



ID документа: 118950

Обновлено: 04 мая 2015

Внесенный Дезом Хиллом, специалистом службы технической поддержки Cisco.



[PDF загрузки](#)



[Печать](#)



[Feedback](#)

Родственные продукты

- [Cisco 7000 Series Routers](#)

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Трафик с ITD](#)

[Настройка](#)

[Шаг 1: Настройте группу устройств ITD](#)

[Тестовая конфигурация](#)

[Резерв уровня узла](#)

[Шаг 2: Настройте сервис ITD](#)

[Настройте сервис ITD](#)

[Определите группу устройств](#)

[Настройте входной интерфейс](#)

[Настройте виртуальный IP - адрес ITD](#)

[Определите ITD, распределяют нагрузку метод](#)

[Шаг 3: Определите поведение аварийного переключения](#)

[Шаг 4: Настройте VIP ITD как интерфейс обратной связи на серверах узла](#)

[Другие параметры конфигурации](#)

[Назначьте веса на узлы](#)

[Настройте Failaction](#)

[Проверка](#)

[Verify ITD Services](#)

[Проверьте динамично созданные списки доступа и Карту маршрутизации](#)

[Проверьте конфигурацию входного интерфейса](#)

[Проверьте тестовую конфигурацию](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает основные шаги, чтобы устранить неполадки и проверить Умное устройство управления трафиком (ITD) на Nexus 7000. Этот документ использует развертывания распределения нагрузки сервера для иллюстрирования понятий,

отнесенных к ITD.

Для получения дополнительной информации на ITD, обратитесь к этим ресурсам:

- [Cisco умное устройство управления трафиком С первого взгляда](#)
- [Cisco Nexus NX-OS серии 7000 интеллектуальный Справочник по командам устройства управления трафиком](#)

Предварительные условия

Требования

Cisco рекомендует ознакомиться с ITD.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Cisco Nexus серии 7000
- Версия 6.2 (10) Cisco NX-OS

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

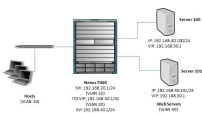
Общие сведения

ITD используется для распределения нагрузки трафика что входы на определенном Интерфейсе уровня 3 между многими устройствами, настроенными как узлы ITD.

- ITD поддерживается на Nexus 7000 в Версии 6.2 (8) NX-OS и позже и имеет существенно новые функции в Версии 6.2 (10).
- ITD может быть внедрен независимые от оборудования компоненты (типы линейной платы, тип шасси, и так далее).
- ITD не добавляет загрузки к ЦП модуля супервизора.

Трафик с ITD

Сведения в этом документе основываются на этой топологии. В этом сценарии нужный эффект для трафика от хостов в VLAN 10, адресованном Web-серверам в VLAN 40, чтобы быть с балансировкой нагрузки между Сервером 100 и Сервером 101.



- ITD использует маршрутизацию на основе политик для реализации распределения нагрузки в аппаратных средствах на Nexus 7000. Когда ITD настроен, списки доступа и Карта маршрутизации динамично созданы для передачи трафика на основе политики распределения нагрузки, определенной в ITD.
- Эти списки доступа созданы и применены к входной интерфейс, настроенный в конфигурации ITD. В этом случае, трафик, что входы на VLAN 20 поражают или "bucket_1" или "bucket_2" на основе значимого бита в последнем октете, определенном маской списка доступа: `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
```

- Карта маршрутизации тогда передает трафик, на основе которого пункта ingressing трафик совпадает против. Данный пример показывает, что трафик, который поражает "bucket_1", передан к 192.168.40.100 узлам и трафику, который совершает нападки, "bucket_2" передан 192.168.40.101 узлам. `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-адрес не преобразован ITD. Трафик, что выходы Nexus 7000 к узлам имеют 192.168.30.1 адреса назначения (DA) и сохраняют IP-адрес исходного источника.
- Ответный трафик одноадресно передан назад исходному отправителю с адресом источника VIP ITD 192.168.30.1.

Совет: Только один экземпляр Маршрутизации на основе политик (PBR) поддерживается на семейство адресов на входной интерфейс. При определении интерфейса как входного интерфейса ITD вы не будете в состоянии настроить дополнительные экземпляры PBR на этом интерфейсе, так как ITD использует PBR для реализации распределяющего нагрузку алгоритма.

Настройка

Эти опции должны быть активированы в контексте виртуального устройства (VDC), в котором вы настраиваете ITD:

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

Шаг 1: Настройте группу устройств ITD

Группа устройств ITD состоит из узлов, между которыми трафик будет распределен на нагрузку, такие как веб-серверы, межсетевые экраны, и так далее. Группа устройств настроена следующим образом:

```
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
```

Тестовая конфигурация

Тестовая конфигурация позволяет вам определять эти тестовые типы:

icmp	Передает запрос эха Протокола ICMP и прислушивается к ответу. Если сервер возвращает ответ, ITD отмечает сервер, как передано.
dns	Отправляет запрос к Серверу доменных имен (DNS), который передает настроенный домен к серверу. Если сервер отвечает настроенным IP - адресом для того домена, ITD отмечает адрес как.
udp	Передает пакет UDP к серверу и отмечает сервер, как подведено, только если сервер возвращает порт ICMP Недостижимое сообщение.
tCP /*	Иницирует трехстороннее квитирование TCP и ожидает, что сервер передаст ответ. Если квитирование успешно, ITD передает FIN для окончания сеанса. Если ответ не допустим или нет никакого ответа, ITD отмечает сервер, как подведено.

Обычно DNS, UDP и зонды TCP использовались бы к задницам доступность определенных сервисов, которые работают на серверах узла.

Тестовая конфигурация также позволяет вам определять эти параметры:

- frequency - ITD пропинговывает узел каждый x секунды
- таймаут - ITD ожидает ответ от узла в течение y секунд
- retry-down-count - сколько раз зондировать узел, прежде чем он будет отмечен как "Тестовый Сбой", и failaction выполняется
- retry-up-count - сколько раз зондировать узел, прежде чем он будет отмечен как "ОК" и повторно добавленный к пулу

Например, рассмотрите эту конфигурацию (это - конфигурация по умолчанию при настройке тестового icmp):

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

1 2 3 4

1. Пропинговывайте узел каждые 10 секунд.
2. Позвольте 5 секундам для узла отвечать.
3. После того, как узел не в состоянии отвечать 3 раза, отмечать узел как "Тестовый Сбой".
4. После того, как узел отвечает 3 раза подряд, отметьте узел как "ОК".

Учитывая эту конфигурацию, ITD реагирует на узел, который становится недостижимым по крайней мере после 35 секунд (3 x частоты + таймаут).

Резерв уровня узла

Узел может быть настроен как резерв на уровне узла или уровне группы устройств. Резерв уровня узла получает трафик, только если отказывает его связанный активный узел. Если какой-либо из активных узлов отказывает, резерв уровня группы устройств получает трафик.

Конфигурация резерва уровня устройств:

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

Конфигурация резерва группы устройств:

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

Шаг 2: Настройте сервис ITD

В этом шаге сервис ITD определен, т.е. трафик, которого вы хотите сбалансировать нагрузку и как.

Настройте сервис ITD

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

Определите группу устройств

Сошлитесь на ранее настроенную группу устройств:

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

Настройте входной интерфейс

Трафик, что входы на этом интерфейсе распределены нагрузке ITD. Входным интерфейсом **должен быть Интерфейс уровня 3** (физический интерфейс, portchannel, или коммутируемый виртуальный интерфейс (SVI)).

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

Каждый Интерфейс уровня 3 может только быть назначен как входной интерфейс для одного экземпляра ITD.

Внимание: Входным интерфейсом ITD должен быть Интерфейс уровня 3.

Настройте виртуальный IP - адрес ITD

Виртуальный IP - адрес ITD (VIP) должен быть в **другой подсети** и, чем хосты и, чем узлы:

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

VIP ITD является по существу фиктивным интерфейсом с точки зрения Nexus 7000 - например, коммутатор не отвечает на запросы проверки доступности (ping request), адресованные VIP. Это используется для соответствия с трафиком против Карты маршрутизации, которая автоматически создана и применена к входной интерфейс ITD.

Совет: Вы не будете в состоянии успешно пропинговать VIP ITD, пока конечные узлы не будут настроены с адресом VIP.

Определите ITD, распределяют нагрузку метод

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

Распределять нагрузку метод позволяет вам определять свой механизм хеширования распределения нагрузки. Эти опции доступны:

<pre>ip src IP-адрес отправителя ip-l4port src Source IP и порт L4 ip dst IP-адрес назначения ip-l4port dst IP - адрес назначения и порт L4</pre>

Совет: Сервис ITD должен быть в закрытом состоянии для изменения сервиса ITD или конфигурации группы устройств.

Шаг 3: Определите поведение аварийного переключения

Необходимо настроить поведение аварийного переключения, или ITD не будет реагировать на сбой узла:

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

Для отображения связанной конфигурации ITD введите **показ** выполненная команда **сервисов**:

```
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
```

Шаг 4: Настройте VIP ITD как интерфейс обратной связи на серверах узла

Для серверов для обслуживания трафика, адресованного VIP ITD, они должны быть

настроены как псевдоним IP на интерфейсе обратной связи на сервере. Сервер принимает запросы об адресе назначения (DA) VIP и получает ответ от адреса VIP ITD.

[Виртуальный сетевой интерфейс Configuring в Linux](#)

[Как установить Microsoft Loopback adapter в Windows](#)

Примечание: VIP - конфигурация IDT на сервере только требуется в случае Прямого сервера возвращается (DSR). В случае распределения нагрузки устройства (такого как устройство адаптивной защиты Cisco (ASA) распределение нагрузки), не требуется VIP - конфигурация.

Другие параметры конфигурации

Назначьте веса на узлы

Распределять нагрузку метод также позволяет вам определять сколько блоков для разделения трафика в к. Конфигурация блока является дополнительной. По умолчанию количество блоков равно количеству настроенных узлов. Если вы хотите настроить количество блоков, значение должно быть питанием 2 (2, 4, 8, 16, 32, и так далее). Конфигурация приведена ниже:

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

По умолчанию блоки назначены на активные узлы в круговом образце. Однако можно взвесить определенные узлы с большим количеством блоков, который в действительности трафик весов для одобрения одного или более устройств. Вы назначаете вес под конфигурацией группы устройств. В этом сервере конфигурации 101 получает вдвое больше трафика как Сервер 100.

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

Можно проверить присвоения блока с выходными данными **показа itd** команда:

```
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
```

Настройте Failaction

Когда узел отказывает, зонд обнаруживает его и помещает его в "Тестовый Сбой" состояние. По умолчанию ITD продолжает передавать трафик к неисправному узлу. Для имени ITD, отклоняют трафик далеко от неисправного узла, это должно быть настроено:

```
itd TEST  
failaction node reassign
```

Когда узел становится недостижимым, что происходит:

- Если **failaction reassign узла** будет настроен - то ITD поместит недостижимый узел в **Тестовый режим Сбоя** и направит трафик к другим узлам в группе устройств.
- Если НЕ настроен **failaction reassign узла**: Сценарий 1: Зонд настроил/резервным узел настроенный: трафик, направленный к первому доступному резервному узлу. Сценарий 2: Зонд настроил, никакой резервный узел не настроил: трафик, не повторно назначенный, маршрутизируется. Ситуация 3: Никакой зонд не настроил: ITD не может обнаружить сбой, трафик продолжает быть переданным к недоступному узлу.
- Если **все** узлы недостижимы, трафик маршрутизируется.

Проверка

В этом разделе описывается проверить основную конфигурацию ITD и операцию.

Verify ITD Services

Для просмотра статуса ITD введите **показ itd** команда.

- Проверьте, что сервис находится в **Состоянии Активно**.
- Проверьте, что аппаратный пул находится в **Работоспособном состоянии**.
- Verify, что узлы находятся в статусе **ОК**.

```
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
```

Проверьте динамично созданные списки доступа и Карту маршрутизации

Эта конфигурация динамично создана при настройке ITD:

- Будет одна запись Списка доступа и Карты маршрутизации на настроенный блок.
- Карты маршрутизации и списки доступа созданы со снабженным префиксом именем сервиса ITD (такой как, <имя сервиса> _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 ]
```

Проверьте конфигурацию входного интерфейса

Проверьте, что Карта маршрутизации применена к входному интерфейсу 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
```

Проверьте тестовую конфигурацию

Проверьте, что тестовая частота запрограммирована в этих выходных данных от этой команды:

```
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
```

Когда ITD настроен, объекты Internet Protocol Service Level Agreement (IPSLA) динамично созданы. На эти объекты ссылаются в Карте маршрутизации ITD.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- [Cisco Nexus NX-OS серии 7000 интеллектуальный Справочник по командам устройства управления трафиком](#)
- [Cisco Nexus NX-OS серии 7000 интеллектуальное руководство по конфигурации устройства управления трафиком, выпуск 6. x](#)
- [Cisco умное устройство управления трафиком С первого взгляда](#)
- [Cisco Systems – техническая поддержка и документация](#)

Действительно ли этот документ был полезен? [Да](#) [Нет](#)

Спасибо за ваш отзыв.

[Адресовать вопрос техподдержке \(требуется контракт сервиса Cisco.📄\)](#)

Связанные обсуждения Сообщества Cisco Support

[Сообщество Cisco Support](#) является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

См. [Cisco Technical Tips Conventions](#) для получения информации об условных обозначениях, используемых в этом документе.