

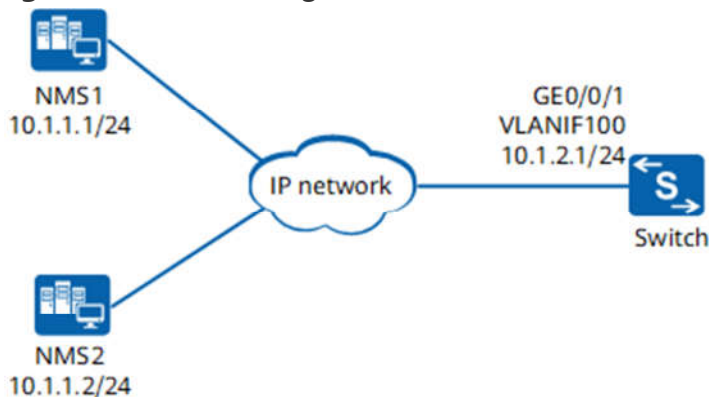
Configurando o switch para se comunicar com o NMS através do SNMPv3

Requerimentos de Rede

Na rede mostrada na Figura 1, NMS1 e NMS2 gerenciam dispositivos na rede. A rede é grande e insegura. Portanto, os dispositivos na rede usam SNMPv3 para se comunicar com os NMSs e a autenticação e a criptografia são configuradas para aumentar a segurança. Um novo switch é implantado na rede e precisa ser gerenciado pelo NMS2.

Os usuários desejam gerenciar o switch usando os recursos de rede existentes e esperam que as falhas no switch possam ser rapidamente identificadas e corrigidas.

Figura 1 Switch configurado com o SNMPv3



Roteiro de Configuração

Como a rede é grande e insegura, o novo switch ainda usa SNMPv3. Para reduzir as cargas nos NMSs, configure o NMS2 para gerenciar o switch e o NMS1 para não gerenciar o switch.

O roteiro de configuração é conforme a seguir:

1. Configure a versão SNMP no switch para SNMPv3.
2. Configure o direito de acesso para permitir que o NMS2 gerencie objetos ISO no switch.

3. Configure o host de trap para o switch para entregar os traps gerados no switch para NMS2. Para ajudar a identificar rapidamente as falhas de acordo com as mensagens de trap e reduzir os traps inúteis, configure o switch para enviar apenas os traps dos módulos habilitados por padrão.
4. Configure as informações de contato do administrador na central para que os usuários possam contatar o administrador rapidamente quando ocorrer uma falha na central.
5. Configurar NMS2.

Procedimento

1. Configure um endereço IP para uma interface do switch para fornecer uma rota acessível entre o NMS e o switch.

Configure um endereço IP para uma interface do switch de acordo com a Figura 1.

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type hybrid
[Switch-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 100
[Switch-Vlanif100] ip address 10.1.2.1 24
[Switch-Vlanif100] quit
```

2. Configure a interface para receber e responder aos pacotes de solicitação de NMS no switch.

```
[Switch] snmp-agent protocol source-interface vlanif 100
```

3. Defina a versão SNMP na chave para SNMPv3.

```
[Switch] snmp-agent sys-info version v3
```

4. Configure os direitos de acesso.

Configure uma ACL que permita que o NMS2 gerencie o switch e evite que o NMS1 gerencie o switch.

```
[Switch] acl 2001
[Switch-acl-basic-2001] rule 5 permit source 10.1.1.2 0.0.0.0
[Switch-acl-basic-2001] rule 6 deny source 10.1.1.1 0.0.0.0
[Switch-acl-basic-2001] quit
```

Configure a visualização MIB.

```
[Switch] snmp-agent mib-view included isoview iso
```

Configure o grupo de usuários.

```
[Switch] snmp-agent group v3 admin privacy read-view isoview write-view isoview  
notify-view isoview acl 2001
```

Configure o usuário.

```
[Switch] snmp-agent usm-user v3 nms2-admin group admin
```

Configure a autenticação de pacotes do usuário e defina a senha de autenticação para Authe@1234.

```
[Switch] snmp-agent usm-user v3 nms2-admin authentication-mode sha2-256
```

Please configure the authentication password (8-64)

Enter Password: //Enter the authentication password. It is
Authe@1234 in this example.

Confirm Password: //Confirm the password. It is Authe@1234 in this
example.

Configure a criptografia de pacotes do usuário e defina a senha de criptografia para Priva@1234.

```
[Switch] snmp-agent usm-user v3 nms2-admin privacy-mode aes128
```

Please configure the privacy password (8-64)

Enter Password: //Enter the encryption password. It is Priva@1234
in this example.

Confirm Password: //Confirm the password. It is Priva@1234 in this
example.

5. Configure o host para o qual devem ser enviados traps.

```
[Switch] snmp-agent target-host trap address udp-domain 10.1.1.2 params  
securityname nms2-admin v3 privacy
```

6. Configure as informações de contato do administrador.

```
[Switch] snmp-agent sys-info contact call Operator at 010-12345678
```

7. Configure o NMS2.

Em um NMS executando SNMPv3, você deve definir um nome de usuário e selecionar um nível de segurança. Em seguida, defina o modo de autenticação, a senha de autenticação, o modo de criptografia e a senha de criptografia de acordo com o nível de segurança selecionado. Para obter detalhes sobre a configuração do NMS, consulte o manual do NMS.

NOTE

A configuração do parâmetro de autenticação no NMS deve ser igual à do switch. Caso contrário, o NMS não pode gerenciar o switch.

8. Verifique a configuração.

Depois de concluir a configuração, execute os seguintes comandos para verificar se as configurações entraram em vigor.

Visualize a versão SNMP.

```
[Switch] display snmp-agent sys-info version
SNMP version running in the system:
    Polling: SNMPv1:disable, SNMPv2c:disable, SNMPv3:enable
    Trap   : SNMPv1:disable, SNMPv2c:disable, SNMPv3:enable
```

Ver informações do grupo de usuários.

```
[Switch] display snmp-agent group admin
Group name: admin
    Security model: v3 AuthPriv
    Readview: ViewDefault
    Writeview: isoview
    Notifyview :<no specified>
    Storage-type: nonVolatile
    Acl:2001
```

Ver informações da MIB.

```
[Switch] display snmp-agent mib-view viewname isoview
View name:isoview
    MIB Subtree:iso
    Subtree mask:FC (Hex)
    Storage-type: nonVolatile
    View Type:included
    View status:active
```

Ver a configuração do host para o qual são enviados traps.

```
[Switch] display snmp-agent target-host
Target-host NO. 1
```

```
-----
IP-address   : 10.1.1.2
Domain       : -
Source interface : -
VPN instance : -
Security name : nms2-admin
Port         : 162
Type         : trap
Version      : v3
Level        : Privacy
NMS type     : NMS
With ext-vb  : No
-----
```

Ver as informações de contato do administrador.

```
[Switch] display snmp-agent sys-info contact
The contact person for this managed node:
    call Operator at 010-12345678
```

Arquivos de Configuração

Arquivo de configuração do Switch

```
#
sysname Switch
#
vlan batch 100
#
acl number 2001
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
#
interface Vlanif100
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
snmp-agent
snmp-agent local-engineid 800007DB0300259E0370C3
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v3
snmp-agent group v3 admin privacy read-view isoview write-view isoview notify-view
isoview acl 2001
snmp-agent target-host trap address udp-domain 10.1.1.2 params securityname nms2-
admin v3 privacy
snmp-agent mib-view included isoview iso
snmp-agent usm-user v3 nms2-admin
snmp-agent usm-user v3 nms2-admin group admin
snmp-agent usm-user v3 nms2-admin authentication-mode sha2-256 cipher
%^%#odaJ7R)/O7k$pwQx0qfD0\`u*'GI1(|;ZQXHzrN%^%#
snmp-agent usm-user v3 nms2-admin privacy-mode aes128 cipher
%^%#f*K3/|E6d"SJes9)5naXPIqCTpR"}BUC=yW;!(f9%^%#
snmp-agent protocol source-interface Vlanif100
#
return
```