 3 se puede asignar solamente como una interfaz de ingreso para un caso del ITD.

Caution: La interfaz de ingreso ITD debe ser una **interfaz de la capa 3**.

Configure a la dirección IP virtual ITD

La dirección IP virtual ITD (VIP) debe estar en una **diversa subred** que los host y los Nodos:

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

El ITD VIP es esencialmente una interfaz simulada de la perspectiva del nexo 7000 - por ejemplo, el Switch no responde a los pedidos de ping dirigidos al VIP. Se utiliza para hacer juego el tráfico contra el Route Map que se crea y se aplica automáticamente a la interfaz de ingreso ITD.

Tip: Usted **no podrá hacer ping con éxito el ITD VIP** hasta que los nodos extremos se configuren con el direccionamiento VIP.

Defina el método del balance de la carga ITD

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

El método del balance de la carga permite que usted defina su mecanismo del picado del balanceo de carga. Estas opciones están disponibles:

IP del src IP de la fuente
src ip-l4port De la fuente puerto IP y L4
IP del dst IP de destino
dst ip-l4port IP de destino y puerto L4

Tip: El servicio ITD necesita ser en el estado **cerrado** para modificar el servicio ITD o la configuración del grupo de dispositivos.

Paso 3: Defina el comportamiento de la Conmutación por falla

Usted debe configurar un comportamiento de la Conmutación por falla o el ITD no reaccionará a la falla de nodo:

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

Para visualizar la configuración relacionada ITD, ingrese el comando de los **servicios del funcionamiento de la demostración**:

```
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
```

Paso 4: Configure el ITD VIP como Loopback Interface en los servidores del nodo

Para que los servidores sirvan el tráfico dirigido al ITD VIP, deben ser configurados como IP alias en el Loopback Interface en el servidor. El servidor valida los pedidos la dirección destino VIP y las fuentes que la respuesta del ITD VIP dirige.

[Configurar la interfaz de red virtual en Linux](#)

[Cómo instalar el adaptador de Loopback de Microsoft en Windows](#)

Note: La configuración de VIP IDT en el servidor se requiere solamente en el caso de una vuelta directa del servidor (DSR). En el caso del balanceo de carga del dispositivo (tal como balanceo de carga adaptante del dispositivo de seguridad de Cisco (ASA)), la configuración de VIP no se requiere.

Otras opciones de configuración

Asigne las ponderaciones a los Nodos

El método del balance de la carga también permite que usted defina cuántos compartimientos para partir el tráfico adentro. La configuración del compartimiento es opcional. Por abandono, el número de compartimientos es igual al número de Nodos configurados. Si usted quiere configurar el número de compartimientos, el valor debe ser un poder de 2 (2, 4, 8, 16, 32, y así sucesivamente). La configuración es la siguiente:

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

Por abandono, los compartimientos se asignan a los nodos activos en un modelo del ordenamiento cíclico. Sin embargo, usted puede cargar ciertos Nodos con más compartimientos, que en efecto carga el tráfico para favorecer a uno o más el dispositivo. Usted asigna la ponderación bajo configuración del grupo de dispositivos. En este servidor de configuración 101 recibe dos veces más tráfico como el servidor 100.

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

Usted puede verificar las asignaciones del compartimiento con la salida del comando del **itd de la demostración**:

```
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
```

Configuración Failaction

Cuando un nodo falla, la sonda lo detecta y lo pone en “el estado del fall de la sonda”. **Por abandono, el ITD continúa remitiendo el tráfico al nodo fallado.** Para hacer que el ITD desvíe el tráfico lejos de un nodo fallado, esto debe ser configurada:

```
itd TEST
failaction node reassign
```

Qué sucede cuando un nodo llega a ser inalcanzable:

- Si se configura el **nodo del failaction reassigna** - El ITD pondrá el nodo inalcanzable en el modo del **fall de la sonda** y ruteará el tráfico a otros Nodos en el grupo de dispositivos.
- Si el **nodo del failaction reassigna** no se configura: Escenario 1: Sonda configurada/nodo espera configurado: tráfico dirigido al primer nodo espera disponible. Escenario 2: Sonda configurada, ningún nodo espera configurado: el tráfico no reasignado, consigue ruteado. Escenario 3: Ninguna sonda configurada: El ITD no puede detectar el error, tráfico continúa siendo remitido a un nodo inasequible.
- Si **todos los Nodos** son inalcanzables, se rutea el tráfico.

Verificación

Esta sección describe cómo verificar la configuración básica y la operación ITD.

Verifique los servicios ITD

Para ver el estatus del ITD, ingrese el comando del **itd de la demostración**.

- Verifique que el servicio esté en el **estado activo**.
- Verifique que la agrupación de dispositivos esté en el estado **ASCENDENTE**.
- Verifique que los Nodos estén en el estatus **ACEPTABLE**.

```
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
```

Verifique las Listas de acceso dinámicamente creadas y el Route Map

Esta configuración se crea dinámicamente cuando usted configura el ITD:

- Habrá una entrada de la lista de acceso y del Route Map por el compartimento configurado.
- Los mapa del ruta y las Listas de acceso se crean con el nombre del servicio ITD prefijado (por ejemplo, el <service name>_itd_vip_1_bucket_1).

```
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 ]
```

Verifique la configuración de la interfaz de ingreso

Verifique que el Route Map esté aplicado a la interfaz de ingreso ITD:

```
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
```

Verifique la configuración de sonda

Verifique que la frecuencia de la sonda esté programada en esta salida de este comando:

```
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
```

Los objetos del Service Level Agreement del protocolo de Internet (IPSLA) se crean dinámicamente cuando se configura el ITD. Estos objetos se refieren al Route Map ITD.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Referencia de comandos inteligente del Traffic Director de las 7000 Series NX-OS del nexa de Cisco](#)

- [Guía de configuración inteligente del Traffic Director de las 7000 Series NX-OS del nexo de Cisco, versión 6.x](#)
- [Traffic Director inteligente de Cisco de un vistazo](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)