

H3C IMC NTA/UBA NetStreamの設定例

ソフトウェアバージョン:IMC NTA7.3(E0503)

Copyright(C)2013-2017New H3C Technologies Co.,Ltd.All rights reserved.このマニュアルのいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしに、いかなる形式または手段によっても複製または転送することはできません。

本ドキュメントの情報は、予告なく変更されることがあります。

The H3C logo is displayed in a bold, red, sans-serif font. The '3' is stylized with a horizontal bar through it.

内容

はじめに	3
前提条件	3
制限事項およびガイドライン	3
例:NetStreamを介したトラフィックモニタリングにNTA/UBAを使用する.....	3
ネットワーク構成.....	3
手順.....	4
IPアドレスおよびインターフェース情報の表示.....	4
NTA/UBAの構成.....	5
ルーターでのNetStreamの設定.....	7
インターフェーストラフィック情報の表示.....	7
ユーザーの動作の監査.....	10
NTA/UBAおよびNetStreamのトラブルシューティング	11
NTA/UBAサーバーでNetStreamデータを受信しませんでした。.....	11
NTA上にNetStreamデータがありません	11
UBAの監査結果がない.....	12

はじめに

このドキュメントでは、NTA/UBAを使用してデバイス上のネットワークトラフィックをNetStreamを介してリアルタイムで監視する例を示します。

前提条件

ネットワークトラフィックを監視するようにNTA/UBAおよびNetStreamを設定する前に、次の設定を完了します。

- デバイスがNTA/UBA A/UBAサーバーと通信できることを確認します。
- デバイス上でNetStreamを有効にして、NTA/UBAサーバーがデバイスからNetStreamデータを受信できるようにします。
- デバイスおよびNTA/UBAサーバーの基本パラメータを構成します。

制限事項およびガイドライン

NTA/UBA NetStreamを設定する場合は、次の制約事項およびガイドラインに従ってください。

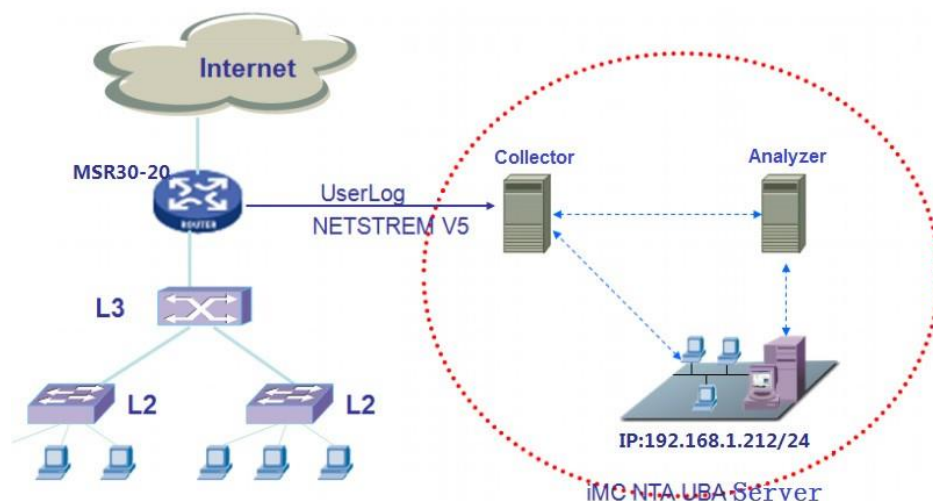
- NTAでは、次のログタイプがサポートされています
 - IPFIX
 - NetFlow v5
 - NetFlow v9(v5およびCisco Flexible NBAR)
 - NetStream v5
 - NetStream v9(H3C VPN、IPv4、およびIPv6)
 - sFlow v5
- UBAでは、次のログタイプがサポートされています。
 - Flow 1.0
 - Flow 3.0
 - IPFIX
 - NAT1.0
 - NetFlow v5
 - NetFlow v9(v5およびCisco Flexible NBAR)
 - NetStream v5
 - NetStream v9(IPv4およびIPv6)

例:NetStreamを介したトラフィックモニタリングにNTA/UBAを使用する

ネットワーク構成

図1に示すように、NetStream経由のネットワークトラフィックを分析および監視するようにNTA/UBAを構成します。

図1 ネットワーク図



手順

IPアドレスおよびインタフェース情報の表示

1. NTA/UBAサーバーのIPアドレスを識別します。
NTA/UBAサーバーのIPアドレスは192.168.1.212/24です。
2. MSR30-20ルーターの管理IPアドレスを識別します。MSR30-20ルーターのIPアドレスは90.16.0.240/24です。
3. インタフェース情報の表示:
 - a. Resourceタブをクリックします。
 - b. 左側のナビゲーションツリーから、**Resource Management > Add Device**を選択します。
 - c. 開いたページで、**Host Name/IP**にIPアドレスを入力します。
 - d. デバイス上と同じ**SNMP**、Telnet、およびSSH設定を構成します。
 - e. **OK**をクリックします。
 - f. デバイスが正常に追加されたことを示すページで、**Device Details**リンクをクリックします。
Device Detailsページが開きます。
 - g. 図2に示すように、**Interface List**リンクをクリックすると、**Interface List**ページが開きます。

図2 Interface Listページ

Resource > MSR30-20(90.16.0.240) > Interface List Help

<input type="checkbox"/>	Interface Status	Interface Description	Interface Alias	Last Change	Media Type	Interface IP	Up/Down Alarm	Interface Link Type
<input type="checkbox"/>	Down	Aux0	Aux0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface
<input type="checkbox"/>	Down	Cellular0/0	Cellular0/0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface
<input type="checkbox"/>	Down	Vlan-interface1	Vlan-interface1 Inte...	2016-02-15 09:06:30	Other	1.1.1.1	System Settings	Idle Interface
<input type="checkbox"/>	Down	Vlan-interface300	Vlan-interface300 L...	2016-02-15 09:06:30	Other		System Settings	Idle Interface
<input type="checkbox"/>	Up	Ethernet5/0	Ethernet5/0 Interface	2016-02-15 09:06:40	Electrical	10.1.1.1	System Settings	SNMP Device-connected ...
<input type="checkbox"/>	Up	Ethernet7/0	Ethernet7/0 Interface	2016-02-15 09:06:40	Electrical	10.1.2.1	System Settings	SNMP Device-connected ...
<input type="checkbox"/>	Up	GigabitEthernet8/0	GigabitEthernet8/0 ...	2016-02-15 09:06:40	Electrical	172.9.0.6	System Settings	Idle Interface
<input type="checkbox"/>	Up	GigabitEthernet8/1	GigabitEthernet8/1 ...	2016-02-15 09:06:40	Electrical	172.8.8.114	System Settings	SNMP Device-connected ...
<input type="checkbox"/>	Up	GigabitEthernet0/0	GigabitEthernet0/0 ...	2016-02-15 09:06:40	Electrical	90.16.0.240	System Settings	SNMP Device-connected ...
<input type="checkbox"/>	Up	GigabitEthernet0/1	GigabitEthernet0/1 ...	2016-02-15 09:06:40	Electrical	172.10.0.10	System Settings	SNMP Device-connected ...
<input type="checkbox"/>	Up	NULL0	NULL0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface

1-11 of 11. Page 1 of 1. 1 50

Data Captured at: 2016-02-22 17:16:53

NTA/UBAの構成

MSR30-20ルーターの追加

1. **Service**タブをクリックします。
2. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Settings**を選択します。**Settings**ページが開きます。
3. **Guide to Quick Traffic Analysis And Audit Management**領域で、**Device Management**をクリックします。
Device Managementページが開きます。
4. **Add**をクリックします。
Add Deviceページが開きます。
5. 図3に示すように、ルーターのパラメータを設定し、OKをクリックします。

図3 デバイスの追加


Service > Settings > Device Management > Add Device Help

Add Device

Basic Information

Device IP *	<input type="text" value="90.16.0.240"/>	<input type="button" value="Select"/>
Name *	<input type="text" value="MSR30-20"/>	
Description	<input type="text"/>	
SNMP Community	<input type="text" value="*****"/>	
SNMP Port	<input type="text" value="161"/>	
Log Source IP	<input type="text"/>	
NetStream Statistics Identifier	<input type="text" value="Valid"/>	▼
NetStream New Feature	<input type="text" value="Enable"/>	▼
sFlow Settings	<input type="text" value="Disable"/>	▼

サーバー構成のデプロイ

1. **Service**タブをクリックします。
2. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Settings**を選択します。**Settings**ページが開きます。
3. **Guide to Quick Traffic Analysis And Audit Management**領域で、**Server Management**をクリックします。
Server Listページが開きます。
4. 構成を配布する、NTA/UBAサーバーの **Modify**  アイコンをクリックします。**Server Configuration**ページが表示されます。
5. 図4に示すように、必要に応じてNTA/UBAサーバーパラメータを構成します。
 - a. NTA/UBAサーバー上のFTP設定と同じFTPメインディレクトリ、ユーザー名およびパスワードを構成します。
 - b. [Traffic Analysis]および[User Behavior Audit]領域でMSR30-20ルーターを選択します。

c. デバイスのイントラネットモニタ情報を設定します。

6. Deployをクリックします。

図4 サーバーの構成

Service > Settings > Server Management > Server Configuration Help

Server Configuration

Basic Information

Server Name *	127.0.0.1
Server Description	
Server IP *	127.0.0.1
Listening Port *	9020,9021,6343
FTP Main Directory	
FTP Username	
FTP Password	
Traffic Analysis Log Aggregation Policy	Aggregation (Rough Granulari
Filter Policy	Not Filter
Usage Threshold of the Database Disk (1-95%) *	90
When Database Disk Usage Reaches Threshold	Stop Receiving Logs

Traffic Analysis

Device Information

Select	Device Name	Device IP	Device Description
<input checked="" type="checkbox"/>	MSR30-20	90.16.0.240	

Probe Information

Select	Probe Name	Probe IP	Enable Layer 7 Application Identific
No match found.			

User Behavior Audit

Device Information

Select	Device Name	Device IP	Device Description
<input checked="" type="checkbox"/>	MSR30-20	90.16.0.240	

Probe Information

Select	Probe Name	Probe IP	Enable Layer 7 Application I	Enable Special Audit
No match found.				

Intranet Monitor Information

Intranet Information	<input type="text"/>	?	Add
Intranet Information		Delete	
192.168.0.0/16			

Deploy **Cancel**

インターフェイストラフィック分析タスクの追加

1. **Service**タブをクリックします。
2. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Settings**を選択します。**Settings**ページが開きます。
3. **Guide to Quick Traffic Analysis And Audit Management**領域で、**Traffic Analysis Task Management**をクリックします。**Traffic Analysis Task Management** ページが開きます。
4. **Add**をクリックします。**Select task Type**ページが開きます。
5. **Interface**を選択し、**Next**をクリックします。**Add Traffic Analysis Task**ページが開きます。

- 図5に示すように、基本タスク情報を構成し、インタフェースを選択してOKをクリックします。この例では、タスク名としてInterfaceを使用しています。

図5 インターフェイストラフィック分析タスクの追加

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

Add Traffic Analysis Task

Basic Information

Task Name:

Task Description:

Server:

Task Type:

Reader:

Vlan Analysis:

Interface Information

There are 6 records

Interface Description	Interface Alias	Interface Index	Interface IP	Max Rate	Device Name	Device IP	Modify	Delete
GigabitEthernet8/0	GigabitEthernet8/0 Interface	7	172.9.0.6	0.10 Gbps	MSR30-20	90.16.0.240		
GigabitEthernet8/1	GigabitEthernet8/1 Interface	8	172.8.8.114	0.10 Gbps	MSR30-20	90.16.0.240		
GigabitEthernet0/1	GigabitEthernet0/1 Interface	10	172.10.0.10	0.10 Gbps	MSR30-20	90.16.0.240		
Ethernet7/0	Ethernet7/0 Interface	6	10.1.2.1	0.10 Gbps	MSR30-20	90.16.0.240		
Ethernet5/0	Ethernet5/0 Interface	5	10.1.1.1	0.10 Gbps	MSR30-20	90.16.0.240		
GigabitEthernet0/0	GigabitEthernet0/0 Interface	9	90.16.0.240	1.00 Gbps	MSR30-20	90.16.0.240		

ルーターでのNetStreamの設定

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。	ip netstream export host ip-address udp-port [vpn-instance vpn-instance-name]	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・ビューを入力します。	Interface interface-type interface-number	該当なし
4. インタフェースでNetStreamを有効にします。	Ip netstream { inbound outbound }	デフォルトでは、NetStreamはインタフェース上でディセーブルです。

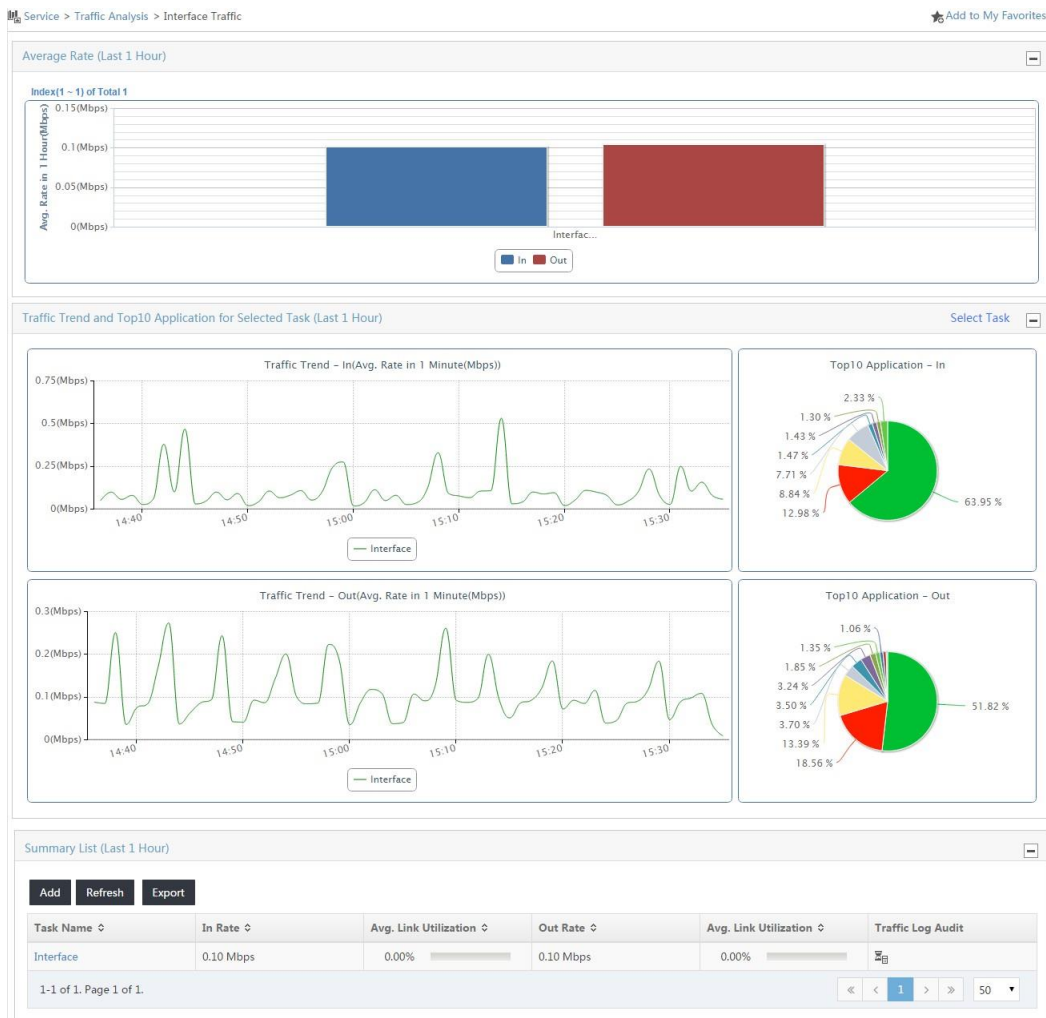
インターフェイストラフィック情報の表示

インターフェイストラフィック分析タスクのサマリー情報の表示

- Serviceタブをクリックします。
- 左側のナビゲーションツリーで、Traffic Analysis and Audit>Interface Traffic Analysis Taskを選択します。

図6に示すように、Interface Trafficページが開きます。

図6 インターフェイストラフィック分析タスクの概要情報

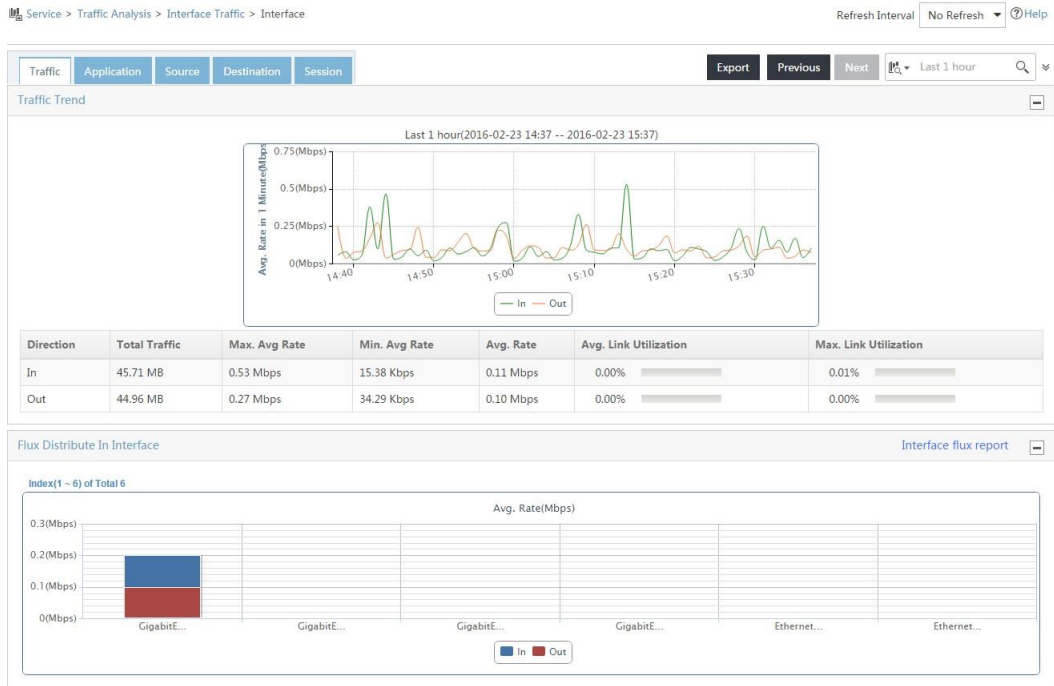


インターフェイストラフィック分析タスクのトラフィック情報の表示

1. **Service**タブをクリックします。
2. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Interface Traffic Analysis Task**を選択します。
Interface Trafficページが開きます。
3. 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を表示するには、次のいずれかを実行します。
 - **Summary List**で、表示するインターフェイストラフィック分析タスクの名前をクリックします。
 - 左側のナビゲーションツリーで、**Interface Traffic Analysis Task**の横にある**Expand**アイコンの上にマウスを置き、表示されたメニューで**Interface**をクリックします。

Interface traffic analysisページが開き、図7に示すように、インターフェイストラフィック分析タスクの合計トラフィック情報が表示されます。

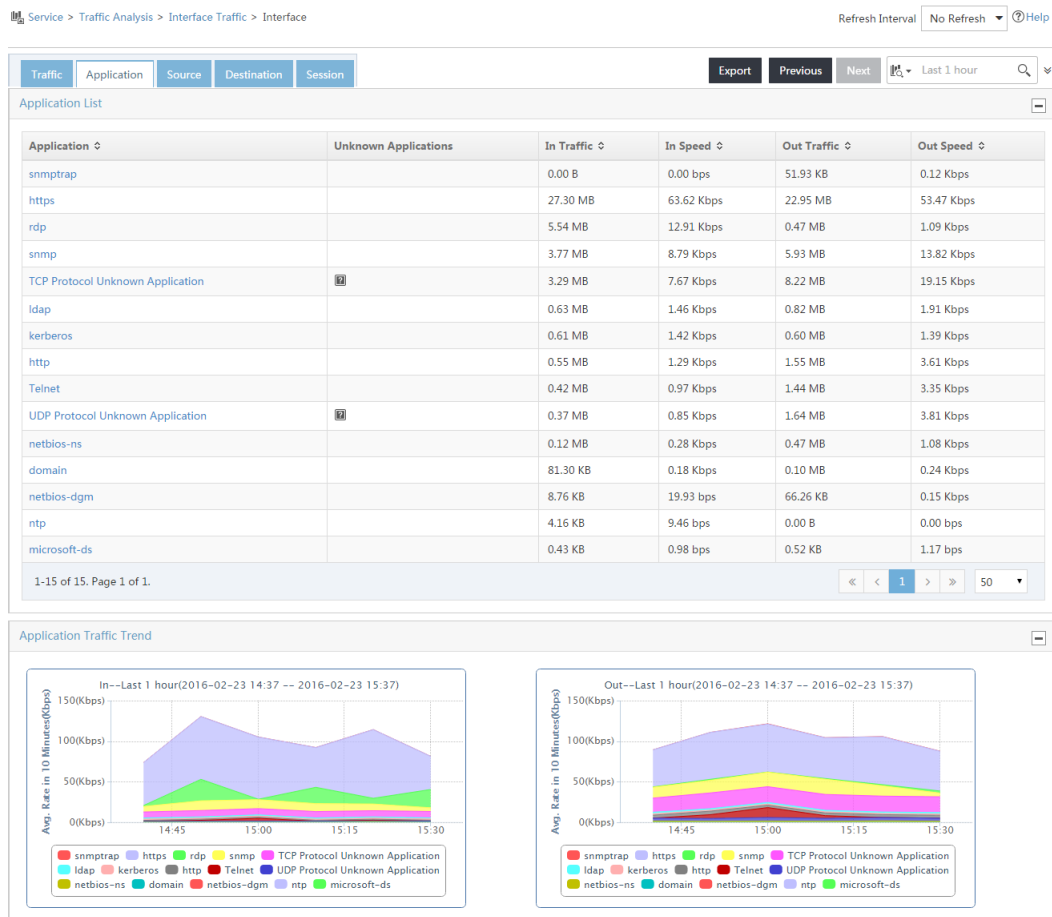
図7 インターフェイストラフィック分析タスクのトラフィック情報



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の表示

Interface traffic analysisページで、Applicationタブをクリックします。このタブには、図8に示すように、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トラフィック情報が表示されます。

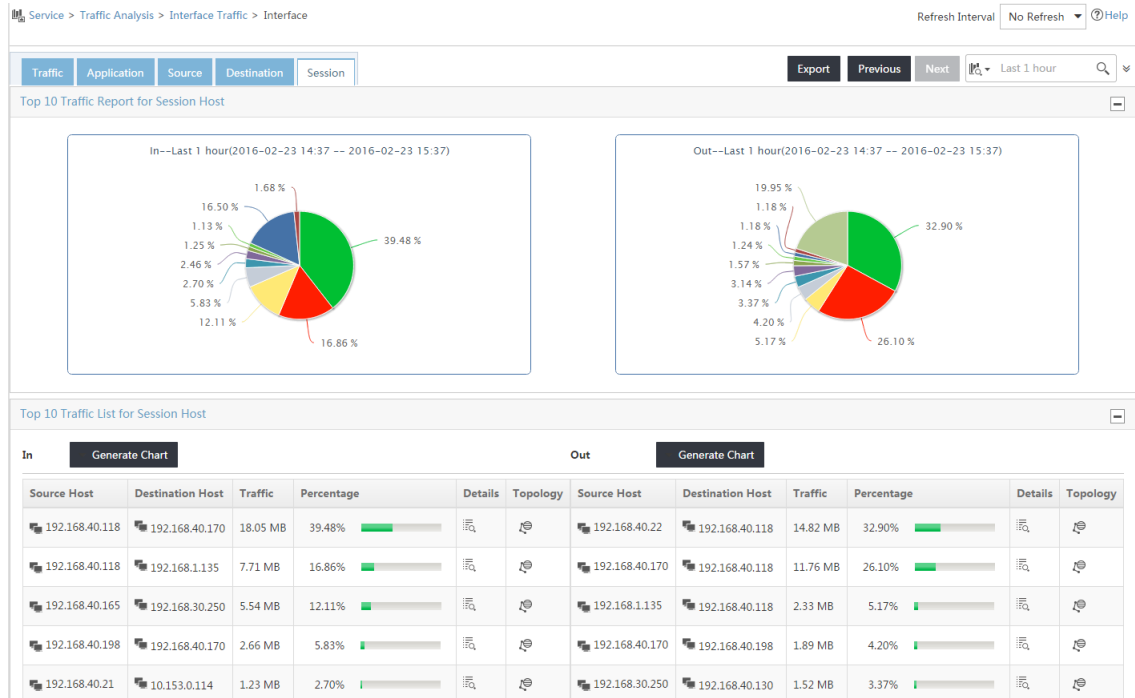
図8 インターフェイストラフィック分析タスクのアプリケーション情報



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の表示

Interface traffic analysis ページで、Session タブをクリックします。このタブには、図9に示すように、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が表示されます。

図9 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



ユーザーの動作の監査

1. Service タブをクリックします。
2. 左側のナビゲーションツリーで、Traffic Analysis and Audit > User Behavior Audit を選択します。User Behavior Audit ページが開きます。
3. 監査条件を入力し、Audit をクリックします。Audit Result ページが開きます(図10を参照)。

図10 監査結果のログ

The screenshot shows the 'User Behavior Audit' page with a table of audit results for the period 2016-02-23 15:30:26-2016-02-23 15:42:50. The table includes columns for Start Time, Source, Destination, Source Port, Destination Port, Protocol, Application, Packets Count, Flux, and Device. The data shows multiple entries for https traffic from 192.168.40.118 to 192.168.1.135 on port 443, with various destination ports (51486, 51482, 51483) and packet counts (1, 7).

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

NTA/UBAおよびNetStreamのトラブルシューティング

NTA/UBAサーバーでNetStreamデータを受信しませんでした。

問題を解決する手順は、次のとおりです。

1. ログを受信するためのUDPポート番号が、デバイスとNTAサーバーで同じであることを確認します。
2. デバイスとNTAサーバーが相互に接続できることを確認します。
3. NTAサーバーでファイアウォールが有効かどうかを判別します。ファイアウォールが有効な場合は、ファイアウォールを無効にするか、UDPポート9020、9021および6343を起動します。
4. ディレクトリ内に多数のファイルがあるかどうかを確認します。
\$IMC_INSTALL/data/recieverDataおよび\$IMC_INSTALL/data/processorData/data。
5. ディレクトリ内に多数のファイルがある場合は、次のタスクを実行します。
 - a. IMCプロセスを停止します。
 - b. ディレクトリ内のファイルを削除します。
 - c. データベース内のunba_slave.tbl_storing_task表を消去します。
 - d. IMCプロセスを再起動します。
6. データベースのディスク使用率を表示します。
 - a. **Service**タブをクリックします。
 - b. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Database Space**を選択します。
7. ディスク使用量がデータベースディスクの使用量しきい値を超えた場合は、ディスク容量を拡張するか、不要なデータを削除します。

NTA上にNetStreamデータがありません

問題を解決する手順は、次のとおりです。

1. デバイスのインターフェイスインデックスがNetStreamパケットのインターフェイスインデックスと同じであるかどうかを確認します。
2. これらが異なる場合は、次の手順に従ってインターフェイスインデックスを設定します。
 - a. **Service**タブをクリックします。
 - b. 左側のナビゲーションツリーで、**Traffic Analysis and Audit>Settings**を選択します。
Settingsページが開きます。
 - c. **[Guide to Quick Traffic Analysis And Audit Management]**領域で、**[Traffic Analysis Task Management]**をクリックします。
Task Managementページが開きます。
 - d. **Traffic Annalysis Task List**で**Add**をクリックします。**Select Task Type**ページが表示されます。
 - e. **Interface**を選択し、**Next**をクリックします。
Add Traffic Analysis Taskページが開きます。
 - f. 基本タスク情報を設定し、**Interface Information**領域で**Select**をクリックします。
 - g. **Add Interface**ページで、**Configure Manually**タブをクリックします。
 - h. 開いたページで、インターフェイスインデックスを設定します。

- i. OKをクリックします。

UBAの監査結果がない

問題を解決する手順は、次のとおりです。

1. **Server Configuration**ページのイントラネット情報を確認します。

UBAが監視するホストのIPアドレスがイントラネットネットワークに属していない場合、そのIPアドレスは監視されません。監視対象のIPアドレスを追加する手順は、次のとおりです。

- a. **Intranet Monitor Information**領域で、監視対象ホストのIPアドレスをイントラネット情報フィールドで

- b. 図4に示すように、**Add**をクリックします。

イントラネット情報エリアにIPアドレスが表示されます。

2. データベースにログインし、**unba_slave_tbl_nets_YYMMDDHH**テーブルが存在するかどうかを確認します。

- テーブルが存在する場合、NTA/UBAサーバーはNetStreamデータを受信できます。デバイスの時刻設定とタイムゾーンがNTA/UBAサーバーの設定と一致していることを確認してください。
- テーブルが存在しない場合、NTA/UBAサーバーはNetStreamデータを受信できません。問題の解決方法の詳細は、「NTA/UBAサーバーでNetStreamデータが受信されない」を参照してください。