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。

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
手順 IPマドレスおとびインタフェース情報の表示	44
NTA/UBAの構成	
ルーターでのNetStreamの設定 インターフェイストラフィック情報の表示	7 7
ユーザーの動作の監査 NTA/URAおとびNetStreamのトラブルシューティング	10 11
NTA/UBAサーバーでNetStreamデータを受信しませんでした。	
NTA上にNetStreamデータがありません UBAの監査結果がない	11 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)
 - \circ sFlow v5
- UBAでは、次のログタイプがサポートされています。
 - $\circ \quad Flow \ 1.0$
 - Flow 3.0
 - o 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

- 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。
- 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. Resouce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

Interface Status 🗘	Interface Description \Rightarrow	Interface Alias ≎	Last Change \$	Media Type ≎	Interface IP ≎	Up/Down Alarm F	Interface Link Type ≎
🕴 Down	Aux0	Aux0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface
S Down	Cellular0/0	Cellular0/0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface
🛿 Down	Vlan-interface1	Vlan-interface1 Inte	2016-02-15 09:06:30	Other	1.1.1.1	System Settings	Idle Interface
8 Down	Vlan-interface300	Vlan-interface300 L	2016-02-15 09:06:30	Other		System Settings	Idle Interface
🕏 Up	Ethernet5/0	Ethernet5/0 Interface	2016-02-15 09:06:40	Electrical	10.1.1.1	System Settings	SNMP Device-connected .
🕏 Up	Ethernet7/0	Ethernet7/0 Interface	2016-02-15 09:06:40	Electrical	10.1.2.1	System Settings	SNMP Device-connected .
🕏 Up	GigabitEthernet8/0	GigabitEthernet8/0	2016-02-15 09:06:40	Electrical	172.9.0.6	System Settings	Idle Interface
🕑 Up	GigabitEthernet8/1	GigabitEthernet8/1	2016-02-15 09:06:40	Electrical	172.8.8.114	System Settings	SNMP Device-connected
🕏 Up	GigabitEthernet0/0	GigabitEthernet0/0	2016-02-15 09:06:40	Electrical	90.16.0.240	System Settings	SNMP Device-connected .
🕑 Up	GigabitEthernet0/1	GigabitEthernet0/1	2016-02-15 09:06:40	Electrical	172.10.0.10	System Settings	SNMP Device-connected .
🛇 Up	NULLO	NULL0 Interface	2016-02-15 09:06:23	Other		System Settings	Idle Interface

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。
- Guide to Quick Traffic Analysis And Audit Management領域で、Device 3. 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。

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。 5.

図3 デバイスの追加

dd Device		
Basic Information		
Device IP *	90.16.0.240	Select
Name *	MSR30-20	
Description		
SNMP Community	•••••	
SNMP Port	161	
Log Source IP		
NetStream Statistics Identifier	Valid 🔻	
NetStream New Feature	Enable 👻	
sFlow Settings	Disable •	

OK Cancel

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。
- Guide to Quick Traffic Analysis And Audit Management領域で、Server 3. Managementをクリックします。 Server Listページが開きます。
- デアイコンをクリックします。 Server 4. 構成を配布する、NTA/UBAサーバーの Modify **Configuration**ページが表示されます。
- 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。 5.
 - 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

erver Configuration				
Basic Informatio	on			
Server Name *			127.0.0.1	
Server Description				
Server IP *			127.0.0.1	
istening Port *			9020,9021,6343	
TP Main Directory				
TP Username				
TP Password				
raffic Analysis Log A	ggregation Policy		Aggregation (Rough	Granulari: 🔻
ilter Policy			Not Filter	
Jsage Threshold of th	he Database Disk (1-95%) *		90	
When Database Disk	Usage Reaches Threshold		Stop Receiving Logs	
Traffic Analysis				
Device Informat	tion			
Select	Device Name	De	evice IP	Device Description
✓	MSR30-20	90	0.16.0.240	
Probe Informati	ion			
Select	Probe Name	Pro	obe IP	Enable Layer 7 Application Identific
No match found.				
User Behavior A	Audit			
Device Informa	ition			
Select	Device Name	De	evice IP	Device Description
✓	MSR30-20	90	0.16.0.240	
Probe Informat	tion			
Select	Probe Name	Probe IP	Enable Layer	7 Application Ic Enable Special Audit
No match found.				
Intranet Monito	or Information			
Intranet Information	n		?	Add
Intranet Informatio	on	C	Delete	
			-	

?Help

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。
- 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。

Deploy Cancel

Traffic Analysis Task Management ページが開きます。

- Addをクリックします。
 Select task Typeページが開きます。
- 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。

6. 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。

dd fraffic Analysis Task								
Basic Information								
Task Name	Interface							
Task Description								
Server *	127.0.0.1		•					
Task Type	Interface							
Reader					_			
					Select			
					Delete			
Vlan Analysis	Disable		•					
nterface Information	1							
Interface Information	1							
nterface Information	1						There	e are 6 records
nterface Information Select Interface Description	I Interface Alias	Interface Index	Interface IP	Max Rate	Device Name	Device IP	There Modify	e are 6 records Delete
Nterface Information Select Interface Description GigabitEthernet8/0	Interface Alias GigabitEthernet8/0 Interface	Interface Index 7	Interface IP 172.9.0.6	Max Rate 0.10 Gbps	Device Name MSR30-20	Device IP 90.16.0.240	There Modify	e are 6 records Delete
Interface Information Select Interface Description GigabitEthernet8/0 GigabitEthernet8/1	Interface Alias GigabitEthernet8/0 Interface GigabitEthernet8/1 Interface	Interface Index 7 8	Interface IP 172.9.0.6 172.8.8.114	Max Rate 0.10 Gbps 0.10 Gbps	Device Name MSR30-20 MSR30-20	Device IP 90.16.0.240 90.16.0.240	There Modify E	e are 6 records Delete
Select Interface Description GigabitEthernet8/0 GigabitEthernet8/1 GigabitEthernet0/1	Interface Alias GigabitEthernet8/0 Interface GigabitEthernet8/1 Interface GigabitEthernet0/1 Interface	Interface Index 7 8 10	Interface IP 172.9.0.6 172.8.8.114 172.10.0.10	Max Rate 0.10 Gbps 0.10 Gbps 0.10 Gbps 0.10 Gbps	Device Name MSR30-20 MSR30-20 MSR30-20	Device IP 90.16.0.240 90.16.0.240 90.16.0.240	There Modify E E E	e are 6 records Delete 1 1 1 1 1 1 1
Interface Information Select Interface Description GigabitEthernet8/0 GigabitEthernet8/1 GigabitEthernet7/1 Ethernet7/0	Interface Alias GigabitEthernet8/0 Interface GigabitEthernet8/1 Interface GigabitEthernet0/1 Interface Ethernet7/0 Interface	Interface Index 7 8 10 6	Interface IP 172.9.0.6 172.8.8.114 172.10.0.10 10.1.2.1	Max Rate 0.10 Gbps 0.10 Gbps 0.10 Gbps 0.10 Gbps 0.10 Gbps 0.10 Gbps	Device Name MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20	Device IP 90.16.0.240 90.16.0.240 90.16.0.240 90.16.0.240	There Modify E E E E	e are 6 records Delete 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Select Interface Description GigabitEthernet8/0 GigabitEthernet8/1 GigabitEthernet0/1 Ethernet7/0 Ethernet5/0	Interface Alias GigabitEthernet8/0 Interface GigabitEthernet8/1 Interface GigabitEthernet0/1 Interface Ethernet7/0 Interface Ethernet5/0 Interface	Interface Index 7 8 10 6 5	Interface IP 172.9.0.6 172.8.114 172.100.10 10.1.2.1	Max Rate 0.10 Gbps 0.10 Gbps	Device Name MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20 MSR30-20	Device IP 90.16.0.240 90.16.0.240 90.16.0.240 90.16.0.240 90.16.0.240 90.16.0.240 90.16.0.240	There Modify E E E E E E E E E	beare 6 records belee b

OK Cancel

図5 インターフェイストラフィック分析タスクの追加

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 <i>ip-address</i> udp-port [vpn-instance <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 ターフェイ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

- 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。

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



Task Name ≎	In Rate \$	Avg. Link Utilization \$	Out Rate \$	Avg. Link Utilization \$	Traffic Log Audit
Interface	0.10 Mbps	0.00%	0.10 Mbps	0.00%	医用

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。
 - を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

		> interface	Traffic > Interfa	ce					Refresh In	terval No Refres	1 • ?
Traffic	Application	Source	Destination	Session			E	xport Previous	Next	Ro - Last 1 hour	C
affic Trer	ıd										
					Last 1 hour	(2016-02-23 14:37 -	- 2016-02-23 15:37)				
			Avg. Rate in 1 Minute(Mi 0.22	(Mbps) (Mbps) (Mbps) (Mbps)	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	15:00 - in - Or	AAA 15.10 15.20 a	AAAA 15:30			
Direction	Total T	raffic	Max. Avg Ra	te	Min. Avg Rate	Avg. Rate	Avg. Link Utilization	N	Max. Link Util	ization	
1	45.71 N	ЛB	0.53 Mbps		15.38 Kbps	0.11 Mbps	0.00%		0.01%		
ut	44.96 N	ЛB	0.27 Mbps		34.29 Kbps	0.10 Mbps	0.00%		0.00%		
C Distrib	ute In Interfac	e								Interface flux r	eport
dex(1 ~ 6	i) of Total 6					22 27 27 27 27 28 28 28 28 28 28 28 28 28 28 28 28 28	2				
dex(1 ~ 6	i) of Total 6					Avg. Rate(Mb	ps)				
dex(1 ~ 6 3(Mbps)	6) of Total 6	0				Avg. Rate(Mb	ps)				
ndex(1 ~ 6).3(Mbps)).2(Mbps)).1(Mbps)	i) of Total 6					Avg. Rate(Mb	05)				
ndex(1 ~ 6).3(Mbps)).2(Mbps)).1(Mbps) 0(Mbps)	i) of Total 6	abitE		GigabitE		Avg. Rate(Mb	os) GigabitE	Ethernet		Ethernet	

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

affic Application Source Destin	ation Session		Export	Previous Next	No ▼ Last 1 hour Q
lication List					
plication \$	Unknown Applications	In Traffic ≎	In Speed ≎	Out Traffic \$	Out Speed \$
mptrap		0.00 B	0.00 bps	51.93 KB	0.12 Kbps
tps		27.30 MB	63.62 Kbps	22.95 MB	53.47 Kbps
p		5.54 MB	12.91 Kbps	0.47 MB	1.09 Kbps
np		3.77 MB	8.79 Kbps	5.93 MB	13.82 Kbps
P Protocol Unknown Application		3.29 MB	7.67 Kbps	8.22 MB	19.15 Kbps
р		0.63 MB	1.46 Kbps	0.82 MB	1.91 Kbps
beros		0.61 MB	1.42 Kbps	0.60 MB	1.39 Kbps
0		0.55 MB	1.29 Kbps	1.55 MB	3.61 Kbps
net		0.42 MB	0.97 Kbps	1.44 MB	3.35 Kbps
Protocol Unknown Application		0.37 MB	0.85 Kbps	1.64 MB	3.81 Kbps
bios-ns		0.12 MB	0.28 Kbps	0.47 MB	1.08 Kbps
nain		81.30 KB	0.18 Kbps	0.10 MB	0.24 Kbps
bios-dgm		8.76 KB	19.93 bps	66.26 KB	0.15 Kbps
		4.16 KB	9.46 bps	0.00 B	0.00 bps
rosoft-ds		0.43 KB	0.98 bps	0.52 KB	1.17 bps
15 of 15. Page 1 of 1. cation Traffic Trend				× <	1 > » 50 •
InLast 1 hour(2016-02-23 1- 150(kbps) 100(kbps) 50(kbps) 14:45 15 somptrap https rdp somp Idap kerbers http Teinet	1:37 2016-02-23 15:37) 00 15:15 15:30 • TCP Protocol Unknown Application UUP Protocol Unknown Application	Qut- Qut- QQUest 150(kbps) WI 100(kbps) QU QUA QUA QUA	Last 1 hour(2016-02-2 14:45 https • rdp • sn erberos • http • Tel	23 14:37 2016-02-23 1 15:00 15:15 mp TCP Protocol Unknow t UDP Protocol Unknow	5:37) 15:30 n Application n Application

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。
- 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。
- 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

enty of logs e	xist, it may take sev	veral minutes or lon	ger time to query log	s.)				
:30:26-2016-0	2-23 15:42:50							
						Group No	t Group	^
ie 0	Destination \$	Source Port \$	Destination Port \$	Protocol \$	Application \$	Packets Count \$	Flux ¢	Device ≎
2.168.40.118	R. 192.168.1.135	443	51486	тср	https	1	40.00 B	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51486	ТСР	https	1	40.00 B	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51486	ТСР	https	7	3.43 KB	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51482	ТСР	https	7	4.84 KB	90.16.0.240
2.168.40.118	L. 192.168.1.135	443	51482	ТСР	https	1	40.00 B	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51482	тср	https	1	40.00 B	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51482	ТСР	https	1	40.00 B	90.16.0.240
2.168.40.118	R. 192.168.1.135	443	51483	ТСР	https	7	2.29 KB	90.16.0.240
	:e ¢ 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118 2.168.40.118	Image Image 3:30:26-2016-02-23 15:42:50 Image Destination © 2:168:40.118 Image Image Image Image Image </td <td>Bet institution (*) Source Port (*) 2168-40.118 R. 192.168.1135 443 2168.40.118 R. 192.168.1135 443</td> <td>Image: Source Port © Destination © Source Port © Destination Port © 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482</td> <td>Betination © Source Port © Destination Port © Protocol © 2168-0118 Ph 192.168.1.135 443 51486 TCP 2168-0118 Ph 192.168.1.135 443 51482 TCP 2168-0118 Ph 192.168.1.135 443 51483 TCP</td> <td>Bestination © Source Port © Destination Port © Protocol © Application © 2168.40118 Ña 192.168.1.135 443 51486 TCP https 2168.40118 Ña 192.168.1.135 443 51482 TCP https</td> <td>Note of the second of t</td> <td>Not or option of the start where th</td>	Bet institution (*) Source Port (*) 2168-40.118 R. 192.168.1135 443 2168.40.118 R. 192.168.1135 443	Image: Source Port © Destination © Source Port © Destination Port © 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51486 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482 2168:40.118 %1.192.168.1.135 443 51482	Betination © Source Port © Destination Port © Protocol © 2168-0118 Ph 192.168.1.135 443 51486 TCP 2168-0118 Ph 192.168.1.135 443 51482 TCP 2168-0118 Ph 192.168.1.135 443 51483 TCP	Bestination © Source Port © Destination Port © Protocol © Application © 2168.40118 Ña 192.168.1.135 443 51486 TCP https 2168.40118 Ña 192.168.1.135 443 51482 TCP https	Note of the second of t	Not or option of the start where th

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。
- 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。

- 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。