Gerenciar SNMP (somente administradores de cluster)

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciar SNMP (somente administradores de cluster) 1
Visão geral da SNMP 1
Crie uma comunidade SNMP e atribua-a a um LIF 2
Configure SNMPv3 usuários em um cluster 5
Configure os traphosts para receber notificações SNMP 8
Teste a polling SNMP 9
Comandos para gerenciar SNMP 11

Gerenciar SNMP (somente administradores de cluster)

Visão geral da SNMP

Você pode configurar o SNMP para monitorar SVMs em seu cluster para evitar problemas antes que eles ocorram e responder a problemas se eles ocorrerem. O gerenciamento do SNMP envolve a configuração de usuários SNMP e a configuração de destinos de host SNMP (estações de trabalho de gerenciamento) para todos os eventos SNMP. O SNMP está desativado por padrão em LIFs de dados.

Você pode criar e gerenciar usuários SNMP somente leitura no data SVM. As LIFs de dados devem ser configuradas para receber solicitações SNMP no SVM.

As estações de trabalho de gerenciamento de rede SNMP, ou gerentes, podem consultar o agente SNMP SVM para obter informações. O agente SNMP reúne informações e as encaminha para os gerentes SNMP. O agente SNMP também gera notificações de intercetação sempre que ocorrem eventos específicos. O agente SNMP no SVM tem Privileges somente leitura; ele não pode ser usado para nenhuma operação definida ou para tomar uma ação corretiva em resposta a uma armadilha. O ONTAP fornece um agente SNMP compatível com as versões v1, v2c e v3 do SNMP. O SNMPv3 oferece segurança avançada usando senhas e criptografia.

Para obter mais informações sobre o suporte SNMP em sistemas ONTAP, "TR-4220: Suporte SNMP no Data ONTAP" consulte .

Visão geral da MIB

Um MIB (Management Information base) é um arquivo de texto que descreve objetos e traps SNMP.

As MIBs descrevem a estrutura dos dados de gerenciamento do sistema de armazenamento e usam um namespace hierárquico contendo identificadores de objeto (OIDs). Cada OID identifica uma variável que pode ser lida usando SNMP.

Como MIBs não são arquivos de configuração e o ONTAP não lê esses arquivos, a funcionalidade SNMP não é afetada por MIBs. O ONTAP fornece o seguinte arquivo MIB:

- Um MIB personalizado NetApp (`netapp.mib`)

O ONTAP suporta MIBs IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), que mostram dados IPv4 e IPv6, são suportados.

O ONTAP também fornece uma breve referência cruzada entre identificadores de objeto (OIDs) e nomes curtos de objetos no `traps.dat` arquivo.

> As versões mais recentes dos arquivos MIBs ONTAP e 'traps.dat' estão disponíveis no site de suporte da NetApp. No entanto, as versões desses arquivos no site de suporte não correspondem necessariamente aos recursos SNMP de sua versão do ONTAP. Esses arquivos são fornecidos para ajudá-lo a avaliar os recursos SNMP na versão mais recente do ONTAP.

Traps SNMP

Os traps SNMP capturam informações de monitoramento do sistema que são enviadas como uma notificação assíncrona do agente SNMP para o gerenciador SNMP.

Existem três tipos de traps SNMP: Padrão, embutido e definido pelo usuário. Os traps definidos pelo usuário não são suportados no ONTAP.

Uma armadilha pode ser usada para verificar periodicamente se há limites operacionais ou falhas que são definidos na MIB. Se um limite for atingido ou uma falha for detetada, o agente SNMP enviará uma mensagem (trap) aos hosts que os alertam sobre o evento.

ONTAP suporta SNMPv1 armadilhas e, olhando em ONTAP 9.1, SNMPv3 armadilhas. ONTAP não suporta SNMPv2c armadilhas e informa.

Traps SNMP padrão

Esses traps são definidos no RFC 1215. Existem cinco traps SNMP padrão que são suportados pelo ONTAP: Coldstart, warmStart, linkDown, linkup e autenticationFailure.

A armadilha autenticationFailure é desativada por padrão. Você deve usar o `system snmp authtrap` comando para ativar a armadilha. Para obter mais informações, consulte as páginas de manual: "Referência do comando ONTAP"

Traps SNMP incorporados

Os traps incorporados são predefinidos no ONTAP e são enviados automaticamente para as estações de gerenciamento de rede na lista de traphost se ocorrer um evento. Essas armadilhas, como diskFailedShutdown, cpuTooBusy e volumeNearlyFull, são definidas no MIB personalizado.

Cada armadilha incorporada é identificada por um código de armadilha exclusivo.

Crie uma comunidade SNMP e atribua-a a um LIF

Você pode criar uma comunidade SNMP que atua como um mecanismo de autenticação entre a estação de gerenciamento e a máquina virtual de armazenamento (SVM) ao usar SNMPv1 e SNMPv2c.

Ao criar comunidades SNMP em um SVM de dados, você pode executar comandos como `snmpwalk` e `snmpget` nas LIFs de dados.

Sobre esta tarefa

- Em novas instalações do ONTAP, o SNMPv1 e o SNMPv2c são desativados por padrão.

  SNMPv1 e SNMPv2c são ativados depois de criar uma comunidade SNMP.

- O ONTAP suporta comunidades somente leitura.
- Por padrão, a política de firewall de "dados" atribuída a LIFs de dados tem serviço SNMP definido como `deny`.

  Você deve criar uma nova política de firewall com serviço SNMP definido como `allow` ao criar um usuário

SNMP para um SVM de dados.

> A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- Você pode criar comunidades SNMP para usuários SNMPv1 e SNMPv2c para o SVM admin e o SVM de dados.
- Como um SVM não faz parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Passos

1. Crie uma comunidade SNMP usando o `system snmp community add` comando. O comando a seguir mostra como criar uma comunidade SNMP no cluster SVM admin-1:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

O comando a seguir mostra como criar uma comunidade SNMP nos dados SVM VS1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verifique se as comunidades foram criadas usando o comando system snmp Community show.

O comando a seguir mostra as duas comunidades criadas para SNMPv1 e SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Verifique se o SNMP é permitido como um serviço na política de firewall de "dados" usando o `system services firewall policy show` comando.

O comando a seguir mostra que o serviço snmp não é permitido na política de firewall "dados" padrão (o serviço snmp é permitido somente na política de firewall "mgmt"):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Crie uma nova política de firewall que permita o acesso usando `snmp` o serviço usando o `system services firewall policy create` comando.

   Os comandos a seguir criam uma nova política de firewall de dados chamada "data1" que permite o. `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Aplique a política de firewall a um LIF de dados usando o comando 'Network Interface Modify' com o parâmetro -firewall-policy.

O comando a seguir atribui a nova política de firewall "data1" ao LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Configure SNMPv3 usuários em um cluster

O SNMPv3 é um protocolo seguro quando comparado ao SNMPv1 e ao SNMPv2c. Para utilizar o SNMPv3, tem de configurar um utilizador SNMPv3 para executar os utilitários SNMP a partir do gestor SNMP.

Passo

Use o "security login create command" para criar um usuário SNMPv3.

Você é solicitado a fornecer as seguintes informações:

- ID do motor: O valor predefinido e recomendado é ID do motor local
- Protocolo de autenticação
- Palavra-passe de autenticação
- Protocolo de privacidade
- Senha do protocolo de privacidade

Resultado

O utilizador SNMPv3 pode iniciar sessão a partir do gestor SNMP utilizando o nome de utilizador e a palavra-passe e executar os comandos do utilitário SNMP.

SNMPv3 parâmetros de segurança

O SNMPv3 inclui um recurso de autenticação que, quando selecionado, exige que os usuários digitem seus nomes, um protocolo de autenticação, uma chave de autenticação e seu nível de segurança desejado ao invocar um comando.

A tabela a seguir lista os parâmetros de segurança SNMPv3 :

Parâmetro	Opção de linha de comando	Descrição
EngineID	-E EngineID	ID do motor do agente SNMP. O valor padrão é local EngineID (recomendado).
SecurityName	-U Nome	O nome de utilizador não deve exceder 32 carateres.
AuthProtocol	-A [none	MD5
SHA	SHA-256]	O tipo de autenticação pode ser None, MD5, SHA ou SHA-256.

Authkey	-UMA FRASE-PASSE	Frase-passe com um mínimo de oito carateres.
Segurançanível	-L [authNoPriv	authPriv
noAuthNoPriv]	O nível de segurança pode ser Autenticação, sem Privacidade; Autenticação, Privacidade; ou sem Autenticação, sem Privacidade.	PrivProtocol
aes128	O protocolo de privacidade pode ser nenhum, des ou AES128	PrivPassword

Exemplos para diferentes níveis de segurança

Este exemplo mostra como um usuário SNMPv3 criado com diferentes níveis de segurança pode usar os comandos do lado do cliente SNMP, como `snmpwalk`, para consultar os objetos do cluster.

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

Você deve usar `snmpwalk` 5.3.1 ou posterior quando o protocolo de autenticação for SHA.

Nível de segurança: AuthPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Modo FIPS

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: AuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança authNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade. Como resultado, não é possível configurar um usuário authNoPriv SNMPv3 no modo FIPS.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único

objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nível de segurança: NoAuthNoPriv

A saída a seguir mostra a criação de um usuário SNMPv3 com o nível de segurança noAuthNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Modo FIPS

O FIPS não permite que você escolha **nenhum** para o protocolo de privacidade.

Teste de Snmpwalk

A saída a seguir mostra o usuário SNMPv3 executando o comando snmpwalk:

Para um melhor desempenho, você deve recuperar todos os objetos em uma tabela em vez de um único objeto ou alguns objetos da tabela.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configure os traphosts para receber notificações SNMP

Você pode configurar o traphost (gerenciador SNMP) para receber notificações (PDUs de intercetação SNMP) quando os traps SNMP são gerados no cluster. Você pode especificar o nome do host ou o endereço IP (IPv4 ou IPv6) do traphost SNMP.

Antes de começar

- Os traps SNMP e SNMP devem estar ativados no cluster.

> As traps SNMP e SNMP estão ativadas por predefinição.

- O DNS deve ser configurado no cluster para resolver os nomes do traphost.
- O IPv6 deve estar ativado no cluster para configurar os traphosts SNMP usando endereços IPv6.
- Para o ONTAP 9.1 e versões posteriores, você deve ter especificado a autenticação de um modelo de segurança baseado no usuário predefinido (USM) e credenciais de privacidade ao criar traphosts.

Passo

Adicionar um traphost SNMP:

```
system snmp traphost add
```

> Os traps só podem ser enviados quando pelo menos uma estação de gerenciamento SNMP é especificada como um traphost.

O comando a seguir adiciona um novo host SNMPv3 chamado yyy.example.com com um usuário USM conhecido:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

O comando a seguir adiciona um traphost usando o endereço IPv6 do host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Teste a polling SNMP

Depois de configurar o SNMP, você deve verificar se você pode poll o cluster.

Sobre esta tarefa

Para fazer polling de um cluster, você precisa usar um comando de terceiros, `snmpwalk` como o .

Passos

1. Envie um comando SNMP para poll o cluster a partir de um cluster diferente.

   Para sistemas que executam o SNMPv1, use o comando CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

   Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

Para sistemas que executam o SNMPv2c, use o comando CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Para sistemas que executam o SNMPv3, use o comando CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` para descobrir o conteúdo do MIB (Management Information base).

Neste exemplo, o endereço IP do LIF de gerenciamento de cluster que você está polling é 10.11.12.123. O comando exibe as informações solicitadas do MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Comandos para gerenciar SNMP

Você pode usar os `system snmp` comandos para gerenciar SNMP, traps e traphosts. Você pode usar os `security` comandos para gerenciar usuários SNMP por SVM. Você pode usar os `event` comandos para gerenciar eventos relacionados a traps SNMP.

Comandos para configurar o SNMP

Se você quiser…	Use este comando…
Ative o SNMP no cluster	`options -option-name snmp.enable -option-value on` O serviço SNMP tem de ser permitido na política de firewall de gestão (mgmt). Você pode verificar se o SNMP é permitido usando o comando show de política de firewall de serviços do sistema.
Desative o SNMP no cluster	`options -option-name snmp.enable -option-value off`

Comandos para gerenciar usuários SNMP v1, v2c e v3

Se você quiser…	Use este comando…
Configurar utilizadores SNMP	`security login create`
Exibir usuários SNMP	`security snmpusers and security login show -application snmp`
Eliminar utilizadores SNMP	`security login delete`

Modifique o nome da função de controle de acesso de um método de login para usuários SNMP	`security login modify`

Comandos para fornecer informações de Contato e localização

Se você quiser…	Use este comando…
Apresentar ou modificar os detalhes de contacto do cluster	`system snmp contact`
Exiba ou modifique os detalhes de localização do cluster	`system snmp location`

Comandos para gerenciar comunidades SNMP

Se você quiser…	Use este comando…
Adicione uma comunidade somente leitura (ro) para um SVM ou para todos os SVMs no cluster	`system snmp community add`
Exclua uma comunidade ou todas as comunidades	`system snmp community delete`
Exiba a lista de todas as comunidades	`system snmp community show`

Como os SVMs não fazem parte do padrão SNMP, as consultas sobre LIFs de dados devem incluir o OID raiz do NetApp (1,3.6,1.4,1.789), por exemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando para exibir valores de opção SNMP

Se você quiser…	Use este comando…
Exiba os valores atuais de todas as opções SNMP, incluindo Contato de cluster, localização de Contato, se o cluster está configurado para enviar traps, a lista de traphosts e lista de comunidades e tipo de controle de acesso	`system snmp show`

Comandos para gerenciar traps e traphosts SNMP

Se você quiser…	Use este comando…
Ativar traps SNMP enviados a partir do cluster	`system snmp init -init 1`
Desative traps SNMP enviados a partir do cluster	`system snmp init -init 0`

Adicione um traphost que receba notificações SNMP para eventos específicos no cluster	`system snmp traphost add`
Excluir um traphost	`system snmp traphost delete`
Exibir a lista de hosts	`system snmp traphost show`

Comandos para gerenciar eventos relacionados a traps SNMP

Se você quiser…	Use este comando…
Exibir os eventos para os quais são gerados traps SNMP (internos)	`event route show` Utilize o `-snmp-support true` parâmetro para visualizar apenas eventos relacionados com SNMP. Use o `instance -messagename <message>` parâmetro para exibir uma descrição detalhada do motivo pelo qual um evento pode ter ocorrido e qualquer ação corretiva. O roteamento de eventos individuais de intercetação SNMP para destinos específicos de traphost não é suportado. Todos os eventos de intercetação SNMP são enviados para todos os destinos de traphost.
Exibir uma lista de Registros de histórico de trap SNMP, que são notificações de eventos que foram enviadas para traps SNMP	`event snmphistory show`
Eliminar um registo de histórico de trap SNMP	`event snmphistory delete`

Para obter mais informações sobre os `system snmp` comandos , `security` e `event` , consulte "Referência do comando ONTAP".

Informações sobre direitos autorais

Informações sobre marcas comerciais