H3C SNMP Configuration Examples

Contents

Introduction

This document provides SNMP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

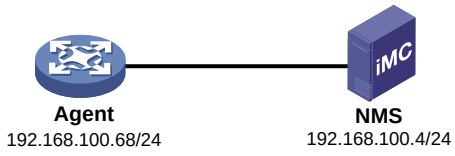
This document assumes that you have basic knowledge of SNMP.

Example: Configuring SNMPv1 or SNMPv2c

Network configuration

As shown in Figure 1, an IMC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv1/SNMPv2c to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS.

Figure 1 Network diagram



Software versions used

This configuration example was created and verified on S7500EXS-CMW710-R7536P05.

Restrictions and guidelines

When you configure SNMPv1 or SNMPv2c, follow these restrictions and guidelines:

- The configuration procedure is the same for SNMPv1 and SNMPv2c. This example uses SNMPv2c.
- For the NMS to manage the SNMP agent, the SNMP settings on the agent and the NMS must match.
- The NMS software configuration varies by vendor. This example uses IMC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.

Procedures

Configuring the SNMP agent

Specify SNMPv2c, and create read-only community **readtest** and read and write community **writetest**.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

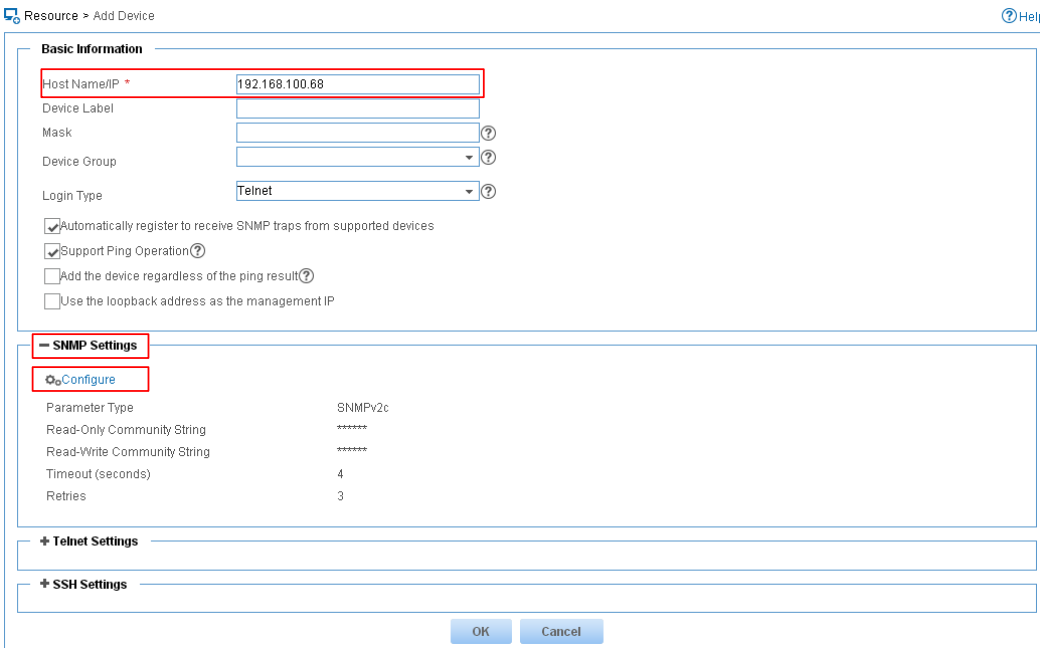
Enable SNMP notifications and configure the agent to send SNMP notifications to the NMS at 192.168.100.4 by using community name **traptest**.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname traptest
```

Configuring the NMS

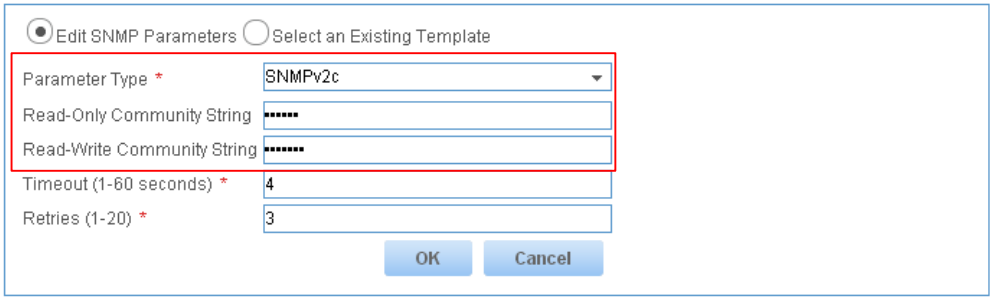
1. Add the device (SNMP agent) to IMC:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Resource Management** > **Add Device**.
   c. On the **Add Device** page, configure the following parameters:
      – Enter **192.168.100.68** in the **Host Name/IP** field.
      – Use the default values for other parameters.

Figure 2 Adding a device



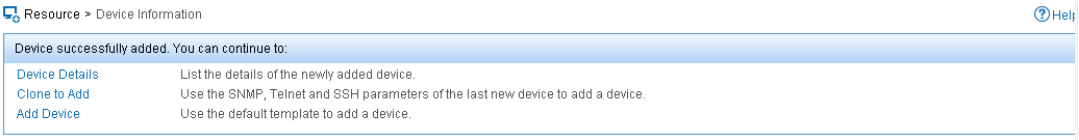
2. Configure SNMP parameters:
   a. Expand the **SNMP Settings** area.
   b. Click **Configure**.
   c. On the page that appears, configure the following parameters:
      – Select **SNMPv2c** from the **Parameter Type** list.
      – Enter **readtest** in the **Read-Only Community String** field.
      – Enter **writetest** in the **Read-Write Community String** field.
      – Use the default values for other parameters.
      – Click **OK**.

   Figure 3 Editing SNMP parameters



3. On the **Add Device** page, click **OK**.
   The device is successfully added to IMC, as shown in Figure 4.

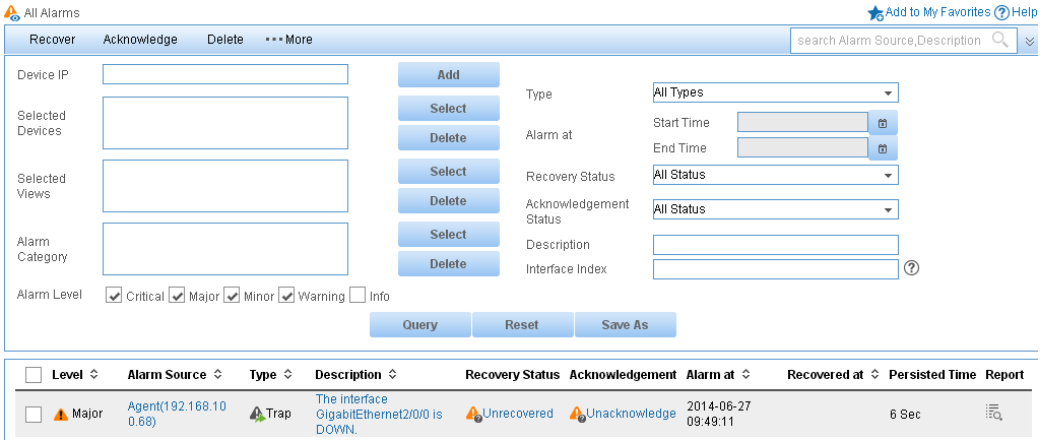
   Figure 4 Device added



Verifying the configuration

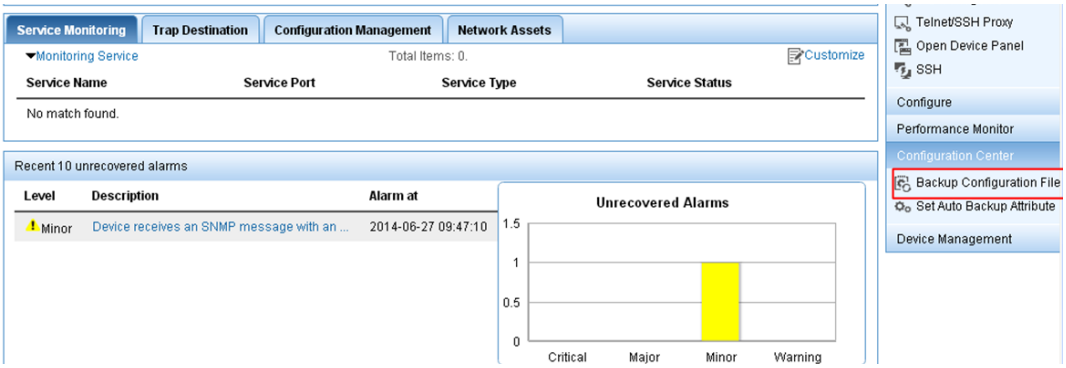
1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
   a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
   b. Click the **Alarm** tab.
   c. From the navigation tree, select **Alarm Browse** > **All Alarms**.
      You can see the alarms in Figure 5.

Figure 5 All Alarms page



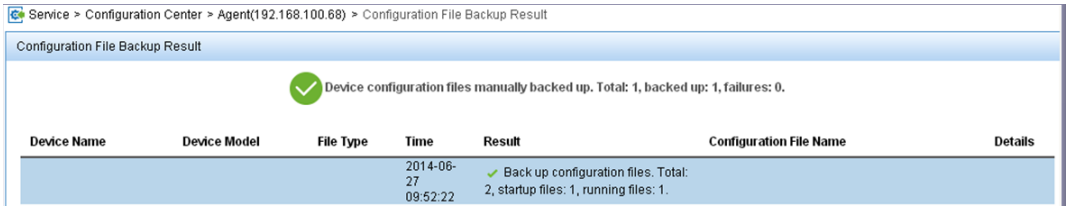
2. Back up the agent configuration file on the NMS:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Device View**.
   c. On the page that appears, click the device label link **Agent(192.168.100.68)**.
   d. On the **Configuration Center** menu, select **Backup Configuration File**.

Figure 6 Backing up the configuration file



The configuration file is backed up, as shown in Figure 7.

Figure 7 Configuration file backed up



Configuration files

```
#
 snmp-agent
 snmp-agent community write writetest
 snmp-agent community read readtest
```

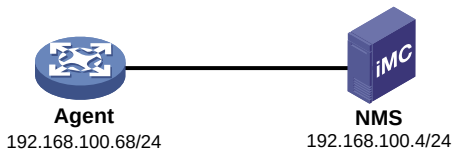
```
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v2c
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname traptest
#
```

Example: Configuring SNMPv3

Network configuration

As shown in Figure 8, an IMC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv3 to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS. The NMS and the agent use the authentication with privacy security model.

Figure 8 Network diagram



Software versions used

This configuration example was created and verified on S7500EXS-CMW710-R7536P05.

Restrictions and guidelines

When you configure SNMPv3, follow these restrictions and guidelines:

- SNMPv3 supports VACM and RBAC access control modes. This example provides SNMPv3 configuration procedures in both modes. See "Configuring SNMPv3 in RBAC mode on the agent" and "Configuring SNMPv3 in VACM mode on the agent".
- For the NMS to manage the SNMP agent, make sure the SNMP settings on the agent and the NMS are the same.
- The NMS software configuration varies by vendor. This example uses IMC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.
- When configuring the notification target host, use an existing SNMPv3 username as the security parameter and make sure the agent and NMS use the same security model.

Procedures

Configuring SNMPv3 in RBAC mode on the agent

Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

Create user role **test**, and assign **test** read and write access to the objects under the **internet** subtree (OID: 1.3.6.1).

```
[Agent] role name test
[Agent-role-test] rule 1 permit read write oid 1.3.6.1
[Agent-role-test] quit
```

Create SNMPv3 user **managev3user**. Assign user role **test** to **managev3user.** Set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encryption key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 managev3user user-role test simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

Configure the SNMP agent to send SNMP notifications to the NMS at **192.168.100.4** by using username **managev3user**.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

Configuring SNMPv3 in VACM mode on the agent

Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

Include the **mib-2** (OID 1.3.6.1) subtree in the **mibtest** view.

```
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```

Create SNMPv3 group **managev3group**, and specify the authentication with privacy security model for the group. Assign the group read, write, and notification accesses to the **mibtest** view.

```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view mibtest
```

Add user **managev3user** to SNMPv3 group **managev3group**, and set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encryption key to **123456TESTencr&!.**

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

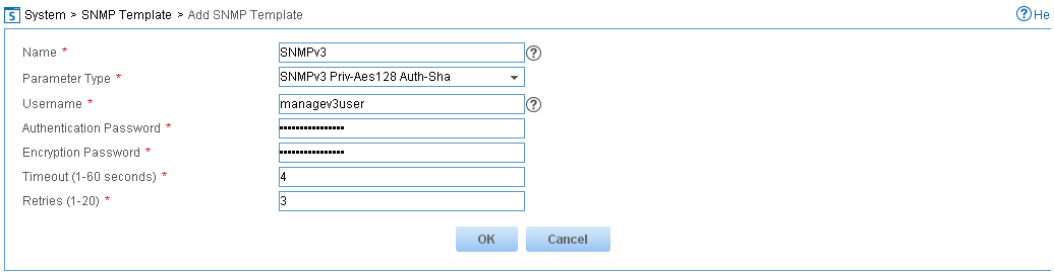
Configure the SNMP agent to send SNMP notifications to NMS at **192.168.100.4** by using username **managev3user**.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

Configuring the NMS

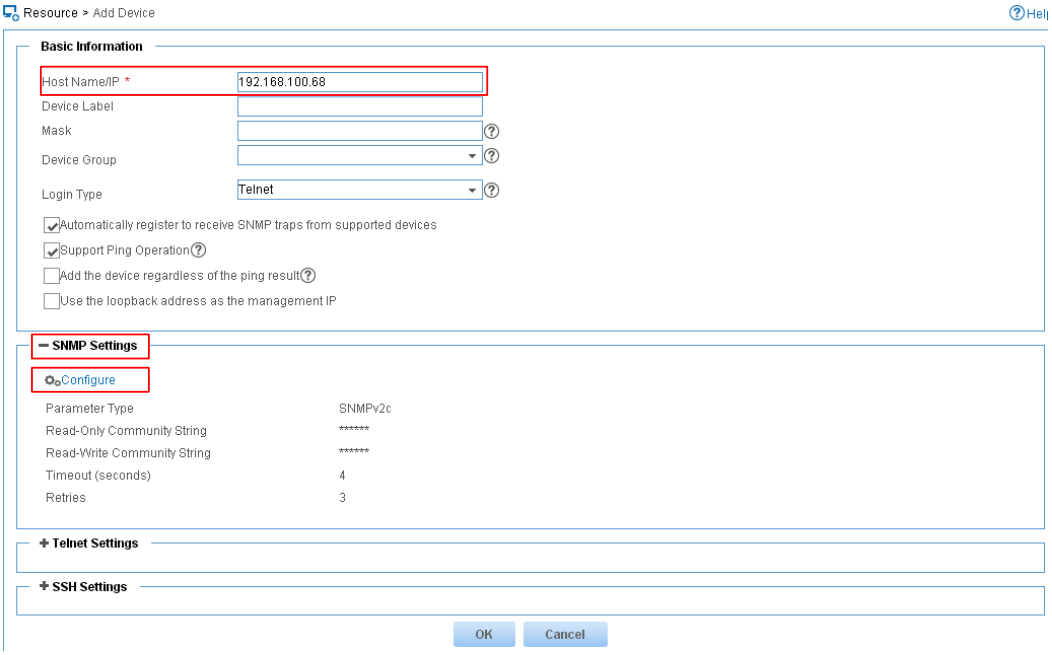
1. Add an SNMP template:
   a. Click the **System** tab.
   b. From the navigation tree, select **Resource Management** > **SNMP Template**.
   c. On the **SNMP Template** page, click **Add**.
   d. On the **Add SNMP Template** page, configure the following parameters:
      – Enter **SNMPv3** in the **Name** field.
      – Select **SNMPv3 Priv-Aes128 Auth-Sha** from the **Parameter Type** list.
      – Enter **managev3user** in the **Username** field.
      – Enter **123456TESTauth&!** in the **Authentication Password** field.
      – Enter **123456TESTencr&!** in the **Encryption Password** field.
      – Use the default values for other parameters.
      – Click **OK**.

   Figure 9 Adding an SNMP template



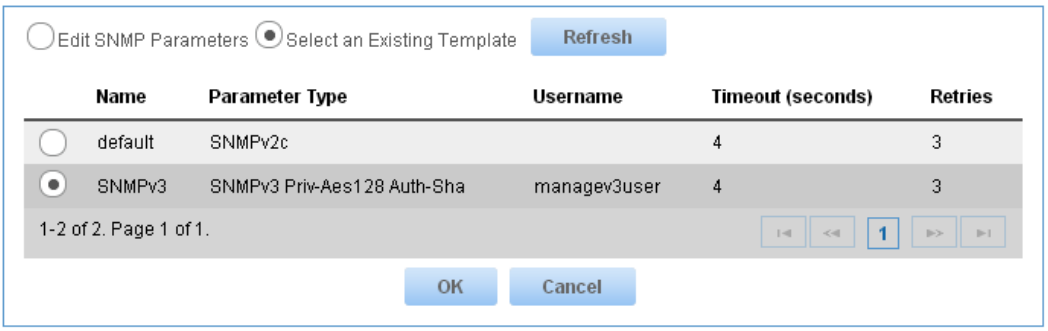
2. Add the device (SNMP agent) to IMC:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Resource Management** > **Add Device**.
   c. On the **Add Device** page, configure the following parameters:
      – Enter **192.168.100.68** in the **Host Name/IP** field.
      – Use the default values for other parameters.

Figure 10 Adding a device



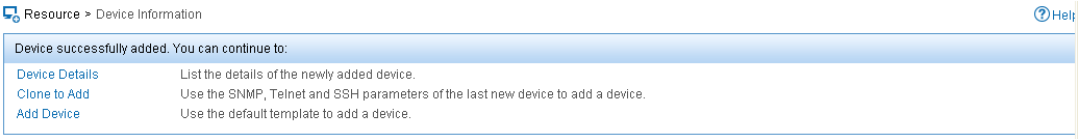
3. Configure SNMP parameters:
   a. Expand the **SNMP Settings** area.
   b. Click **Configure**.
   c. Select the **Select an Existing Template** option.
   d. Select template name **SNMPv3**.
   e. Click **OK**.

Figure 11 Selecting an existing template



4. On the **Add Device** page, click **OK**.
   The device is successfully added to IMC, as shown in Figure 12.

Figure 12 Device added

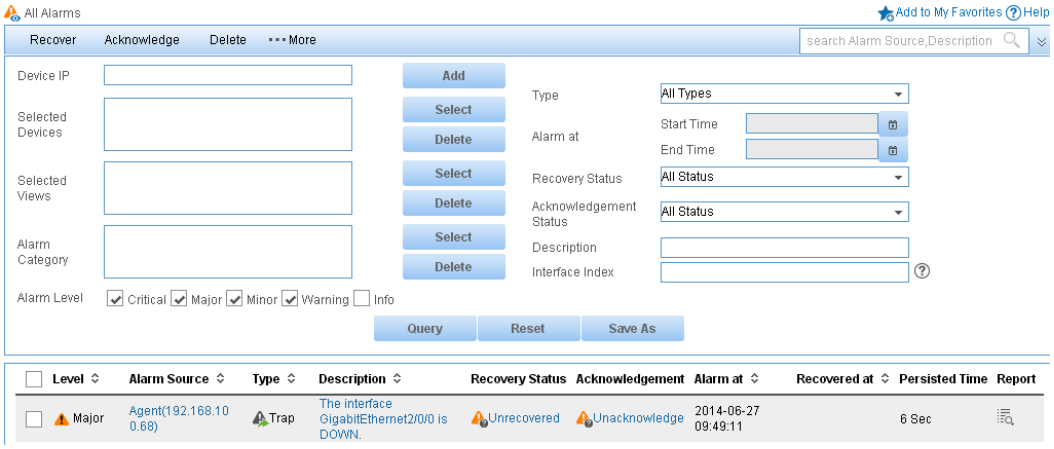


Verifying the configuration

1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
   a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
   b. Click the **Alarm** tab.
   c. From the navigation tree, select **Alarm Browse** > **All Alarms**.

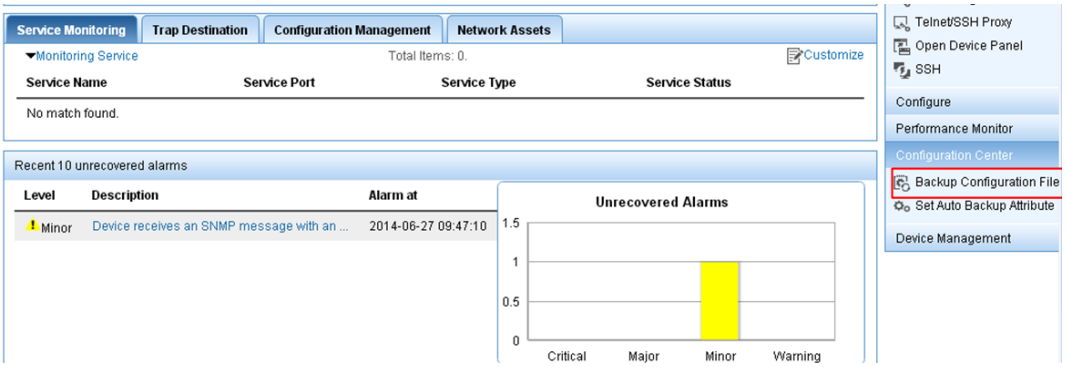
      You can see the alarms in Figure 13.

      Figure 13 All Alarms page



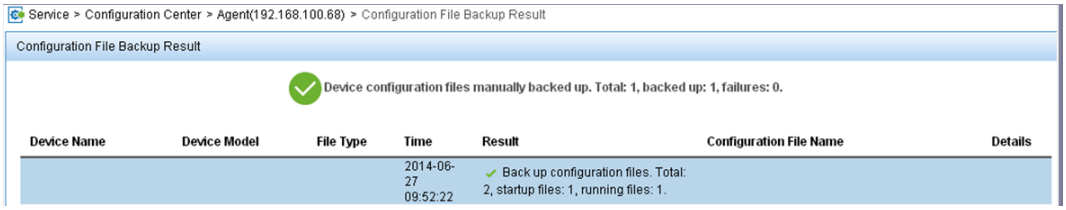
2. Back up the agent configuration file on the NMS:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Device View**.
   c. On the page that appears, click the device label link **Agent(192.168.100.68)**.
   d. On the **Configuration Center** menu, select **Backup Configuration File**.

      Figure 14 Backing up the configuration file



      The configuration file is backed up, as shown in Figure 15.

Figure 15 Configuration file backed up



Configuration files

SNMPv3 configuration in RBAC mode

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user user-role test cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
role name test
 rule 1 permit read oid 1.3.6.1
#
```

SNMPv3 configuration in VACM mode

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest
notify-view mibtest
 snmp-agent mib-view included mibtest internet
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
```

Related documentation

- *H3C S7500E-XS Switch Series Network Management and Monitoring Configuration Guide-R7536P05*
- *H3C S7500E-XS Switch Series Network Management and Monitoring Command Reference-R7536P05*