



# H3C iMC NTAの導入



内容

NTAの特徴

NTAの設定

トラブルシューティング

# iMCのシステム構造



モニタリング

iMC

点

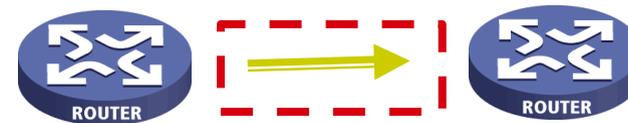
PLAT/APM/SSM



Platform(PLAT)  
Application Manager(APM)  
Security Service Manager(SSM)

線

NTA/NPD/MVM

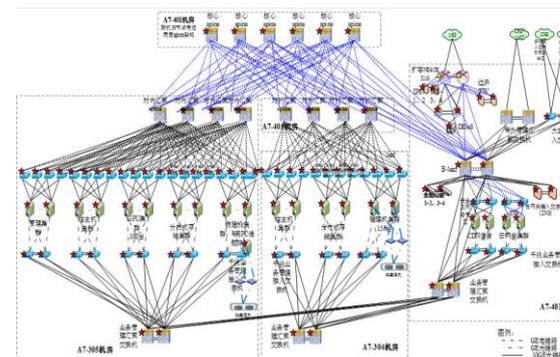


Network Traffic Analyzer(NTA)  
Network Performance Diagnosis(NPD)  
MPLS VPN Manager(MVM)

システム

BSM/CMDB

Business Service Manager(BSM)  
Configuration Management Database Management(CMDB)



# NTAの簡単な紹介



iMC UBA

iMC NTA

User Behavior Auditor (UBA)

iMC PLAT

- NTAは、プラットフォームに基づくiMCのコンポーネントです。
- NTAコンポーネントには、ネットワーク動作解析、ネットワーク動作解析サーバ、ネットワークトラフィック解析、ネットワークトラフィック解析サーバが含まれます。

Component Name	Description	Version	Status	Deployment L...
iMC Platform - Syslog Management	Collects, filters, and analyzes ...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - ACL Management	Configures ACLs for devices to ...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - VLAN Management	Manages VLAN resources.	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - CMDB Management	Manages and maintains the CMDB d...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - User Selfservice M...	Manages the self-service busines...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - Guest Access Manag...	Manages guest accounts.	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - Security Control C...	Monitors network events and cont...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - General Search Ser...	Manages the general search servi...	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - Virtual Resource M...	Manages virtual resources.	iMC PLAT 7.3 (E0703)	Deployed	Master Server
iMC Platform - Server & Storage A...	Manages network resources such a...	iMC SSA 7.3 (E0703)	Deployed	Master Server
iMC Platform - VLAN Management	Manages VLAN in the network.	iMC VLAN 7.3 (E0703)	Deployed	Master Server
iMC Platform - WeChat Management	WeChat Server	iMC PLAT 7.3 (E0703)	Deployed	Master Server
Application Management	Configures and Management of app...	UCenter APM 7.3(E051...	Deployed	Master Server
Application Management Service	Collects data form various types...	UCenter APM 7.3(E051...	Deployed	Master Server
Business Service Performance	Monitors various types of services.	UCenter BSM 7.3 (E0505)	Deployed	Master Server
Network Behavior Analyzer	Provides basic configuration and...	UCenter IOM NTA/UBA ...	Deployed	Master Server
Network Behavior Analyzer Server	Receives network behavior inform...	UCenter IOM NTA/UBA ...	Deployed	Master Server
Network Traffic Analyzer	Manages and displays network tra...	UCenter IOM NTA 7.3 ...	Deployed	Master Server
Network Behavior Analyzer Server	Receives network behavior inform...	UCenter IOM NTA/UBA ...	Undeployed	
Service Health Manager - Service ...	Uses IQIs and services, together...	U-Center IOM SEM 7.3...	Deployed	Master Server
Service Health Manager - NQA Coll...	Samples and analyzes network per...	U-Center IOM SEM 7.3...	Deployed	Master Server
Application Management Service	Collects data form various types...	UCenter APM 7.3(E051...	Undeployed	
Network Traffic Analyzer Server	Collects and analyzes data from...	UCenter IOM NTA 7.3 ...	Deployed	Master Server
Network Traffic Analyzer Server	Collects and analyzes data from...	UCenter IOM NTA 7.3 ...	Undeployed	
Service Health Manager - NQA Coll...	Samples and analyzes network per...	U-Center IOM SEM 7.3...	Undeployed	

- ネットワークトラフィック分析およびネットワークトラフィック分析は、iMCメインサーバーにインストールされたNTAのインターフェースおよび構成を管理します。ネットワークトラフィック分析サービスおよびネットワークトラフィック分析サーバーは、NTA固有のビジネスロジック、ログデータ分析、集計などを管理します。分散した方法で導入できるため、パフォーマンスのロードバランスを実現

# NTA基本環境に関する注意事項



## ・環境要求事項

- ✓ PLATと同じバージョン
- ✓ 高パフォーマンスのサーバー
- ✓ 場合によっては複数サーバーの導入
- ✓ CPU/メモリー/ディスク容量などのハードウェア要因

## ・異なるシナリオ

- ✓ Netstream: 全てのデータを検査するために処理の負荷がかかります。そのため1秒あたりに処理されるログの量に配慮する必要があります
- ✓ SFlow: データをサンプリングして検査するため、データが大量である場合に有効です。考慮する点としては、どれ位の数のインタフェースにSflowを設定するかです
- ✓ DIG: DIGコレクタによって処理されるトラフィック量に配慮

# NTA基本環境に関する注意事項



比較項目	NetFlow	SFlow
データ取得方法	全データ	サンプリング
プロトコル	IPパケットのみ。ただし、v9からはMACアドレスも対象可能。	レイヤー2からレイヤー7のパケットが対象
処理の特徴	大量のトラフィックの場合、高パフォーマンスなサーバーを要求される	大量のトラフィックでもサンプリングするため効率よく処理できる
パケットの検証方法	トラフィックパターンのテンプレートを予め用意し、パターンと異なるトラフィックの発見に強い	トラフィックをサンプリングして検証するためより詳細のデータが確認できる

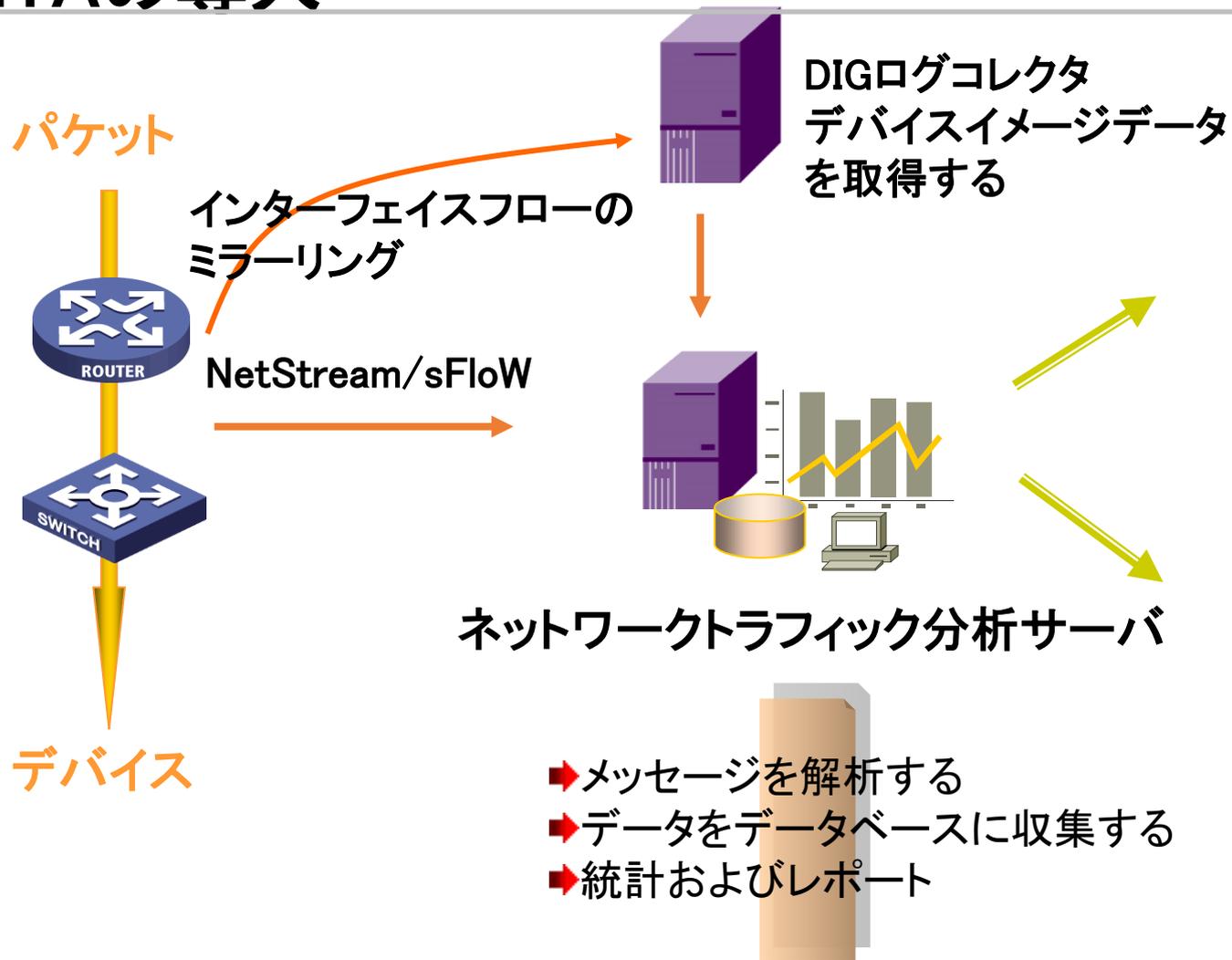
# NTAライセンス



プロジェクトコード	モデル	説明	
0231A816	SWP-IMC-NTAW-CN	functional module-H3C iMC-SW7M1NTAW-Network traffic analysis component-pure software (CD)	The NTA must be configured PLAT
3130A212	LIS-IMC-NTAA-CN-1	License-H3C iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 1 device	
3130A213	LIS-IMC-NTAB-CN-2	License-H3C iMC-SW7M1NTAB-iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 2 device	
3130A214	LIS-IMC-NTAC-CN-5	License-H3C iMC-SW7M1NTAC-iMC-SW7M1NTAA-Network traffic analysis component license fee-manage 5 device	

- iMC NTAは収集ポイント(デバイスまたはプローブ)に従ってライセンスを計算します。デフォルトでは、1つの収集ポイントライセンスが使用され、拡張は1/2/5に分割されます。  
デバイス上に複数のNetStreamボードがある場合、各NetStreamボードは収集ポイントとなります。

# NTAの導入



## 主な機能

H3Cのさまざまなルータ、スイッチ、およびポートミラーリングをサポートするすべてのネットワークデバイスと連携

NetStreamやSflowなどの複数のログフォーマットをサポート

ベースラインのインテリジェントな確立、異常なトラフィックに対する自動アラーム

P2Pアプリケーショントラフィックの監視および分析

MACおよびホスト名に基づくトラフィック監視

データベース使用スペースのリアルタイム監視

# NTAの導入



## ・管理される装置へのNetStreamのコンフィグ

ステップ	コマンド	備考
1.システムビューに入ります。	System-view	該当なし
2.NetStreamの従来のデータエクスポートの宛先アドレスと宛先UDPポート番号を設定します。	<b>ip netstream export host</b> <i>ip-address udp-port</i> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]	デフォルトでは、宛先アドレスまたは宛先UDPポート番号は設定されていません。
3.インタフェースビューに入ります。	<b>Interface</b> <i>interface-type interface-number</i>	該当なし
4.インタフェースでNetStreamを有効にします。	<b>ip netstream { inbound   outbound }</b>	デフォルトでは、NetStreamはインターフェイス上でディセーブルです。

# NTAの導入



- ・管理される装置へのNetStreamのコンフィグ

#Ten-GigabitEthernet0/1上の着信トラフィックに対してNetStreamをイネーブルにします。

```
[NS] system-view
```

```
[NS] interface Ten-GigabitEthernet0/1
```

```
[NS-Ten-GigabitEthernet0/1] ip netstream inbound
```

```
[NS-Ten-GigabitEthernet0/1] quit
```

#NetStreamデータエクスポートのホストとして、iMC NTAのIPアドレスとリスニングポートを指定します。

```
[NS] ip netstream export host 192.168.1.220 9020
```

#NetStreamデータをバージョン9形式でエクスポートするか、この手順をスキップしてデフォルトのNetStreamデータエクスポート形式バージョン5を使用します。

```
[NS] ip netstream export version 9
```

# NTAの導入

## ・管理される装置へのSFlowのコンフィグ

#sFlowエージェントのIPアドレスを90.16.0.9に設定します。

```
<3600V2> system-view
```

```
[3600V2] sflow agent ip 90.16.0.9
```

#sFlowコレクタ用に次のパラメータを設定します。

- sFlowコレクタID1。
- IPアドレス192.168.1.220。
- ポート番号6343(デフォルト)。
- 説明NTA Server。

```
[3600V2] sflow collector 1 ip 192.168.1.220 port 6343 description NTAServer
```

#イーサネット1/0/1でカウンタサンプリングをイネーブルにし、カウンタサンプリング間隔を120秒に設定します。

```
[3600V2] interface Ethernet 1/0/1
```

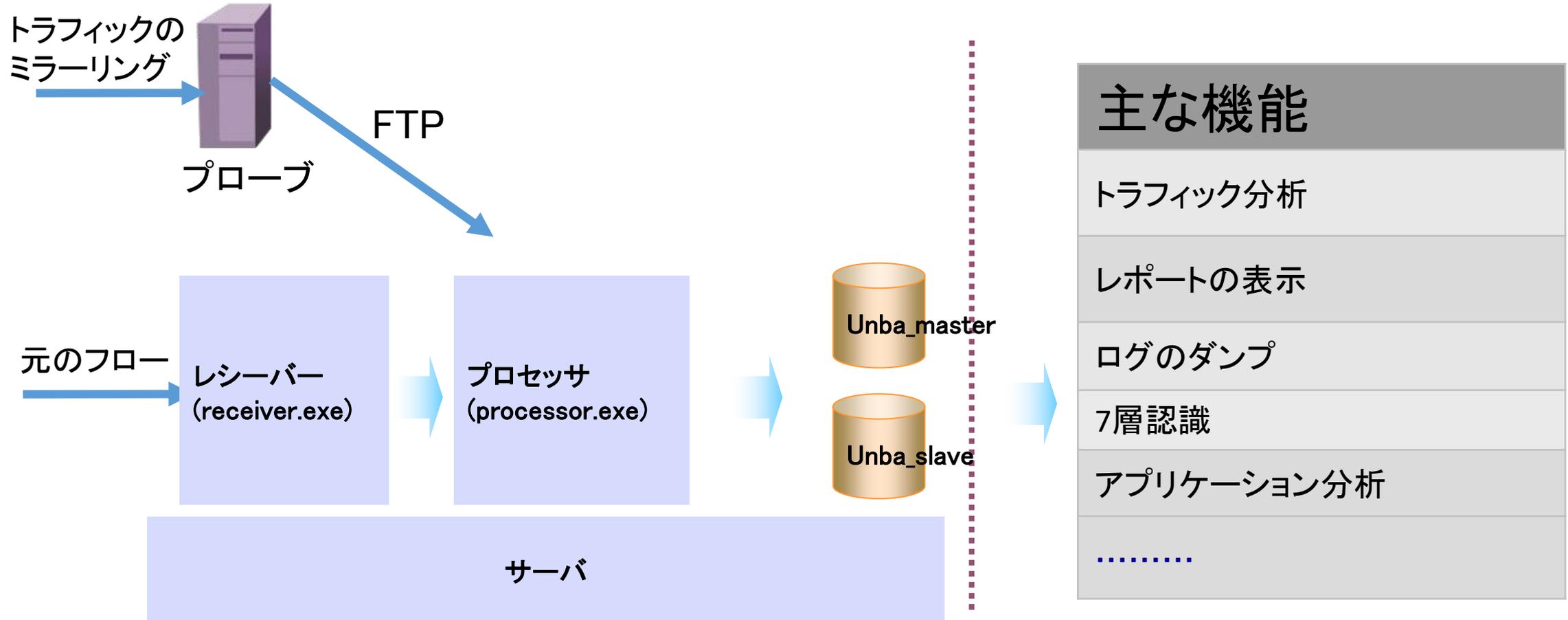
```
[3600V2-Ethernet1/0/1] sflow counter interval 120
```

#カウンタサンプリング用にsFlowコレクタ1を指定します。

```
[3600V2-Ethernet1/0/1] sflow counter collector 1
```

```
[3600V2-Ethernet1/0/1] quit
```

# NTAのシステム構造





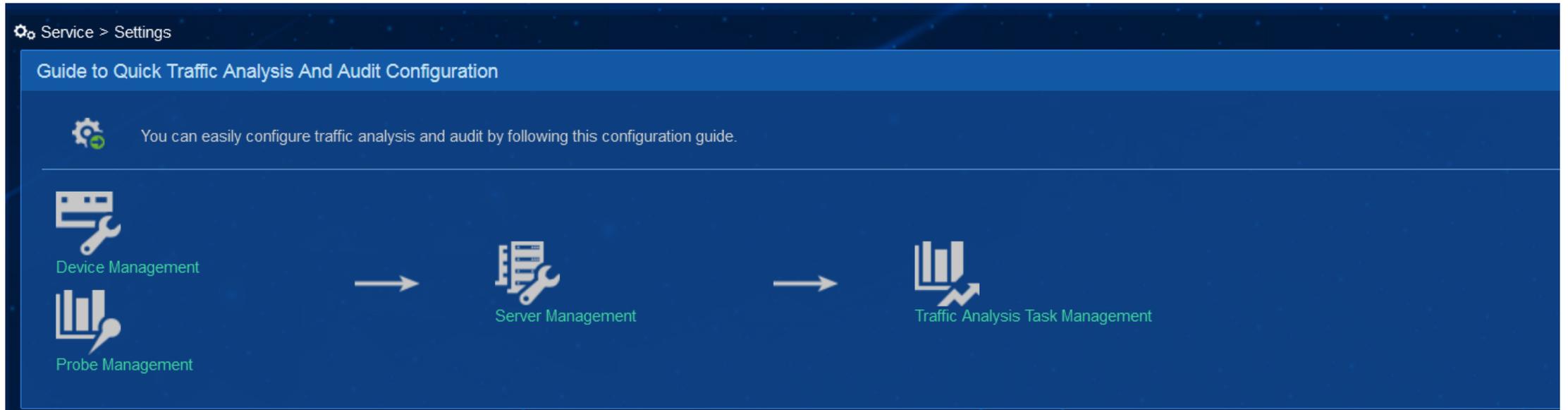
内容

NTAの特徴

NTAの設定

トラブルシューティング

- NTA構成ガイド  
デバイス管理、プローブ管理、サーバ管理、およびトラフィック分析タスク管理を含む



# NTAの設定



- デバイス管理  
トラフィック分析装置操作の追加、変更、および削除を含む

Service > Settings > Device Management Add to My Favorites Help

### Device List

Add Refresh Once the device for traffic analysis is deleted, the corresponding traffic analysis task will be terminated.

Total Items: 1.

Name	Device IP	Description	Device Resource Info	Modify	Delete
MYH	192.168.113.253				

Service > Settings > Device Management > Add Device Help

### Add Device

#### Basic Information

Device IP *	<input type="text"/>	<span>Select</span>
Name *	<input type="text"/>	
Description	<input type="text"/>	
SNMPv3	Disable	
SNMP Read-Only Community	<input type="text"/>	
SNMP Port	161	
Log Source IP	<input type="text"/>	
NetStream Statistics Identifier	Valid	
NetStream New Feature	Enable	
sFlow Settings	Disable	

# NTAの設定



- プローブ管理  
プローブ操作の追加、変更、および削除を含む

The image shows two screenshots of the NTA configuration interface. The left screenshot shows the 'Service > Settings' page with a navigation menu where 'Probe Management' is highlighted with a red box. The right screenshot shows the 'Service > Settings > Probe Management > Add Probe' page, which contains a form for adding a new probe.

**Service > Settings**

Guide to Quick Traffic Analysis And Audit Configuration

You can easily configure traffic analysis and audit by following this configuration guide.

Device Management → Server Management

**Probe Management**

**Service > Settings > Probe Management > Add Probe**

**Add Probe**

**Basic Information**

Name *	<input type="text"/>
IP *	<input type="text"/> ?
Description	<input type="text"/>
Enable Layer 7 Application	No
Identification	<input type="text"/>
Probe Password	<input type="password"/>
Analysis Network Card	Disable

# NTAの設定



- サーバ管理

サーバ設定とは、配置されたネットワークトラフィック分析サーバコンポーネントに関連する情報の設定を指します。

サーバの設定が完了したら、新しい設定を受信側、プロセッサ側、およびプロブ側で有効にする前に、設定を配信する必要があります。

Service > Settings > Server Management

★ Add to My Favorites ? Help

Server List

Refresh

Total Items: 1.

Server Name	Server IP	Description	Capture Flux Log	Deploy Configuration	Modify
127.0.0.1	127.0.0.1				

# NTAの構成(サーバー管理)



Service > Settings > Server Management > Server Configuration

### Server Configuration

**Basic Information**

Server Name \*  
Server Description  
Server IP \*  
Listening Port \*  
FTP Main Directory  
FTP Username  
FTP Password  
Traffic Analysis Log Aggregation Policy  
Filter Policy  
Usage Threshold of the Database Disk (1-95%) \*  
When Database Disk Usage Reaches Threshold

**Traffic Analysis**

TCP Respons Delay

**Device Information**

Select	Device Name	Device IP	Device Description
<input checked="" type="checkbox"/>	MYH	192.168.113.253	

**Probe Information**

Select	Probe Name	Probe IP	Name	Analysis Network Card	Enable Layer 7 Ap
No match found.					

127.0.0.1  
127.0.0.1  
3000,9021,8343  
Aggregation (Rough Granularity)  
Not Filter  
80  
Stop Receiving Logs  
Disable ?

コレクタの監視を選択します。FTP情報を構成する必要があります。

ネットワークトラフィック解析装置を選択する

Deploy Cancel

# NTAの構成(サーバー管理)

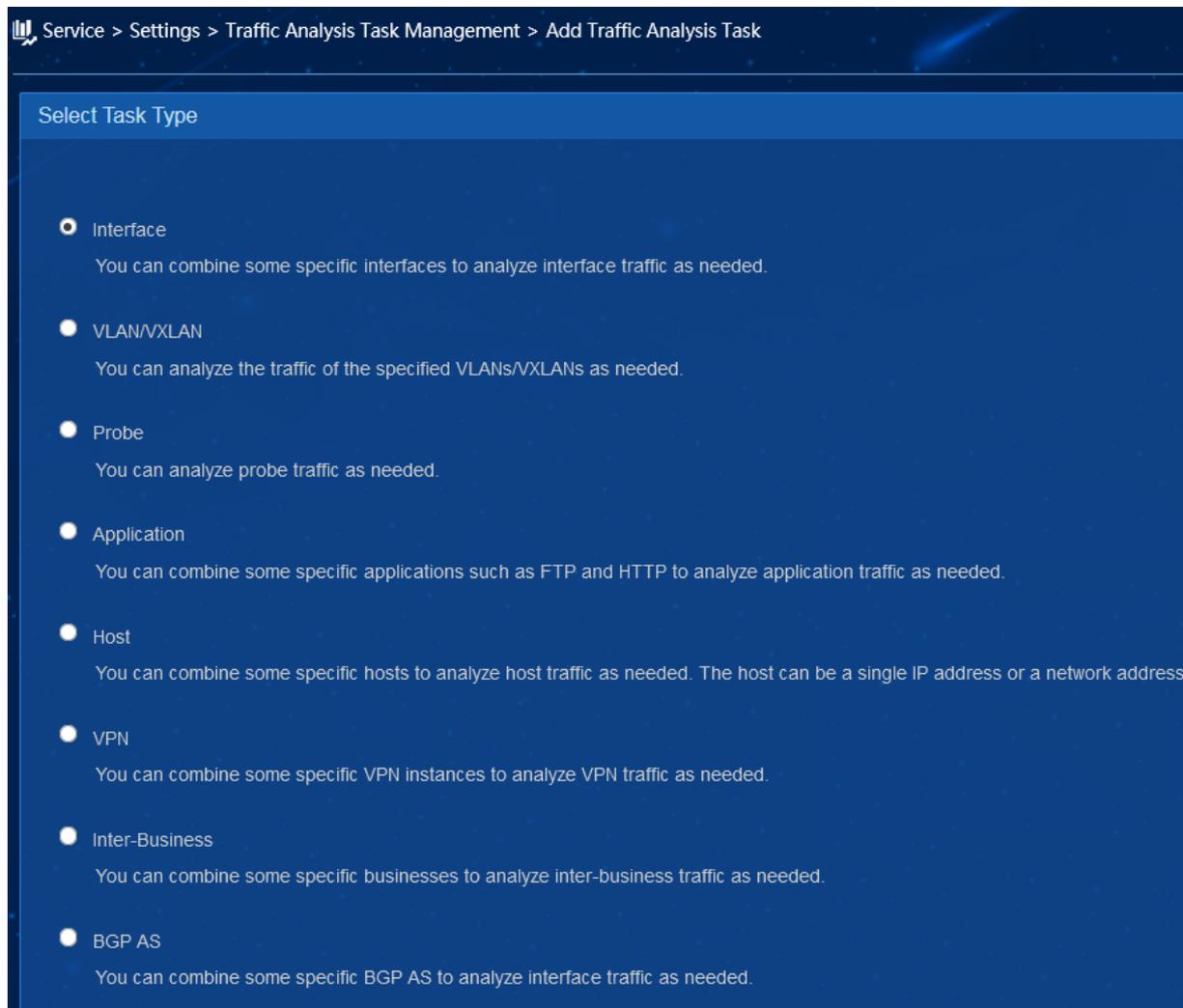


## ● トラフィック分析タスク

NTAコンポーネントは、複数の次元からネットワークトラフィックを分析できます。

- ✓ インターフェイスベースのトラフィック分析
- ✓ VLANベースのトラフィック分析
- ✓ プロブベースのトラフィック分析
- ✓ アプリケーションベースのトラフィック分析
- ✓ ホストベースのトラフィック分析
- ✓ VPNベースのトラフィック分析
- ✓ BGP-ASベースのトラフィック分析

.....



# トラフィック分析タスクインターフェイス



Service > Settings > Traffic Analysis Task Management > Add Traffic Analysis Task

### Add Traffic Analysis Task

**Basic Information**

Task Name

Task Description

Server \*

Task Type

Reader

Vlan Analysis

**Interface Information**

Interface Description	Interface Alias	Interface Index	Interface IP	Max Rate	Device Name	Device IP
No records found.						

タスクに関連付けられたネットワーク・ストリーム・サーバー。つまり、タスクはサーバー間を移動できません。

# トラフィック分析タスク:ホスト



Service > Settings > Traffic Analysis Task Management > Add Traffic Analysis Task ? Help

### Add Traffic Analysis Task

**Basic Information**

Task Name *	<input type="text"/>
Task Description	<input type="text"/>
Server *	127.0.0.1
Task Type	Host
Reader	<input type="text"/>

**Host Information**

IP Stat. Direction *	Include
Host IP	<input type="text"/>
Host IP List	<input type="text"/>
Application List	<input type="text"/>

Task collects traffic logs for analysis according to the specified interface or probe information. If the interface and probe information is not specified, the task collects traffic logs from all interfaces and probes for analysis.

**Interface Information**

各ホストトラフィック分析タスクは、最大10のホスト定義をサポートします。

各ホスト・トラフィック分析タスクは最大10個のアプリケーションをサポート

# トラフィック分析タスク:VPN



Service > Settings > Traffic Analysis Task Management > Add Traffic Analysis Task

### Add Traffic Analysis Task

**Basic Information**

Task Name \*

Task Description

Server \* 127.0.0.1

Task Type VPN

Reader

**VPN Instance List**

Device Name	Device IP	Modify	Delete
No records found.			

VPN Instance Set

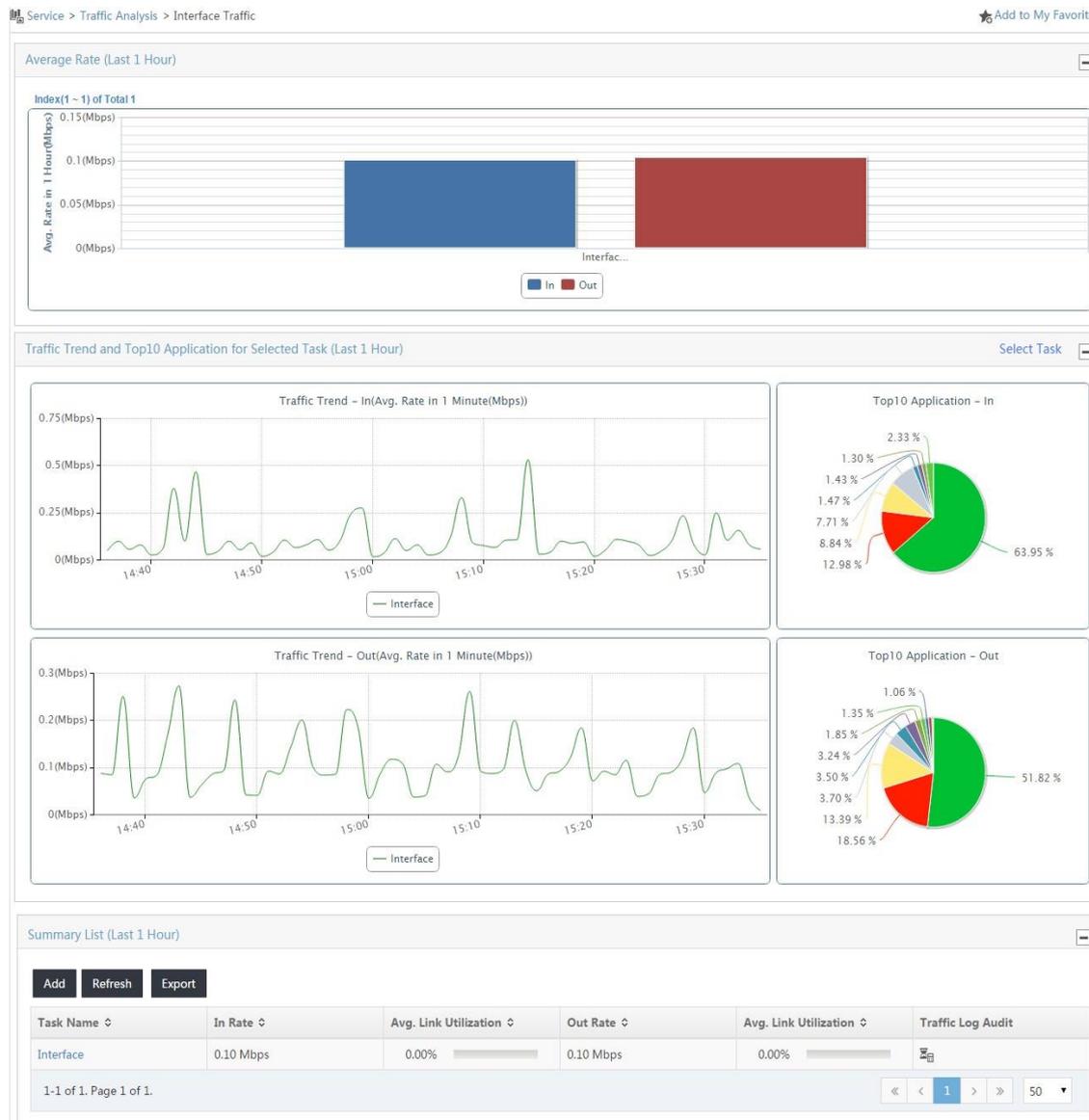
Device Name MYH(192.168.113.253)

VPN ID(1-65535) \*

Description

```
<Sysname> display ip vpn-instance instance-name vpnl  
VPN-Instance Name and ID : vpnl, 2  
Create time : 2006/04/08 13:01:30  
Up time : 0 days, 00 hours, 11 minutes and 42 seconds
```

# トラフィック分析タスクの情報



NetStream: インターフェイストラフィック分析  
タスクの概要情報

Service>Traffic Analysis>Interface Traffic

# トラフィック分析タスクの情報表示



## NetStream: インターフェイストラフィック分析タスクのトラフィック情報 Service>Traffic Analysis>Interface Traffic>Interface

Service > Traffic Analysis > Interface Traffic > Interface

Refresh Interval No Refresh ? Help

Traffic **Application** Source Destination Session Export Previous Next Last 1 hour Search

Traffic Trend



Direction	Total Traffic	Max. Avg Rate	Min. Avg Rate	Avg. Rate	Avg. Link Utilization	Max. Link Utilization
In	45.71 MB	0.53 Mbps	15.38 Kbps	0.11 Mbps	0.00%	0.01%
Out	44.96 MB	0.27 Mbps	34.29 Kbps	0.10 Mbps	0.00%	0.00%

Flux Distribute In Interface

Interface flux report

Index(1 ~ 6) of Total 6



# トラフィック分析タスクの情報表示



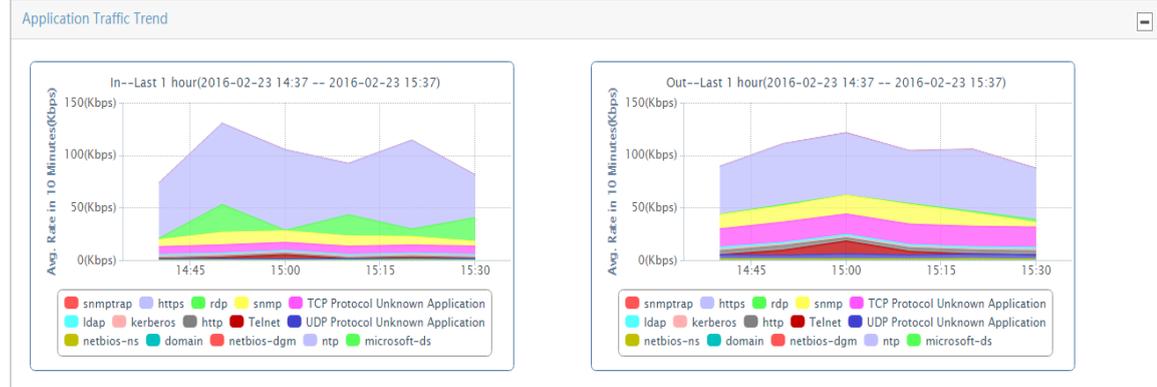
Service > Traffic Analysis > Interface Traffic > Interface

Refresh Interval No Refresh Help

Application	Unknown Applications	In Traffic	In Speed	Out Traffic	Out Speed
snmptrap		0.00 B	0.00 bps	51.93 KB	0.12 Kbps
https		27.30 MB	63.62 Kbps	22.95 MB	53.47 Kbps
rdp		5.54 MB	12.91 Kbps	0.47 MB	1.09 Kbps
snmp		3.77 MB	8.79 Kbps	5.93 MB	13.82 Kbps
TCP Protocol Unknown Application	?	3.29 MB	7.67 Kbps	8.22 MB	19.15 Kbps
ldap		0.63 MB	1.46 Kbps	0.82 MB	1.91 Kbps
kerberos		0.61 MB	1.42 Kbps	0.60 MB	1.39 Kbps
http		0.55 MB	1.29 Kbps	1.55 MB	3.61 Kbps
Telnet		0.42 MB	0.97 Kbps	1.44 MB	3.35 Kbps
UDP Protocol Unknown Application	?	0.37 MB	0.85 Kbps	1.64 MB	3.81 Kbps
netbios-ns		0.12 MB	0.28 Kbps	0.47 MB	1.08 Kbps
domain		81.30 KB	0.18 Kbps	0.10 MB	0.24 Kbps
netbios-dgm		8.76 KB	19.93 bps	66.26 KB	0.15 Kbps
ntp		4.16 KB	9.46 bps	0.00 B	0.00 bps
microsoft-ds		0.43 KB	0.98 bps	0.52 KB	1.17 bps

1-15 of 15. Page 1 of 1.

NetStream: インターフェイストラフィック分析タスクのアプリケーション情報  
Service>Traffic Analysis>Interface Traffic>Interface



# トラフィック分析タスクの情報表示



## NetStream: インターフェイストラフィック分析タスクのセッション情報 Service>Traffice Analysis>Interface Traffic>Interface

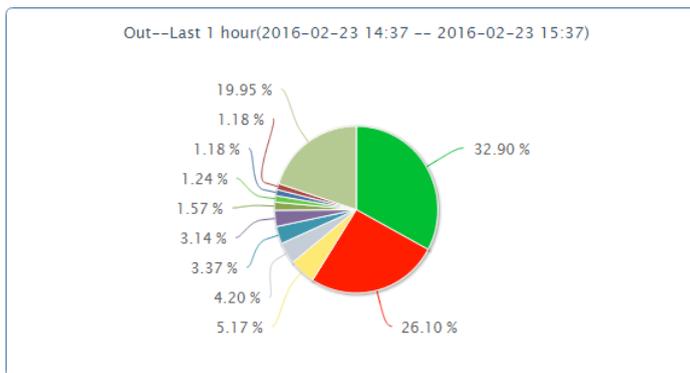
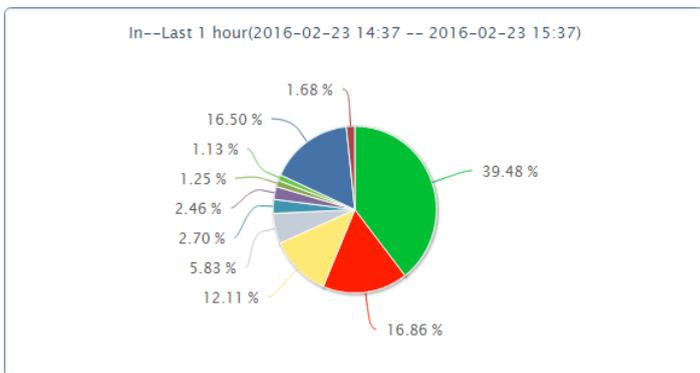
Service > Traffic Analysis > Interface Traffic > Interface

Refresh Interval No Refresh [? Help](#)

Traffic Application Source Destination Session

Export Previous Next Last 1 hour

### Top 10 Traffic Report for Session Host



### Top 10 Traffic List for Session Host

In

Generate Chart

Out

Generate Chart

Source Host	Destination Host	Traffic	Percentage	Details	Topology	Source Host	Destination Host	Traffic	Percentage	Details	Topology
192.168.40.118	192.168.40.170	18.05 MB	39.48%			192.168.40.22	192.168.40.118	14.82 MB	32.90%		
192.168.40.118	192.168.1.135	7.71 MB	16.86%			192.168.40.170	192.168.40.118	11.76 MB	26.10%		
192.168.40.165	192.168.30.250	5.54 MB	12.11%			192.168.1.135	192.168.40.118	2.33 MB	5.17%		
192.168.40.198	192.168.40.170	2.66 MB	5.83%			192.168.40.170	192.168.40.198	1.89 MB	4.20%		
192.168.40.21	10.153.0.114	1.23 MB	2.70%			192.168.30.250	192.168.40.130	1.52 MB	3.37%		

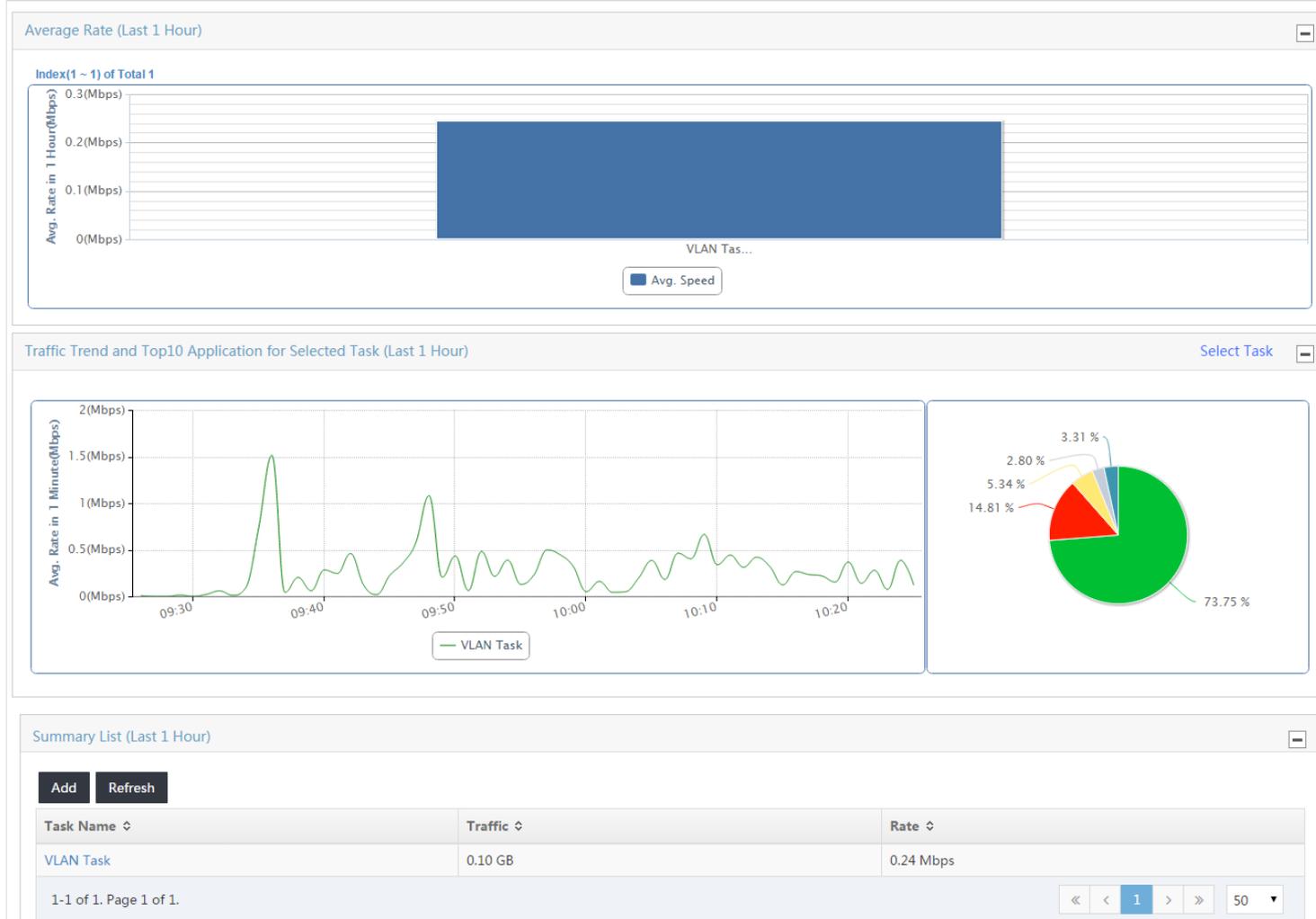
# トラフィック分析タスクの情報表示



## Sflow:VLANトラフィックタスクに関するサマリー情報の表示 Service>Traffic Analysis>VLAN/VXLAN Traffic Analysis

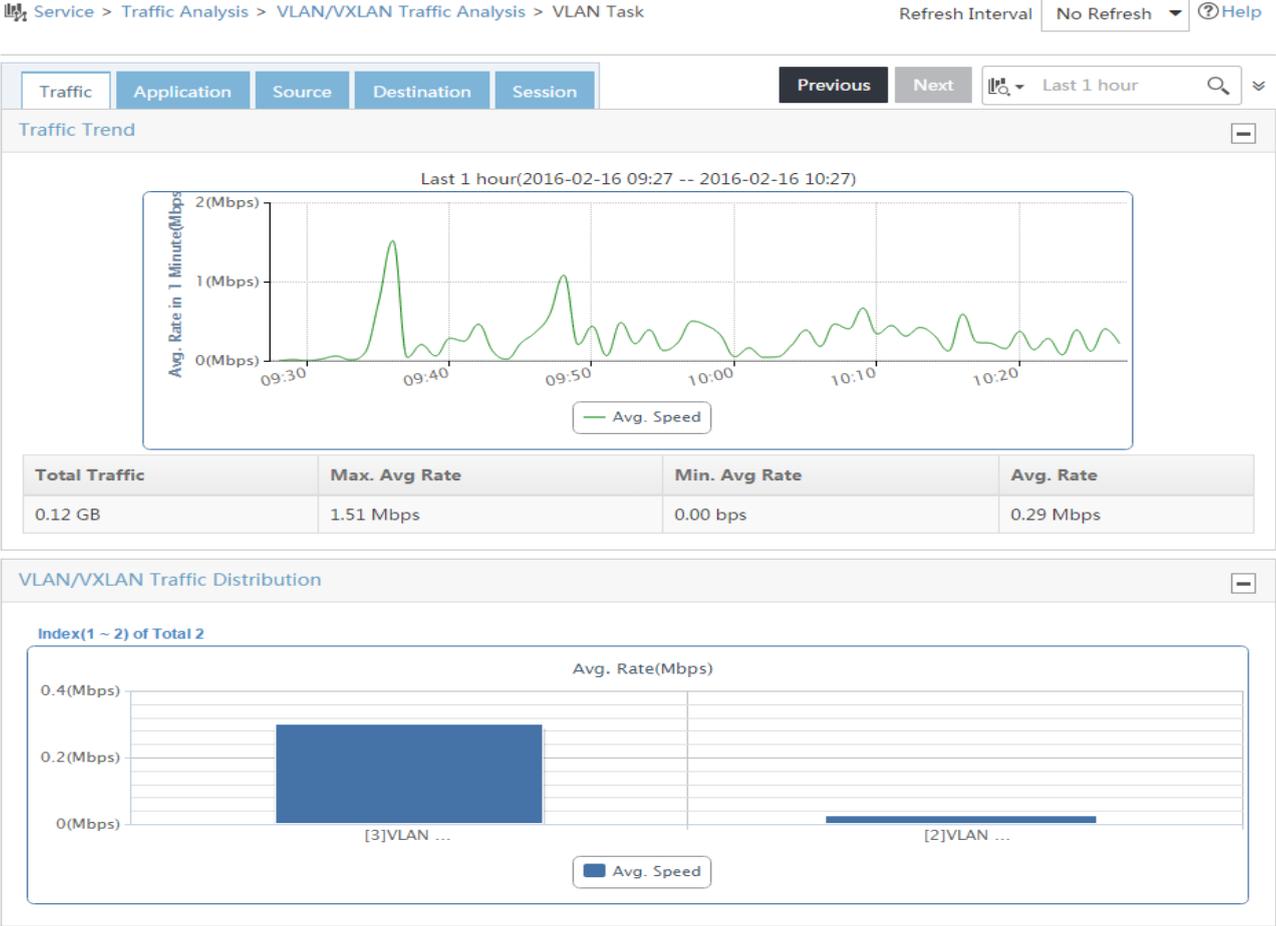
Service > Traffic Analysis > VLAN/VXLAN Traffic Analysis

[★ Add to My Favorites](#)



# トラフィック分析タスクの情報表示

Sflow: VLANトラフィック分析タスクのトラフィック情報の表示  
Service>Traffic Analysis>VLAN/VXLAN Traffic Analysis>VLAN Task



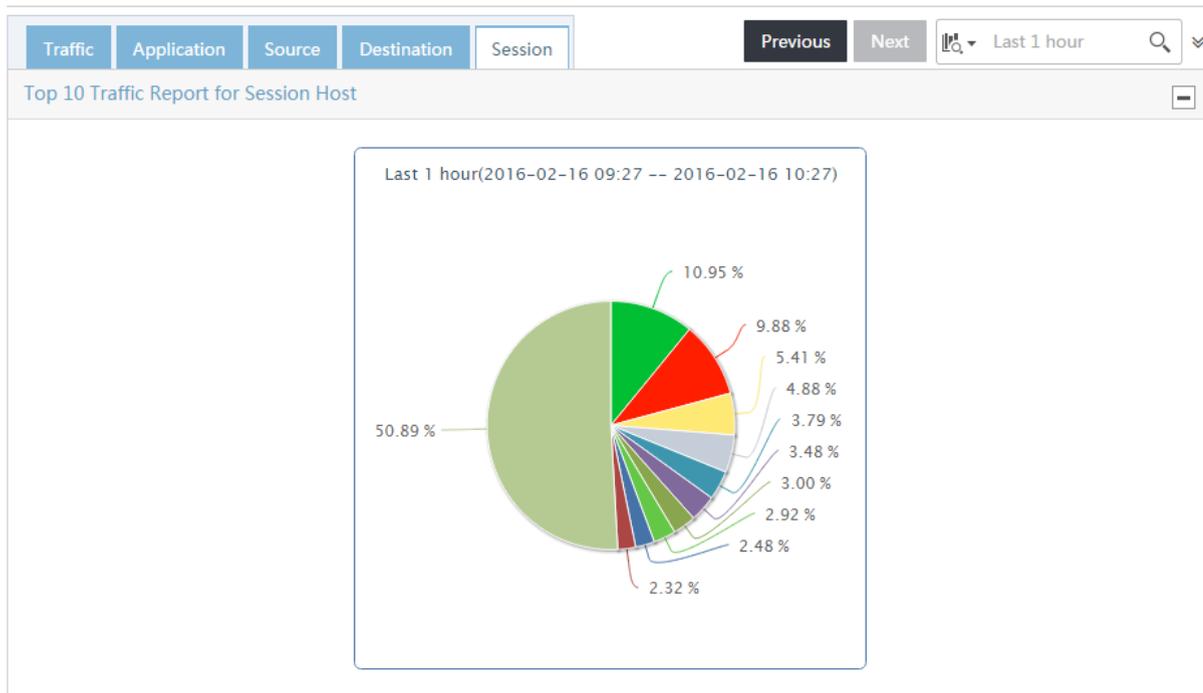


# トラフィック分析タスクの情報表示



Service > Traffic Analysis > VLAN/VXLAN Traffic Analysis > VLAN Task

Refresh Interval No Refresh Help



Top 10 Traffic List for Session Host Generate Chart

Source Host	Destination Host	Traffic	Percentage	Details	Topology
192.168.40.238	192.168.30.25	13.53 MB	10.95%		
192.168.40.238	192.168.30.235	12.20 MB	9.88%		
192.168.40.239	192.168.30.25	6.69 MB	5.41%		
192.168.40.239	192.168.30.235	6.03 MB	4.88%		

Sflow: VLANトラフィック分析タスクのセッション  
トラフィック情報の表示

Service>Traffic Analysis>VLAN/VXLAN  
Traffic Analysis>VLAN Task

# トラフィック分析タスクの情報表示



## NetStream: UBA監査結果のログ Service>User Behavior Audit

Service > User Behavior Audit

Help

Audit Condition (Note: If plenty of logs exist, it may take several minutes or longer time to query logs.)

Audit Result:2016-02-23 15:30:26-2016-02-23 15:42:50

Custom

Continue

Group

Not Group

Start Time	Source	Destination	Source Port	Destination Port	Protocol	Application	Packets Count	Flux	Device
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51486	TCP	https	7	3.43 KB	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	7	4.84 KB	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51482	TCP	https	1	40.00 B	90.16.0.240
2016-02-23 15:4...	192.168.40.118	192.168.1.135	443	51483	TCP	https	7	2.29 KB	90.16.0.240

1-8 of 10000. Page 1 of 1250.

Navigation: << < 1 2 3 4 5 6 7 8 9 10 > >> 8

Save



内容

NTAの特徴

NTAの設定

トラブルシューティング

- ・トラフィックなしの場合、以下を確認する
  - ✓ インテリジェント管理センター(iMC)とSQL Serverが正常に動作しているかどうか
  - ✓ tbl\_nets\_yymmddhhにテーブルがある場合は、SQL Serverのunba\_slaveデータベース  
このようなテーブルが存在しない場合、データは保存されていません。
  - ✓ デバイスがログを送信するかどうか、および送信先がNTAスレーブサーバーかどうか
  - ✓ プローブネットワークモードで、プローブがミラーログメッセージを受信するかどうか
  - ✓ サービス構成内のFTPディレクトリが正しく構成されているかどうか、およびFTPサーバーが起動しているかどうか
  - ✓ デバイスの時間帯設定に一貫性があるかどうか、デバイスのIPが正しく設定されているかどうか、およびインターフェイスインデックスに一貫性があるかどうか
  - ✓ スレーブサーバーに複数のネットワークカードがある場合は、NTA内のスレーブサーバーのIPアドレスが、監視トラフィックが通過するIPアドレスであるかどうかを確認します。



ありがとう

[www.h3c.com](http://www.h3c.com)