

H3C IMC NTA/UBA NAT と IMC UBA によりユーザーの行動監査の 設定例

ソフトウェアバージョン:IMC UBA7.3(E0503)

Copyright©2014-2017New H3C Technologies Co.,Ltd.All rights reserved.
本書のいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしには、いかなる形式または手段によっても複製または変更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	1
制限事項およびガイドライン	1
例:NAT および IMC UBA を介したユーザ動作の監査	1
ネットワーク構成	1
使用されるソフトウェアバージョン	2
NAT デバイスの設定	2
UBA の設定	3
NAT デバイスの UBA への追加	3
UBA サーバー構成の変更	5
NAT 監査タスクの追加	6
設定の確認	8

はじめに

このドキュメントでは、NAT および IMC UBA を使用して、パブリックネットワークにアクセスする際のプライベートネットワークユーザの動作を監視および監査する例を示します。

制限事項およびガイドライン

MSR20-20 ルータは、NAT ログイングをサポートする必要があります。

例:NAT および IMC UBA を介したユーザ動作の監査

ネットワーク構成

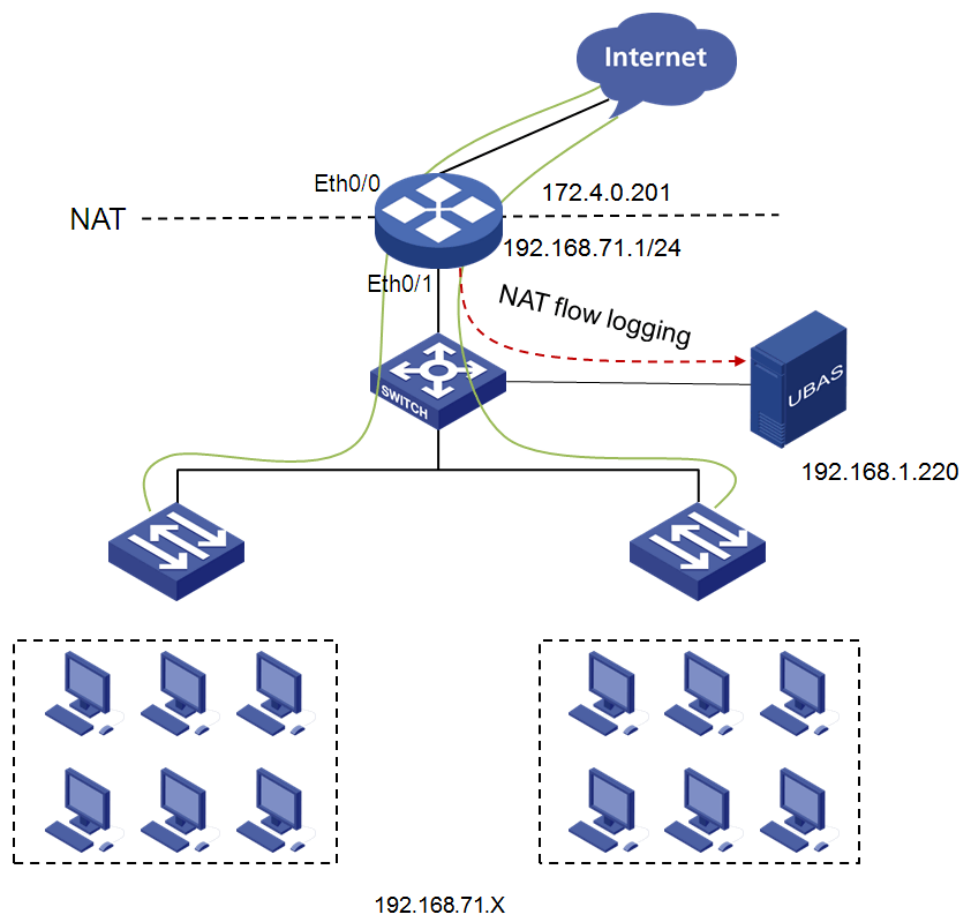
図 1 に示すように、NAT は MSR20-20 ルータ上で設定され、192.168.71.0/24 のユーザがインターネットにアクセスできるようにします。

UBA でユーザの動作を監査するには、次のタスクを実行します。

- MSR20-20 ルータで NAT ログイングをイネーブルにします。
- UBA サーバーを構成します。

ルータと UBA サーバーが相互に到達できることを確認します。

図 1 ネットワーク図



使用されるソフトウェアバージョン

この設定例は、H3C MSR20-20、Comware Software Version5.20、Release2509 で作成および検証されています。

NATデバイスの設定

#NAT ログを伝送する UDP パケットの送信元 IP アドレスを設定します(この例では、送信元 IP アドレスとしてデバイスの管理 IP アドレスが使用されます)。

```
<MSR20-20> system-view
[MSR20-20] userlog nat export source-ip 172.4.0.201
```

#NAT ログを IP アドレス 192.168.1.220 の UBA サーバーのポート番号 9020 にエクスポートします。

```
[MSR20-20] userlog nat export host 192.168.1.220 9020
```

#NAT ログをイネーブルにします。

```
[MSR20-20] nat log enable
[MSR20-20] nat log flow-begin
[MSR20-20] nat log flow-active 10
```

UBAの設定

NAT デバイスの UBA への追加

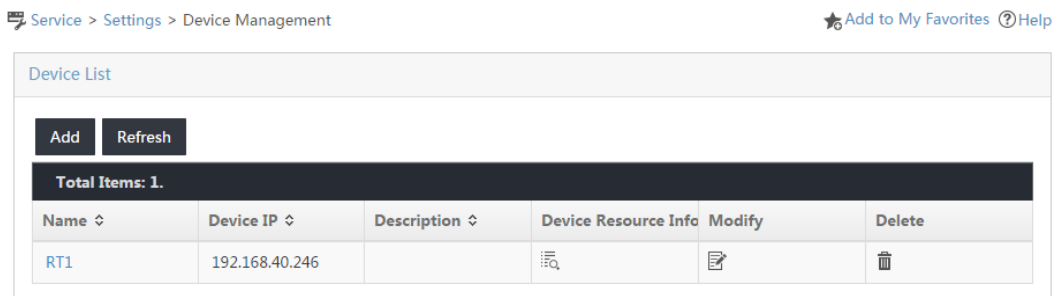
1. Service タブをクリックします。
2. ナビゲーションツリーで、Traffic Analysis and Audit > Settings を選択します。
Settings ページが表示されます(図 2 を参照)。

図 2 Settings ページ



3. Guide to Quick Traffic Analysis And Audit Configuration 領域で、Device Management をクリックします。
Device Management ページが開きます(図 3 を参照)。

図 3 Device Management ページ



4. Add をクリックします。
Add Device ページが表示されます(図 4 を参照)。

図 4 デバイスを追加する

Service > Settings > Device Management > Add Device

Help

Add Device

Basic Information

Device IP * Select

Name *

Description

SNMP Community

SNMP Port

Log Source IP

NetStream Statistics Identifier

NetStream New Feature

sFlow Settings

OK Cancel

5. デバイスを UBA に追加します。
 - デバイスが iMC プラットフォームに追加されている場合は、Select をクリックして選択します。
SNMP コミュニティ、SNMP ポート、およびログソース IP の設定はオプションです。
 - デバイスが iMC プラットフォームに追加されていない場合は、デバイスの IP アドレスと名前をそれぞれ Device IP フィールドと Name フィールドに入力します。
SNMP コミュニティおよび SNMP ポートの設定が必要です。
6. 図 5 に示すように、デバイスに次のパラメータを設定します。
 - SNMP コミュニティおよび SNMP ポートには、それぞれデフォルト設定の public および 161 を使用します。設定がデバイス上の設定と同じであることを確認してください。
 - 必要に応じて、Log Source IP フィールドで IP アドレスを設定します。
IP アドレスは、iMC が SNMP を介してデバイスインターフェイス情報を取得できない場合に使用されます。この例では、このパラメータは使用していません。
 - NetStream Statistics Identifier リストから Invalid を選択します。
 - NetStream New Feature リストから Disable を選択します。
 - sFlow 設定リストから無効を選択します。
7. OK をクリックします。

図 5 NAT デバイスの UBA への追加

Service > Settings > Device Management > Add Device Help

Add Device

Basic Information

Device IP *	<input type="text" value="172.4.0.201"/>	Select
Name *	<input type="text" value="MSR2020"/>	
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="Invalid"/>	
NetStream New Feature	<input type="text" value="Disable"/>	
NetStream Sampling Ratio *	<input type="text" value="1"/>	
sFlow Settings	<input type="text" value="Disable"/>	

UBA サーバー構成の変更

NAT ログを UBA サーバに送信するデバイスを指定できます。

1. Guide to Quick Traffic Analysis And Audit Configuration 領域で、Server Management をクリックします。


Server Management ページが表示されます(図 6 を参照)。

図 6 Server Management ページ

Service > Settings > Server Management Add to My Favorites Help

Server List

Total Items: 1.

Server Name	Server IP	Description	Capture Flux Log	Deploy Configuration	Modify
127.0.0.1	127.0.0.1			<input checked="" type="checkbox"/>	

2.  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(図 7 を参照)。

図 7 サーバー構成の変更

Service > Settings > Server Management > Server Configuration

Help

Server Configuration

Basic Information

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

User Behavior Audit

Device Information

Select	Device Name	Device IP	Device Description
<input checked="" type="checkbox"/>	MSR2020	172.4.0.201	
<input type="checkbox"/>	RT1	192.168.40.246	

Probe Information

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

Intranet Monitor Information

Intranet Information ?

Intranet Information	Delete
192.168.71.0/24	<input type="button" value="Delete"/>

3. Basic Information 領域の既定の設定を使用します。
4. Device Information 領域で NAT デバイス MSR2020 を選択します。
5. イントラネットモニタ情報領域にイントラネット IP アドレスを入力し、追加をクリックします。イントラネット情報エリアにアドレスが表示されます。
6. Deploy をクリックします。

NAT 監査タスクの追加

1. Guide to Quick Traffic Analysis And Audit Configuration 領域で、User Behavior Audit Management をクリックします。
User Behavior Audit Management ページが開きます(図 8 を参照)。

図 8 User Behavior Audit Management ページ

Service > Settings > User Behavior Audit Management

Custom Audit List

Add Refresh Delete

<input type="checkbox"/>	Name ▲	Server	Type	Audit	Modify	Delete
No match found.						

0-0 of 0. Page 1 of 1. << < > >> 50 ▼

2. Add をクリックします。
Select Audit Type ページが開きます(図 9 を参照)。

図 9 監査タイプの選択

Service > Settings > User Behavior Audit Management > Select Audit Type

Select Audit Type

General Audit
Query audit result by source, destination, port, protocol and application.

NAT Audit
Audit and track user network behavior according to the IP addresses before and after translation, and the port.

Next Back

3. NAT Audit を選択し、Next をクリックします。
Add Custom NAT Audit ページが開きます(図 10 を参照)。

図 10 カスタム NAT 監査タスクの追加

Service > Settings > User Behavior Audit Management > Add Custom NAT Audit ? Help

Add Custom NAT Audit

Name *

Server *

Reader

NAT Condition

NAT IP

NAT Port

Operator

Basic Audit Condition

Meet All Meet Any

Source

Destination

Source Port

Destination Port

Protocol

Application

Device

4. Name フィールドに NAT Audit と入力します。
5. Server リストから 127.0.0.1 を選択します。
6. Audit Condition 領域で Meet All を選択します。
7. 他のパラメータの既定の設定を使用します。
8. OK をクリックします。

設定の確認

1. ナビゲーションツリーで、Traffic Analysis and Audit > NAT Audit を選択します。
Custom Audit List ページに監査タスク NAT Audit が表示されます(図 11 を参照)。

図 11 監査タスクの表示

Service > Settings > User Behavior Audit Management

Custom Audit List						
Add Refresh Delete						
<input type="checkbox"/>	Name ▲	Server	Type	Audit	Modify	Delete
<input type="checkbox"/>	NAT Audit	127.0.0.1	NAT			

1-1 of 1. Page 1 of 1. << < 1 > >> 50 ▼

2. NAT Audit の Audit アイコンをクリックします。

結果の生成には時間がかかります。

図 12 監査結果ページ

Service > User Behavior Audit Management > NAT Audit > NAT Audit Last 1 hour Help

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

Audit Time: Last 1 hour
 Start Time: 2016-03-12 09:54
 End Time: 2016-03-12 10:54 Audit

Audit Result: 2016-03-12 10:00:41-2016-03-12 10:50:36

Custom										
Start Time	Source	Destination	Source Port	Destination Port	Protocol	Application	NAT IP	NAT Port	Operator	Device
2016-03-12 10:...	192.168.71.2	10.63.16.77	49389	80	TCP	http	172.4.0.201	1255	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.8	10.63.16.77	49390	80	TCP	http	172.4.0.201	1256	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.131	68.232.45.48	49387	80	TCP	http	172.4.0.201	1253	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.13	68.232.45.48	49388	80	TCP	http	172.4.0.201	1254	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.131	74.125.23.138	49385	443	TCP	https	172.4.0.201	1251	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.8	74.125.23.138	49386	443	TCP	https	172.4.0.201	1252	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.2	74.125.23.138	49385	443	TCP	https	172.4.0.201	1251	Aged upon Ti...	172.4.0.201
2016-03-12 10:...	192.168.71.13	74.125.23.138	49386	443	TCP	https	172.4.0.201	1252	Aged upon Ti...	172.4.0.201
2016-03-12 10:...	192.168.71.131	74.125.23.139	49383	443	TCP	https	172.4.0.201	1249	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.2	74.125.23.139	49384	443	TCP	https	172.4.0.201	1250	Creation Recor...	172.4.0.201
2016-03-12 10:...	192.168.71.36	74.125.23.139	49383	443	TCP	https	172.4.0.201	1249	Aged upon Ti...	172.4.0.201
2016-03-12 10:...	192.168.71.36	74.125.23.139	49384	443	TCP	https	172.4.0.201	1250	Aged upon Ti...	172.4.0.201
2016-03-12 10:...	192.168.71.2	74.125.23.100	49381	443	TCP	https	172.4.0.201	1247	Creation Recor...	172.4.0.201

変換された送信元 IP アドレスと送信元ポートを確認できます。