Hewlett Packard Enterprise

# Configuration Examples for Auditing User Behaviors through IMC UBA and NetStream or NetFlow

Part number: 5200-4109
Software version: iMC UBA 7.3 (E0503)

# Contents

# Introduction

This document provides examples for using IMC UBA and H3C NetStream or Cisco NetFlow to monitor and audit private network user behaviors in accessing a public network.

# Restrictions and guidelines

The device must support NetStream or NetFlow.

# Example: Auditing user behaviors through IMC UBA and NetStream or NetFlow

This example uses the following networking schemes:

- **Scheme 1**—The NetStream-capable H3C MSR 26-00-10 router and IMC UBA
- **Scheme 2**—The H3C S7503E switch, H3C SecBlade NetStream card, and IMC UBA
- **Scheme 3**—NetFlow-capable Cisco 2901/K9 router and IMC UBA

## Network configuration (available for scheme 1)

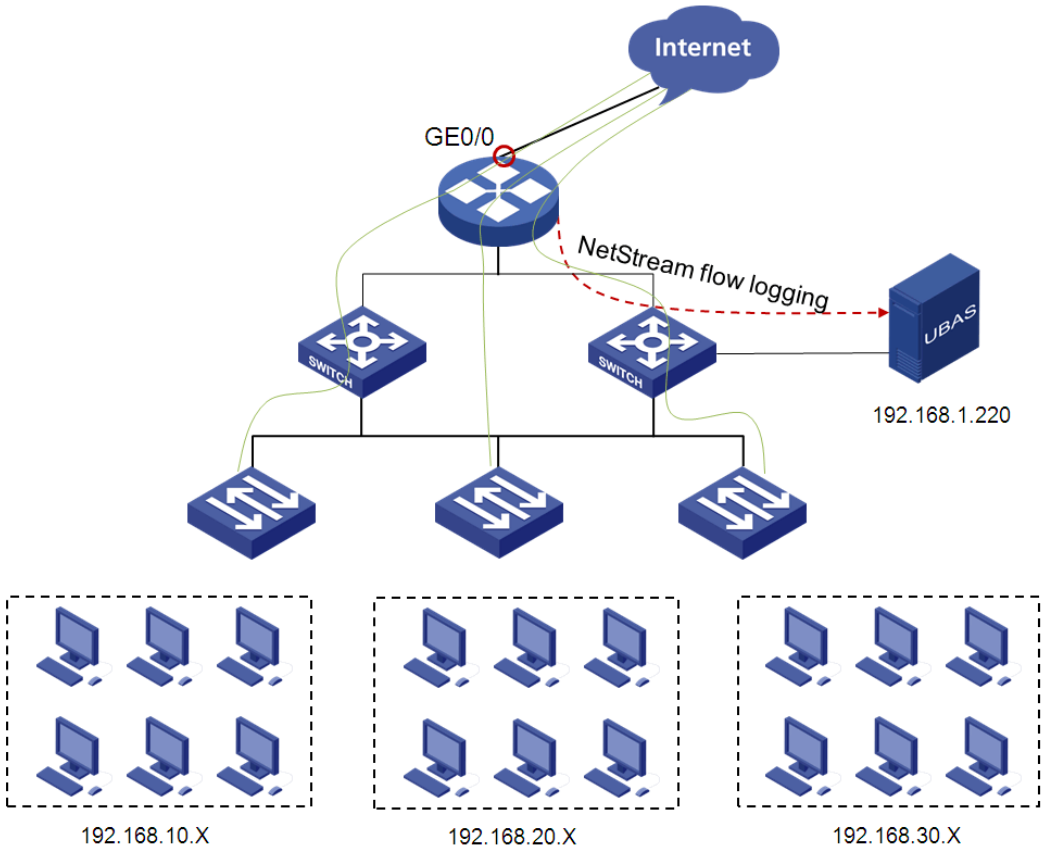
As shown in Figure 1, users on segments 192.168.10.255, 192.168.20.255, and 192.168.30.255 access the Internet through the MSR 26-00-10 router.

To audit user behaviors in UBA, perform the following tasks:

- Enable NetStream for both incoming and outgoing traffic on GigabitEthernet 0/0 on the MSR 26-00-10 router to collect statistics on packets passing through the router.
- Configure the router to send NetStream logs to the UBA server for user behavior audit.

Make sure the router and the UBA server can reach each other.

**Figure 1 Network diagram**




# Software versions used

This configuration example was created and verified on the following platforms:

- H3C MSR 26-00-10, Comware Software Version 5.20 Release 2313
- H3C S7503E, Comware Software Version 5.20 Release 6708P08
- H3C SecBlade NetStream card, Comware Software Version 5.20 Release 3109P03
- Cisco 2901/K9, Version 15.1 (4) M2

# Configuring NetStream on the MSR 26-00-10 router (available for scheme 1)

# Enable NetStream for incoming and outgoing traffic on GigabitEthernet 0/0.

```
<Router> system-view
[Router] interface GigabitEthernet 0/0
[Router-GigabitEthernet0/0] ip netstream outbound
[Router-GigabitEthernet0/0] ip netstream inbound
[Router-Ethernet1/0] quit
```

# Specify the export destination host as 192.168.1.220 with UDP port 9998.

```
[Router] ip netstream export host 192.168.1.220 9998
```

# Configure the router to export NetStream data in the version 9 format. The NetStream traditional data export uses the version 5 format by default.

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

# Network configuration (available for scheme 2)

As shown in Figure 2:

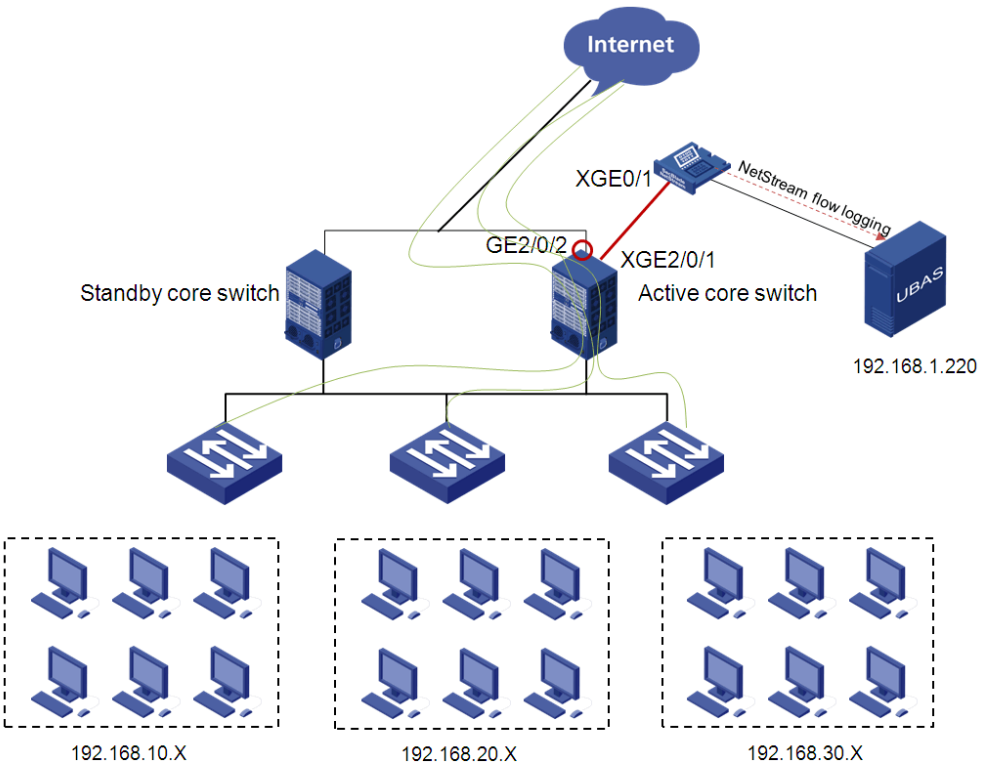
- Users on segments 192.168.10.255, 192.168.20.255, and 192.168.30.255 access the Internet through two S7503E core switches. This example uses the active core switch.
- A NetStream card is installed in the active core switch. Ten-GigabitEthernet 0/1 on the NetStream card is connected to Ten-GigabitEthernet 2/0/1 on the switch.

To audit user behaviors in UBA, perform the following tasks:

- Configure port mirroring on GigabitEthernet 2/0/2 on the switch.

  Port mirroring copies the traffic to the NetStream card.
- Enable NetStream on the NetStream card, and make sure the NetStream card and the UBA server can reach each other.
- Configure the switch to send NetStream logs to the UBA server for user behavior audit.

**Figure 2 Network diagram**




# Configuring NetStream on the S7503E switch (available for scheme 2)

1. Configure the S7503E switch:

   # Create local mirroring group 1.

```
[Sysname] system-view
[Sysname] mirroring-group 1 local
```

# Configure mirroring group 1 to monitor the incoming and outgoing traffic on GigabitEthernet 2/0/2.

```
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet2/0/2 both
```

# Configure Ten-GigabitEthernet 2/0/1 as the monitor port of mirroring group 1.

```
[Sysname] mirroring-group 1 monitor-port Ten-GigabitEthernet2/0/1
```

# Enable ACSEI server so that the NetStream card can synchronize the clock of the MPU on the switch.

```
[Sysname] acsei server enable
```

**2.** Configure the NetStream card:

# Create blackhole-type inline forwarding entry 1.

```
[Sysname] inline-interfaces 1 blackhole
```

# Assign Ten-GigabitEthernet 0/1 to inline forwarding entry 1.

```
[Sysname] interface Ten-GigabitEthernet0/1
[Sysname-Ten-GigabitEthernet0/1] port inline-interfaces 1
```

# Enable NetStream for incoming traffic on Ten-GigabitEthernet 0/1.

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

# Enable ACSEI client on Ten-GigabitEthernet 0/1 so that the NetStream card can synchronize the clock of the MPU on the switch.

```
[Sysname-Ten-GigabitEthernet0/1] acsei-client enable
[Sysname-Ten-GigabitEthernet0/1] quit
```

# Specify the export destination host as 192.168.1.220 with UDP port 9020.

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

# Configure the switch to export NetStream data in the version 9 format. The NetStream traditional data export uses the version 5 format by default.

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

# Network configuration (available for scheme 3)

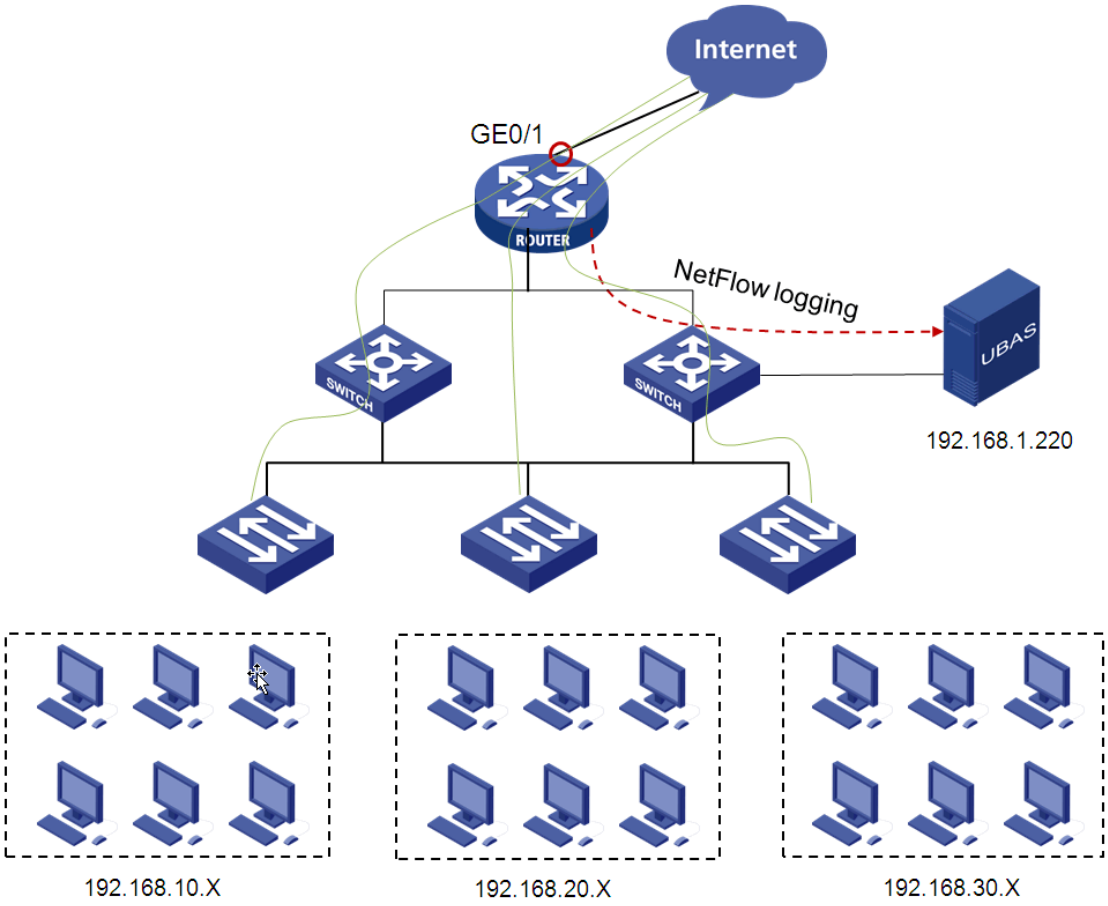
As shown in Figure 3, users on segments 192.168.10.255, 192.168.20.255, and 192.168.30.255 access the Internet through the Cisco 2901/K9 router.

To audit user behaviors in UBA, perform the following tasks:

- Enable NetFlow for both incoming and outgoing traffic on GigabitEthernet 0/1 on the Cisco 2901/K9 router to collect statistics on packets passing through the router.
- Configure the router to send NetFlow logs to the UBA server for user behavior audit.

Make sure the router and the UBA server can reach each other.

**Figure 3 Network diagram**




# Configuring NetFlow on the Cisco 2901/K9 router (available for scheme 3)

# Enable NetFlow for both incoming and outgoing traffic on GigabitEthernet 0/1 on the router.

```
Router#config
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
```

# Specify the NetFlow export destination host as 192.168.1.220 with UDP port 9991.

```
Router(config-if)#exit
Router(config)#ip flow-export destination 192.168.1.220 9991
```

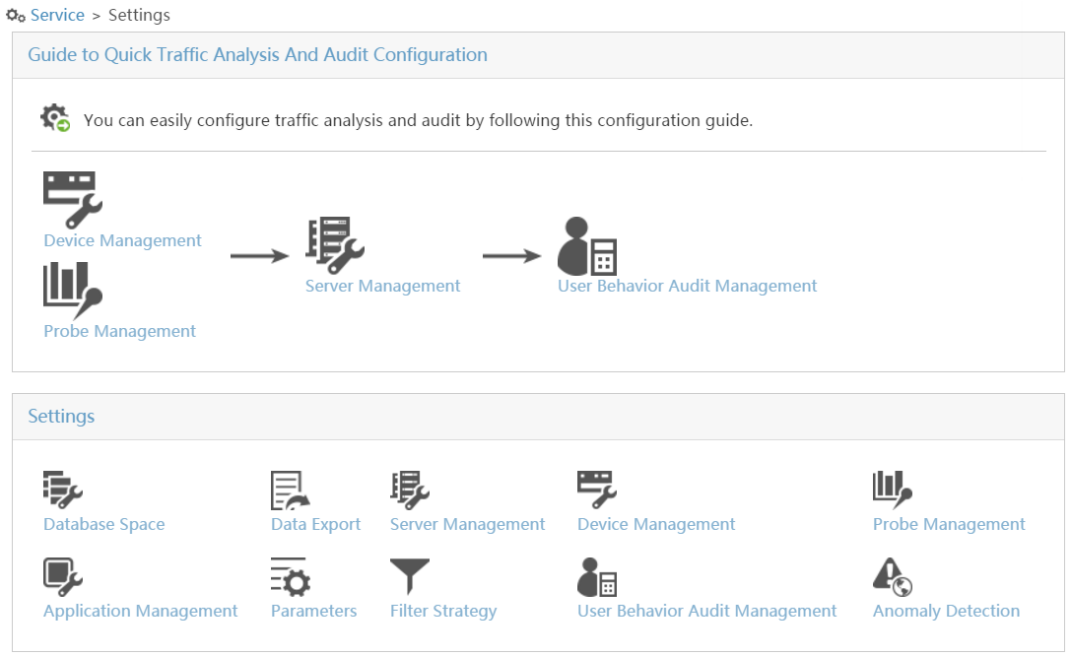
# Configuring UBA (available for schemes 1, 2, and 3)

The UBA server configuration is similar for the above networking schemes. The differences are included in the steps.

# Adding the NetStream or NetFlow device to UBA

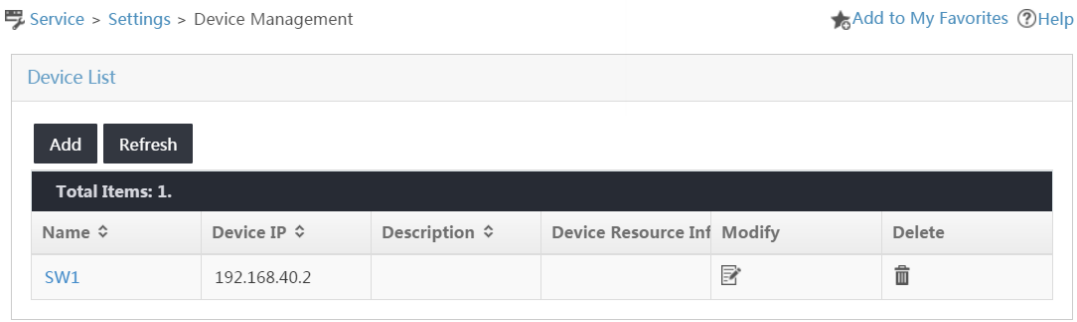
1. Click the **Service** tab.
2. From the navigation tree, select **Traffic Analysis and Audit** > **Settings**.
   The **Settings** page opens, as shown in Figure 4.

   **Figure 4 Settings page**



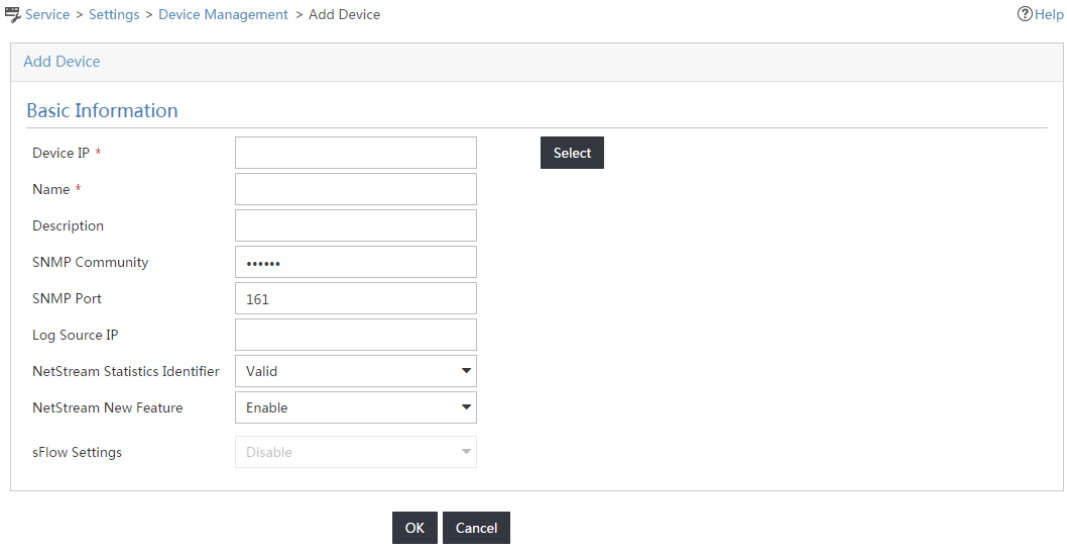

3. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **Device Management**.
   The **Device Management** page opens, as shown in Figure 5.

   **Figure 5 Device Management page**




4. Click **Add**.
   The **Add Device** page opens, as shown in Figure 6.

**Figure 6 Adding a device**




5. Add a device to UBA:
   - If the device has been added to the IMC Platform, click **Select** to select it.

     Settings for **SNMP Community**, **SNMP Port**, and **Log Source IP** are optional.
   - If the device is not added to the IMC Platform, enter the device's IP address and name in the **Device IP** and **Name** fields, respectively.

     Settings for **SNMP Community** and **SNMP Port** are required.

**NOTE:**

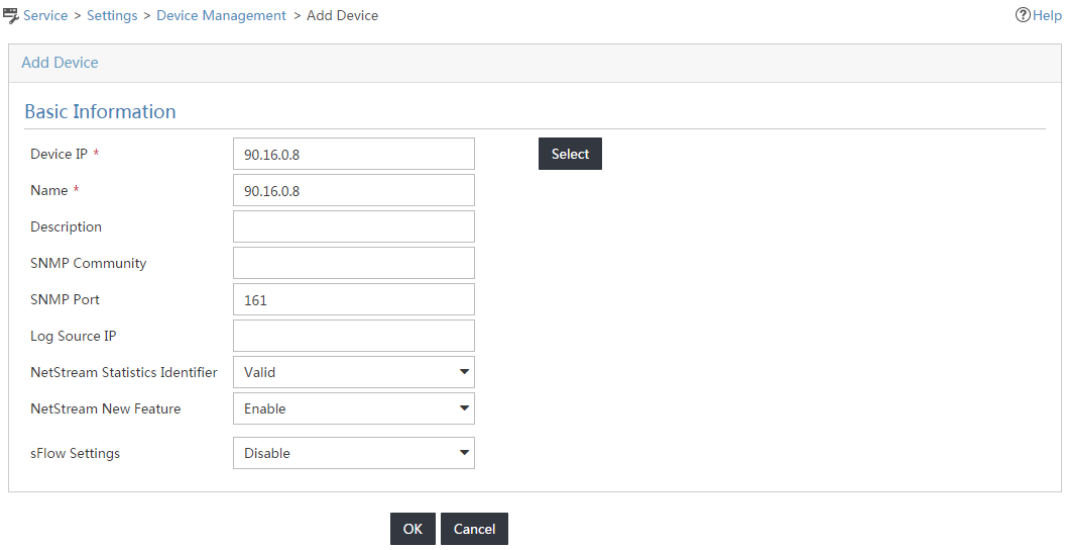
For the networking scheme in Figure 2, the NetStream card should be added because it has its own management IP address.

6. Configure the following parameters for the device, as shown in Figure 7:
   - Use the default settings **public** and **161** for **SNMP Community** and **SNMP Port**, respectively. Make sure the settings are the same as those on the device.
   - Configure an IP address in the **Log Source IP** field as needed.

     The IP address is used when IMC cannot obtain the device interface information through SNMP. This example does not use this parameter.
   - Select **Valid** from the **NetStream Statistics Identifier** list.
   - Select **Enable** from the **NetStream New Feature** list.

   The device uses NetStream sampling in Comware V5.
7. Click **OK**.

**Figure 7 Adding the NetStream device to UBA**



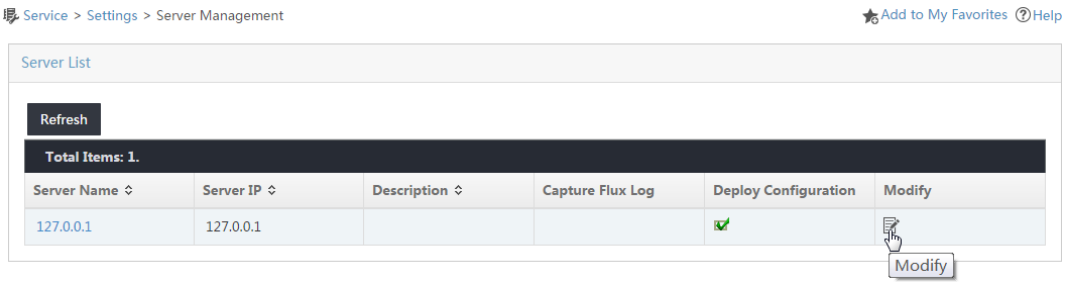

# Modifying the UBA server configuration

You can specify a device that sends NetStream or NetFlow logs to the UBA server.

1. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **Server Management**.

   The **Server Management** page opens, as shown in Figure 8.

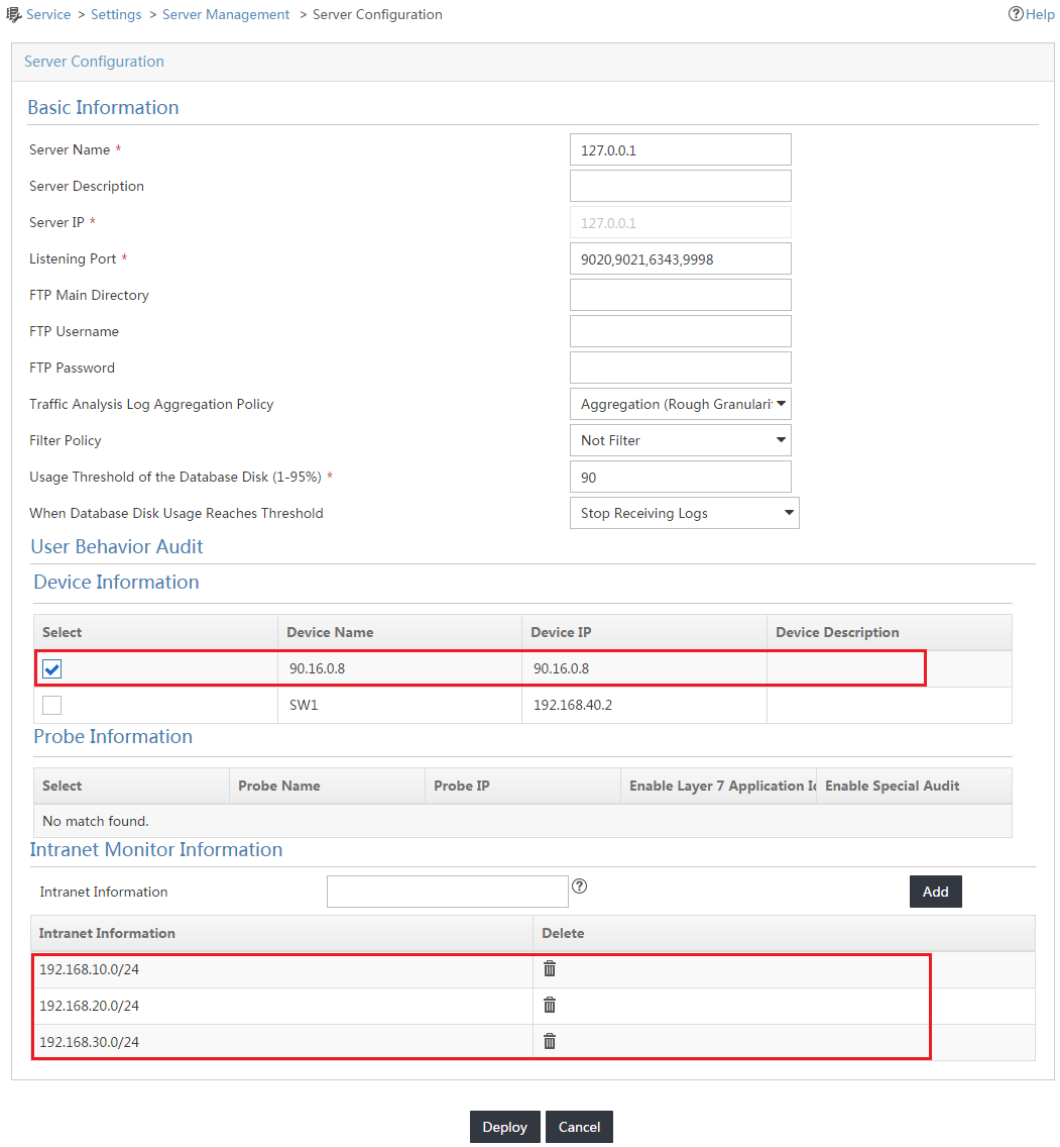
   **Figure 8 Server Management page**




2. Click the **Modify** icon  for the UBA server.

   The **Server Configuration** page opens, as shown in Figure 9.

**Figure 9 Modifying the server configuration**

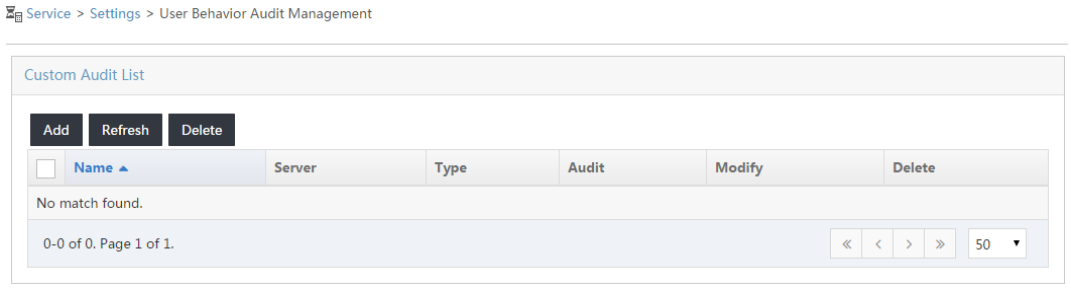



3. Keep the default settings in the **Basic Information** area.
4. Select 90.16.0.8 in the **Device Information** area in this example.
5. Enter intranet IP addresses in the **Intranet Monitor Information** area, and click **Add**.
   The intranet network segments are displayed in the **Intranet Information** area.
6. Click **Deploy**.

# Adding a user behavior audit task

1. In the **Guide to Quick Traffic Analysis And Audit Configuration** area, click **User Behavior Audit Management**.
   The **User Behavior Audit Management** page opens, as shown in Figure 10.

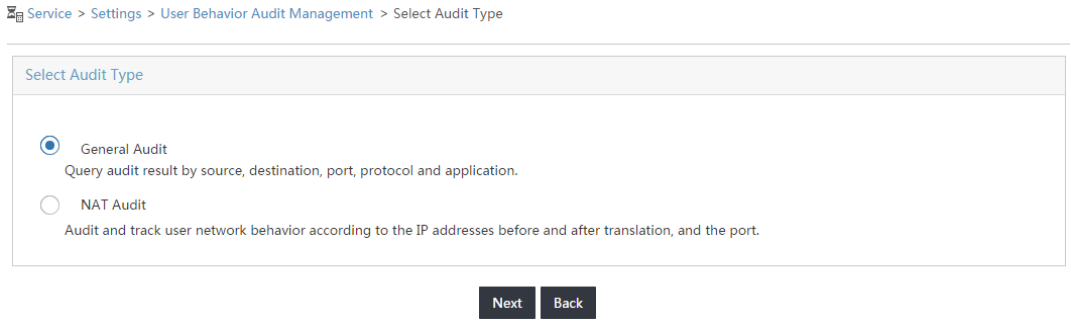
**Figure 10 User Behavior Audit Management page**




2. Click **Add**.

   The **Select Audit Type** page opens, as shown in Figure 11.

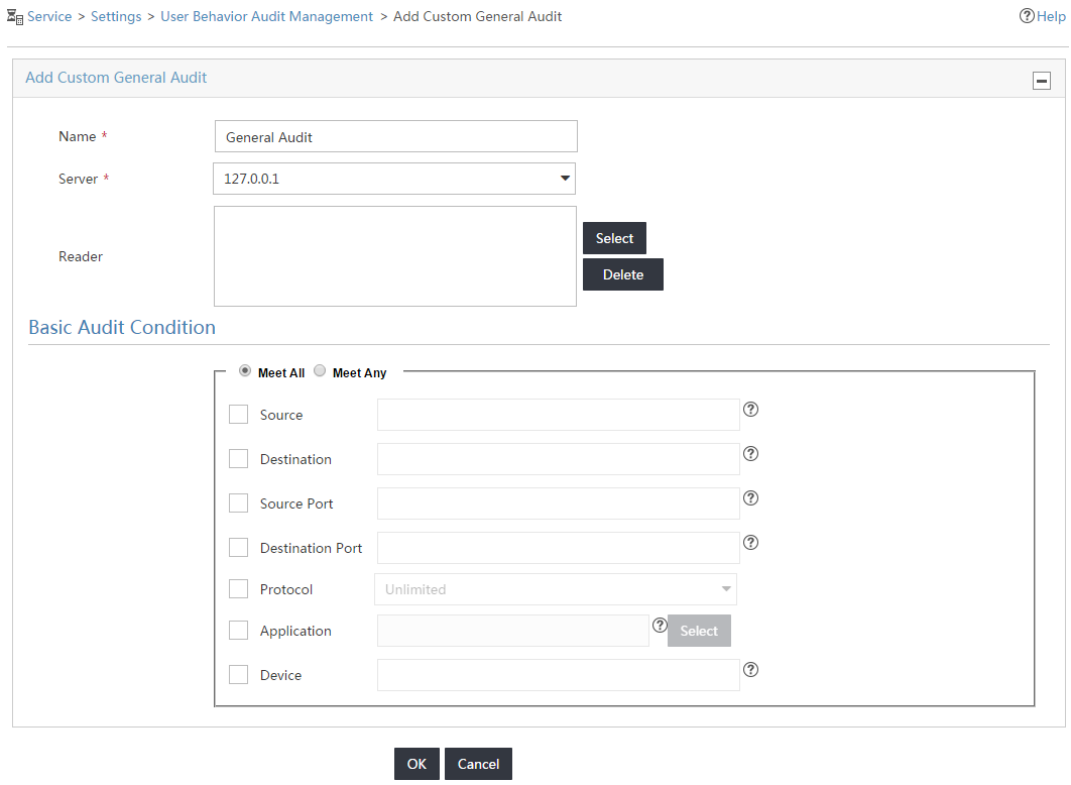
**Figure 11 Selecting an audit type**




3. Select **General Audit**, and click **Next**.

   The **Add Custom General Audit** page opens, as shown in Figure 12.

**Figure 12 Adding a custom general audit task**

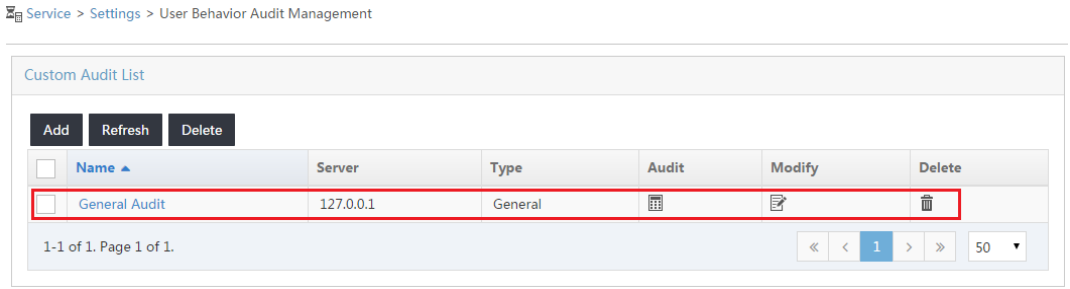


4. Enter **General Audit** in the **Name** field.
5. Select **127.0.0.1** from the **Server** list.
6. Select **Meet All** in the **Audit Condition** area.
7. Use the default settings of other parameters.
8. Click **OK**.

# Verifying the configuration (available for schemes 1, 2, and 3)

1. From the navigation tree, select **Traffic Analysis and Audit** > **General Audit**.
   The audit task **General Audit** is displayed on the **Custom Audit List** page.

   **Figure 13 Viewing the audit task**




2. Click the **Audit** icon  for **General Audit**.

It takes time to generate the result. You can see the information such as source IP addresses, destination IP addresses, source ports, and destination ports, as shown in Figure 14.

**Figure 14 Audit result page**