[iMC] Device receives an SNMP message with an erroneous community string

PLAT SNMP **Liangjinbao** 2022-09-27 14:12:20 Published

Network Topology

irrelevant

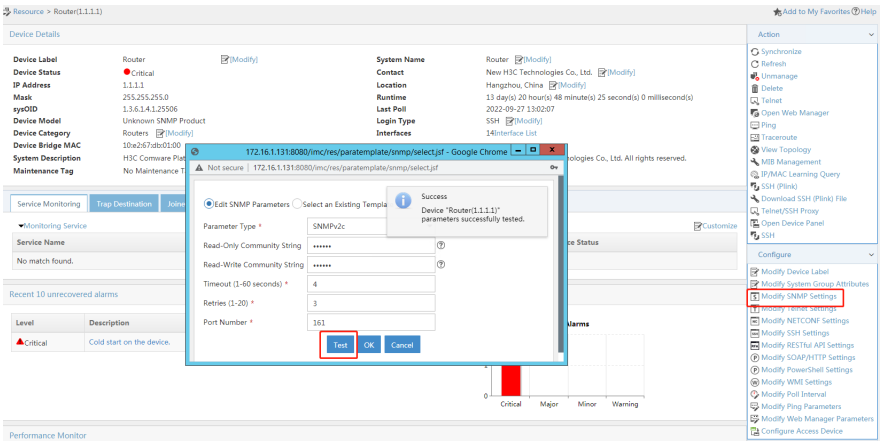
Problem Description

- The IMC receives the following alarm all the time

Trap Name	Authentication Failure
Trap OID	1.3.6.1.6.3.1.1.5.5
Enterprise Name	SNMP
Enterprise ID	1.3.6.1.6.3.1.1.5
Trap Level	Minor
Description	Device receives an SNMP message with an erroneous community string
Trap Cause	SNMP agent receives an SNMP message with an erroneous community string.
Remediation Suggestion	Check if: 1. There are hacker attacks on the network. 2. The SNMP community string is inconsistent with that in the NMS.
Maintenance Experience	

Process Analysis

1.Check whether the SNMP of devices managed by the IMC is correct

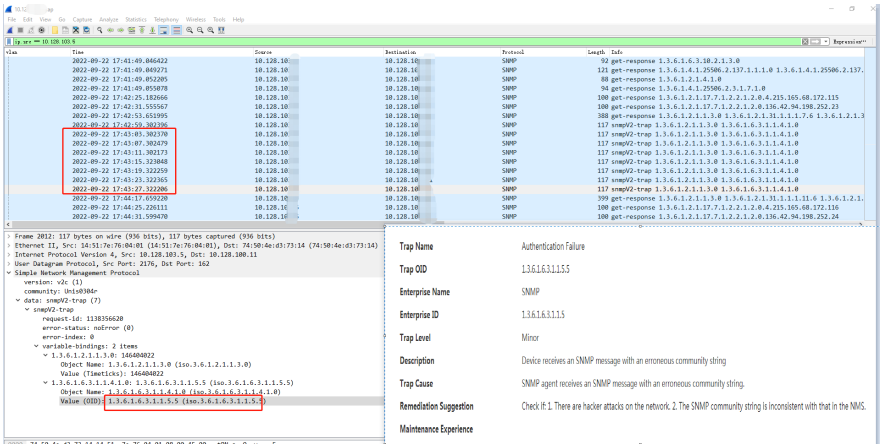


2.Capture packets on the IMC server and check whether a trap 1.3.6.1.6.3.1.1.5.5 is received

2.1 if your iMC installed on a linux OS, you can using this command to capture packets

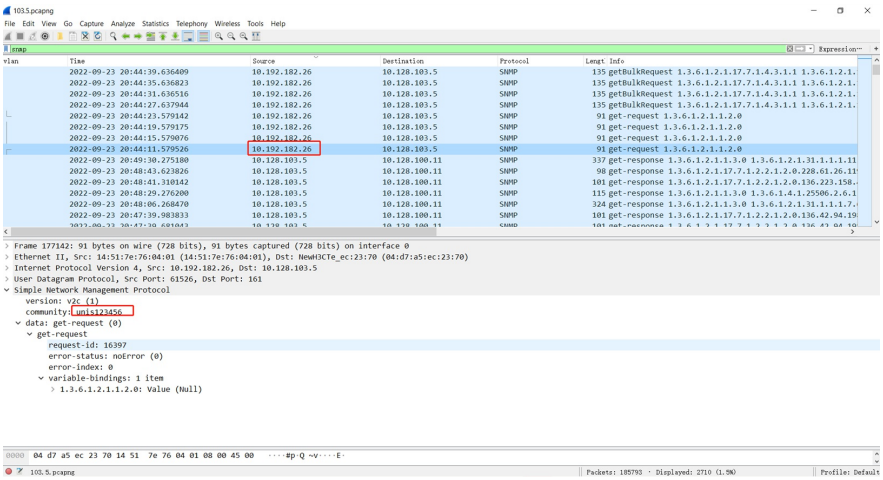
tcpdump -i bond0 host 10.128.x.x and port 161 or port 162 -w /home/xx.cap

We found that iMC received trap from device.



3.Capture packets on the device and check whether another NMS system polling device wit h wrong community.

we found that 10.192.182.26 is polling with wrong community.



Solution

Check the source of abnormal NMS in the network, and complete the overall planning and deployment of the NMS system.