Utilize a monitorização SNMP

StorageGRID

NetApp
March 12, 2025

Índice

Utilize a monitorização SNMP

Usar monitoramento SNMP: Visão geral

Se você quiser monitorar o StorageGRID usando o Protocolo de Gerenciamento de rede simples (SNMP), configure o agente SNMP incluído no StorageGRID.

- "Configure o agente SNMP"
- "Atualize o agente SNMP"

Recursos

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB do StorageGRID contém definições de tabela e notificação para alertas e alarmes. O MIB também contém informações de descrição do sistema, como plataforma e número do modelo para cada nó. Cada nó StorageGRID também suporta um subconjunto de objetos MIB-II.

Veja "Acesse arquivos MIB" se você deseja baixar os arquivos MIB em seus nós de grade.

Inicialmente, o SNMP está desativado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Ele fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

Armadilhas

Traps são notificações enviadas pelo agente SNMP que não requerem confirmação pelo sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu dentro do StorageGRID, como um alerta sendo acionado.

Traps são suportados em todas as três versões do SNMP.

Informa

Os informes são semelhantes aos traps, mas requerem reconhecimento pelo sistema de gestão. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenvia a informação até que uma confirmação seja recebida ou o valor máximo de tentativa tenha sido atingido.

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de intercetação e informação são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP para um alerta, tem de "configure um silêncio"o alertar. As notificações de alerta são enviadas pelo "Nó Admin. Remetente preferido".

  Cada alerta é mapeado para um dos três tipos de armadilha com base no nível de gravidade do alerta: ActiveMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem acionar esses traps, consulte "Referência de alertas".

- Alguns "alarmes (sistema legado)" são acionados em níveis de gravidade especificados ou superiores.

As notificações SNMP não são enviadas para cada alarme ou para cada gravidade do alarme.

Suporte à versão SNMP

A tabela fornece um resumo de alto nível do que é suportado para cada versão SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (OBTER e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de carateres da comunidade	Cadeia de carateres da comunidade	Utilizador do modelo de segurança baseado no utilizador (USM)
Notificações (ARMADILHA e INFORMAÇÃO)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Utilizador USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.
- SNMPv3: O StorageGRID não suporta o modo de suporte de transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é AES.

Configure o agente SNMP

Você pode configurar o agente SNMP do StorageGRID para usar um sistema de gerenciamento SNMP de terceiros para acesso MIB somente leitura e notificações.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

O agente SNMP do StorageGRID suporta SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, apenas é suportada a autenticação modelo de segurança do utilizador (USM).

Todos os nós na grade usam a mesma configuração SNMP.

Especifique a configuração básica

Como primeira etapa, habilite o agente StorageGRID SMNP e forneça informações básicas.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   A página do agente SNMP é exibida.

2. Para ativar o agente SNMP em todos os nós de grade, marque a caixa de seleção **Enable SNMP** (Ativar SNMP*).
3. Introduza as seguintes informações na secção Configuração básica.

Campo	Descrição
Contacto do sistema	Opcional. O Contato principal do sistema StorageGRID, que é retornado em mensagens SNMP como sysContact. Normalmente, o contacto do sistema é um endereço de correio eletrónico. Esse valor se aplica a todos os nós no sistema StorageGRID. **O contacto do sistema** pode ter um máximo de 255 carateres.
Localização do sistema	Opcional. A localização do sistema StorageGRID, que é retornado em mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde o sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. Esse valor se aplica a todos os nós no sistema StorageGRID. **A localização do sistema** pode ter no máximo 255 carateres.
Ativar notificações de agente SNMP	• Se selecionado, o agente SNMP do StorageGRID envia trap e informa notificações. • Se não estiver selecionado, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.
Ativar traps de autenticação	Se selecionado, o agente SNMP do StorageGRID envia traps de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Introduza cadeias de carateres da comunidade

Se você usar SNMPv1 ou SNMPv2c, complete a seção cadeias de Comunidade.

Quando o sistema de gerenciamento consulta o MIB do StorageGRID, ele envia uma string de comunidade. Se a cadeia de carateres da comunidade corresponder a um dos valores especificados aqui, o agente SNMP enviará uma resposta ao sistema de gerenciamento.

Passos

1. Para **comunidade somente leitura**, opcionalmente, insira uma cadeia de carateres comunitária para permitir acesso MIB somente leitura em endereços de agentes IPv4 e IPv6.

   Para garantir a segurança do seu sistema StorageGRID, não use "public" como a cadeia de carateres da comunidade. Se você deixar esse campo em branco, o agente SNMP usará o ID da grade do seu sistema StorageGRID como a cadeia de carateres da comunidade.

   Cada string de comunidade pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

2. Selecione **Adicionar outra string de comunidade** para adicionar strings adicionais.

   Até cinco cordas são permitidas.

Crie destinos de armadilha

Use a guia Trap Destinations (destinos de intercetação) na seção Other configurations (outras configurações) para definir um ou mais destinos para o StorageGRID trap (trap de intercetação) ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

Passos

1. Para o campo **Default trap Community** (comunidade de trap padrão), insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de trap SNMPv1 ou SNMPv2.

   Conforme necessário, você pode fornecer uma string de comunidade ("personalizada") diferente quando você define um destino de armadilha específico.

   A comunidade de trap padrão pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco.

2. Para adicionar um destino de armadilha, selecione **criar**.
3. Selecione a versão SNMP que será utilizada para este destino de trap.
4. Preencha o formulário criar destino de armadilha para a versão selecionada.

SNMPv1

Se você selecionou SNMPv1 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Deve ser armadilha para SNMPv1.
Host	Um endereço IPv4 ou IPv6 ou um nome de domínio totalmente qualificado (FQDN) para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de intercetação SNMP, a menos que você precise usar TCP.
Cadeia de carateres da comunidade	Use a comunidade de trap padrão, se uma foi especificada, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço em branco.

SNMPv2c

Se você selecionou SNMPv2c como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de intercetação SNMP, a menos que você precise usar TCP.
Cadeia de carateres da comunidade	Use a comunidade de trap padrão, se uma foi especificada, ou insira uma string de comunidade personalizada para esse destino de trap. A string de comunidade personalizada pode ter no máximo 32 carateres e não pode conter espaço em branco.

SNMPv3

Se você selecionou SNMPv3 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de intercetação SNMP, a menos que você precise usar TCP.
Utilizador USM	O utilizador USM que será utilizado para autenticação. • Se selecionou **Trap**, apenas são apresentados utilizadores USM sem IDs de motor autoritativas. • Se selecionou **inform**, apenas são apresentados utilizadores USM com IDs de motor autoritativas. • Se não forem apresentados utilizadores: i. Crie e salve o destino da armadilha. ii. Vá para Crie utilizadores USM e crie o usuário. iii. Regresse ao separador Trap Destinations (destinos da armadilha), selecione o destino guardado na tabela e selecione **Edit** (Editar). iv. Selecione o utilizador.

5. Selecione **criar**.

   O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agente

Opcionalmente, use a guia endereços de agentes na seção outras configurações para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Se você não configurar um endereço de agente, o endereço de escuta padrão será a porta UDP 161 em todas as redes StorageGRID.

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Protocolo da Internet	Se esse endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se esse endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Qual rede StorageGRID o agente ouvirá. • Redes Grid, Admin e Client: O agente SNMP escutará consultas em todas as três redes. • Rede de rede • Rede de administração • Rede de clientes **Nota**: Se você usar a rede do cliente para dados inseguros e criar um endereço de agente para a rede do cliente, esteja ciente de que o tráfego SNMP também será inseguro.
Porta	Opcionalmente, o número da porta que o agente SNMP deve ouvir. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Nota**: Quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

3. Selecione **criar**.

   O endereço do agente é criado e adicionado à tabela.

Crie utilizadores USM

Se estiver a utilizar o SNMPv3, utilize o separador utilizadores USM na secção outras configurações para definir os utilizadores USM que estão autorizados a consultar o MIB ou a receber traps e informações.

SNMPv3 *inform* destinos devem ter usuários com IDs de motor. SNMPv3 *trap* destino não pode ter usuários com IDs de motor.

Estas etapas não se aplicam se você estiver usando apenas SNMPv1 ou SNMPv2c.

Passos

1. Selecione **criar**.
2. Introduza as seguintes informações.

Campo	Descrição
Nome de utilizador	Um nome exclusivo para este utilizador USM. Os nomes de usuário podem ter um máximo de 32 carateres e não podem conter carateres de espaço em branco. O nome de usuário não pode ser alterado depois que o usuário é criado.
Acesso MIB somente leitura	Se selecionado, este utilizador deverá ter acesso apenas de leitura à MIB.
ID do motor autoritário	Se este utilizador for utilizado num destino de informação, o ID de mecanismo autorizado para este utilizador. Insira 10 a 64 carateres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para utilizadores USM que serão selecionados em destinos de armadilha para informação. Este valor não é permitido para utilizadores USM que serão selecionados em destinos de armadilha para armadilhas. **Nota**: Este campo não é mostrado se você selecionou **Acesso MIB somente leitura** porque os usuários USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o utilizador USM: • **AuthPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe, um protocolo de privacidade e uma palavra-passe. • **AuthNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Tem de especificar um protocolo de autenticação e uma palavra-passe.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Palavra-passe	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Mostrado apenas se você selecionou **authPriv** e sempre definido como AES, que é o único protocolo de privacidade suportado.
Palavra-passe	Mostrado apenas se você selecionou **authPriv**. A senha que este usuário usará para privacidade.

3. Selecione **criar**.

   O utilizador USM é criado e adicionado à tabela.

4. Quando tiver concluído a configuração do agente SNMP, selecione **Save**.

A nova configuração do agente SNMP fica ativa.

Atualize o agente SNMP

Você pode desativar notificações SNMP, atualizar strings da comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de intercetação.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de acesso à raiz".

Sobre esta tarefa

Consulte "Configure o agente SNMP" para obter detalhes sobre cada campo na página do agente SNMP. Você deve selecionar **Salvar** na parte inferior da página para confirmar as alterações feitas em cada guia.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.

   A página do agente SNMP é exibida.

2. Para desativar o agente SNMP em todos os nós de grade, desmarque a caixa de seleção **Ativar SNMP** e selecione **Salvar**.

   Se você reativar o agente SNMP, todas as configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize as informações na seção Configuração básica:
   a. Conforme necessário, atualize o **Contato do sistema** e **localização do sistema**.
   b. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar notificações de agente SNMP** para controlar se o agente StorageGRID SNMP envia trap e informa notificações.

      Quando esta caixa de verificação está desmarcada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

   c. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar traps de autenticação** para controlar se o agente SNMP do StorageGRID envia traps de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usar SNMPv1 ou SNMPv2c, opcionalmente, atualize ou adicione uma comunidade **somente leitura** na seção cadeias de Comunidade.
5. Para atualizar destinos de intercetação, selecione a guia destinos de intercetação na seção outras configurações.

   Utilize este separador para definir um ou mais destinos para o StorageGRID trap ou para informar notificações. Quando você ativa o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

   Para obter detalhes sobre o que introduzir, "Criar destinos de armadilha"consulte .

   - Opcionalmente, atualize ou remova a comunidade de trap padrão.

     Se você remover a comunidade de trap padrão, primeiro deve garantir que todos os destinos de trap

existentes usem uma cadeia de carateres de comunidade personalizada.

- Para adicionar um destino de armadilha, selecione **criar**.
- Para editar um destino de armadilha, selecione o botão de opção e selecione **Editar**.
- Para remover um destino de armadilha, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

6. Para atualizar endereços de agentes, selecione a guia endereços de agentes na seção outras configurações.

   Use esta guia para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

   Para obter detalhes sobre o que introduzir, "Criar endereços de agente"consulte .

   - Para adicionar um endereço de agente, selecione **criar**.
   - Para editar um endereço de agente, selecione o botão de opção e selecione **Editar**.
   - Para remover um endereço de agente, selecione o botão de opção e selecione **Remover**.
   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

7. Para atualizar os utilizadores USM, selecione o separador utilizadores USM na secção outras configurações.

   Utilize este separador para definir os utilizadores USM que estão autorizados a consultar a MIB ou a receber traps e informações.

   Para obter detalhes sobre o que introduzir, "Crie utilizadores USM"consulte .

   - Para adicionar um utilizador USM, selecione **criar**.
   - Para editar um utilizador USM, selecione o botão de opção e selecione **Edit**.

     O nome de utilizador de um utilizador USM existente não pode ser alterado. Se você precisar alterar um nome de usuário, você deve remover o usuário e criar um novo.

     > Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, você deverá editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

   - Para remover um utilizador USM, selecione o botão de opção e selecione **Remover**.

     > Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deve editar ou remover o destino. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

   - Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando tiver atualizado a configuração do agente SNMP, selecione **Save**.

Acesse arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e serviços gerenciados para os nós em sua grade. Você pode acessar arquivos MIB que definem os objetos e notificações do StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Consulte "Utilize a monitorização SNMP" para obter mais informações sobre ficheiros SNMP e MIB.

Acesse arquivos MIB

Siga estes passos para aceder aos ficheiros MIB.

Passos

1. Selecione **CONFIGURATION** > **Monitoring** > **SNMP Agent**.
2. Na página do agente SNMP, selecione o arquivo que deseja baixar:
   - **NetApp-StorageGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os nós de administração.
   - * ES-NetApp-06-MIB.mib*: Define objetos e notificações para dispositivos baseados em série e.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com interface BMC.

     Você também pode acessar arquivos MIB no seguinte local em qualquer nó do StorageGRID: `/usr/share/snmp/mibs`

3. Para extrair os OIDs StorageGRID do arquivo MIB:

   a. Obtenha o OID da raiz do MIB do StorageGRID:

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Resultado: `.1.3.6.1.4.1.789.28669` (`28669` É sempre o OID para StorageGRID)

   a. Grep para o OID StorageGRID em toda a árvore (usando `paste` para unir linhas):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

O `snmptranslate` comando tem muitas opções que são úteis para explorar o MIB. Este comando está disponível em qualquer nó StorageGRID.

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID StorageGRID.

Nome do objeto	Código Objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID.

Objetos MIB

Nome do objeto	Código Objeto (OID)	Descrição
ActiveAlertCount		O número de alertas ativos na activeAlertTable.
ActiveAlertTable		Uma tabela de alertas ativos no StorageGRID.
ActiveAlertId		O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
ActiveAlertName		O nome do alerta.
ActiveAlertInstance		O nome da entidade que gerou o alerta, normalmente o nome do nó.
ActiveAlertSeverity		A gravidade do alerta.
ActiveAlertStartTime		A data e a hora em que o alerta foi acionado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Tipo de notificação	Código Objeto (OID)	Descrição
ActiveMinorAlert		Um alerta com gravidade menor
ActiveMajorAlert		Um alerta com grande gravidade
ActiveCriticalAlert		Um alerta com gravidade crítica

Informações sobre direitos autorais

Informações sobre marcas comerciais