Usar monitoramento SNMP

StorageGRID software

NetApp
December 03, 2025

Índice

Usar monitoramento SNMP

Usar monitoramento SNMP

Se você quiser monitorar o StorageGRID usando o Protocolo Simples de Gerenciamento de Rede (SNMP), deverá configurar o agente SNMP incluído no StorageGRID.

- "Configurar o agente SNMP"
- "Atualizar o agente SNMP"

Capacidades

Cada nó StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB StorageGRID contém definições de tabela e notificação para alertas. 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.

Ver"Acessar arquivos MIB" se você quiser baixar os arquivos MIB nos nós da sua grade.

Inicialmente, o SNMP é desabilitado 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

Armadilhas são notificações enviadas pelo agente SNMP que não exigem confirmação pelo sistema de gerenciamento. As armadilhas servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como um alerta sendo disparado.

As armadilhas são suportadas em todas as três versões do SNMP.

Informa

As informações são semelhantes às armadilhas, mas exigem reconhecimento pelo sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará a informação até que uma confirmação seja recebida ou o valor máximo de novas tentativas seja atingido.

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de captura 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, você deve"configurar um silêncio" para o alerta. As notificações de alerta são enviadas pelo"nó de administração do remetente preferencial" .

  Cada alerta é mapeado para um dos três tipos de armadilhas com base no nível de gravidade do alerta: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem disparar essas armadilhas, consulte o"Referência de alertas" .

Suporte à versão SNMP

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

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de caracteres da comunidade	Cadeia de caracteres da comunidade	Usuário do Modelo de Segurança Baseado no Usuário (USM)
Notificações (ARMAZENAR e INFORMAR)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Usuário 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 oferece suporte ao Modo de Suporte de Transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é o SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é o AES.

Configurar 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 conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

O agente SNMP do StorageGRID oferece suporte a SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, somente a autenticação do Modelo de Segurança do Usuário (USM) é suportada.

Todos os nós na grade usam a mesma configuração SNMP.

Especificar configuração básica

Como primeiro passo, habilite o agente StorageGRID SMNP e forneça informações básicas.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.

   A página do agente SNMP é exibida.

2. Para habilitar o agente SNMP em todos os nós da grade, marque a caixa de seleção **Habilitar SNMP**.
3. Insira as seguintes informações na seção Configuração básica.

Campo	Descrição
Contato do sistema	Opcional. O contato principal do sistema StorageGRID , que é retornado em mensagens SNMP como sysContact. O contato do sistema normalmente é um endereço de e-mail. Este valor se aplica a todos os nós no sistema StorageGRID . **Contato do sistema** pode ter no máximo 255 caracteres.
Localização do sistema	Opcional. A localização do sistema StorageGRID , que é retornada em mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde seu sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço de uma instalação. Este valor se aplica a todos os nós no sistema StorageGRID . **Localização do sistema** pode ter no máximo 255 caracteres.
Habilitar notificações do agente SNMP	• Se selecionado, o agente SNMP StorageGRID envia notificações de interceptação e informação. • Se não for selecionado, o agente SNMP suportará acesso MIB somente leitura, mas não enviará nenhuma notificação SNMP.
Habilitar armadilhas de autenticação	Se selecionado, o agente SNMP do StorageGRID enviará interceptações de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Insira as sequências da comunidade

Se você usar SNMPv1 ou SNMPv2c, preencha a seção Strings da comunidade.

Quando o sistema de gerenciamento consulta o StorageGRID MIB, ele envia uma string de comunidade. Se a sequência de caracteres 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**, insira opcionalmente uma sequência de caracteres de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6.

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

   Cada sequência de caracteres da comunidade pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Selecione **Adicionar outra sequência de comunidade** para adicionar sequências adicionais.

   São permitidas até cinco strings.

Criar destinos de armadilha

Use a guia Destinos de interceptação na seção Outras configurações para definir um ou mais destinos para interceptação do StorageGRID ou informar notificações. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Passos

1. Para o campo **Comunidade de interceptação padrão**, insira opcionalmente a sequência de caracteres da comunidade padrão que você deseja usar para destinos de interceptação SNMPv1 ou SNMPv2.

   Conforme necessário, você pode fornecer uma sequência de caracteres de comunidade diferente ("personalizada") ao definir um destino de captura específico.

   Comunidade de trap padrão pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Para adicionar um destino de armadilha, selecione **Criar**.
3. Selecione qual versão SNMP será usada 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 Trap para SNMPv1.
Hospedar	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 de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços 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.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
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 de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços 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.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
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 de interceptação SNMP padrão, a menos que você precise usar TCP.
Usuário USM	O usuário USM que será usado para autenticação. • Se você selecionou **Trap**, somente usuários do USM sem IDs de mecanismo autoritativos serão exibidos. • Se você selecionou **Informar**, somente usuários do USM com IDs de mecanismo autoritativos serão exibidos. • Se nenhum usuário for exibido: i. Crie e salve o destino da armadilha. ii. Vá paraCriar usuários USM e criar o usuário. iii. Retorne à aba Destinos da armadilha, selecione o destino salvo na tabela e selecione **Editar**. iv. Selecione o usuário.

5. Selecione **Criar**.

   O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agentes

Opcionalmente, use a guia Endereços do agente na seção Outras configurações para especificar um ou mais "endereços de escuta". Esses 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. Insira as seguintes informações.

Campo	Descrição
Protocolo de internet	Se este endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se este endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Em qual rede StorageGRID o agente irá escutar. • Redes de grade, administração e cliente: o agente SNMP escutará consultas em todas as três redes. • Rede de grade • Rede de administração • Rede de clientes **Observação**: 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 na qual o agente SNMP deve escutar. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. **Observação**: 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.

Criar usuários USM

Se você estiver usando SNMPv3, use a guia Usuários do USM na seção Outras configurações para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber traps e informações.

> Os destinos SNMPv3 *inform* devem ter usuários com IDs de mecanismo. O destino SNMPv3 *trap* não pode ter usuários com IDs de mecanismo.

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

Passos

1. Selecione **Criar**.

2. Insira as seguintes informações.

Campo	Descrição
Nome de usuário	Um nome exclusivo para este usuário USM. Os nomes de usuário podem ter no máximo 32 caracteres e não podem conter espaços em branco. O nome de usuário não pode ser alterado após a criação do usuário.
Acesso MIB somente leitura	Se selecionado, este usuário deverá ter acesso somente leitura ao MIB.
ID do mecanismo autoritativo	Se este usuário for usado em um destino de informação, o ID do mecanismo autoritativo para este usuário. Digite de 10 a 64 caracteres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para usuários do USM que serão selecionados em destinos de trap para informações. Este valor não é permitido para usuários do USM que serão selecionados em destinos de armadilhas para armadilhas. **Observação**: Este campo não será exibido se você selecionar **Acesso MIB somente leitura** porque os usuários do USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o usuário USM: • **authPriv**: Este usuário se comunica com autenticação e privacidade (criptografia). Você deve especificar um protocolo de autenticação e uma senha, bem como um protocolo de privacidade e uma senha. • **authNoPriv**: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Você deve especificar um protocolo de autenticação e uma senha.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Senha	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Exibido somente se você selecionou **authPriv** e sempre definiu como AES, que é o único protocolo de privacidade suportado.
Senha	Exibido somente se você selecionou **authPriv**. A senha que este usuário usará para privacidade.

3. Selecione **Criar**.

   O usuário USM é criado e adicionado à tabela.

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

   A nova configuração do agente SNMP fica ativa.

Atualizar o agente SNMP

Você pode desabilitar notificações SNMP, atualizar strings de comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de interceptação.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso root" .

Sobre esta tarefa

Ver"Configurar 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 quaisquer alterações feitas em cada guia.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.

   A página do agente SNMP é exibida.

2. Para desabilitar o agente SNMP em todos os nós da grade, desmarque a caixa de seleção **Habilitar 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 o **Local do sistema**.
   b. Opcionalmente, marque ou desmarque a caixa de seleção **Habilitar notificações do agente SNMP** para controlar se o agente SNMP do StorageGRID envia notificações de interceptação e informação.

      Quando esta caixa de seleção 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 armadilhas de autenticação** para controlar se o agente SNMP do StorageGRID envia armadilhas 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 Strings da comunidade.
5. Para atualizar destinos de armadilhas, selecione a aba Destinos de armadilhas na seção Outras configurações.

   Use esta guia para definir um ou mais destinos para notificações de interceptação ou informação do StorageGRID . Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

   Para obter detalhes sobre o que inserir, consulte"Criar destinos de armadilhas" .

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

  Se você remover a comunidade de armadilhas padrão, primeiro deverá garantir que todos os destinos de armadilhas existentes usem uma sequência de caracteres 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 aba para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

   Para obter detalhes sobre o que inserir, consulte"Criar endereços de agentes" .

   - Para adicionar um endereço de agente, selecione **Criar**.
   - Para editar o endereço de um 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 usuários do USM, selecione a guia Usuários do USM na seção Outras configurações.

   Use esta guia para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber armadilhas e informações.

   Para obter detalhes sobre o que inserir, consulte"Criar usuários USM" .

   - Para adicionar um usuário USM, selecione **Criar**.
   - Para editar um usuário USM, selecione o botão de opção e selecione **Editar**.

     O nome de usuário de um usuário USM existente não pode ser alterado. Se precisar alterar um nome de usuário, você deverá removê-lo e criar um novo.

     > Se você adicionar ou remover o ID de mecanismo autoritativo de um usuário e esse usuário estiver selecionado para um destino, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

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

     > Se o usuário que você removeu estiver selecionado para um destino de interceptação, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

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

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

Acessar arquivos MIB

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

Ver"Usar monitoramento SNMP" para mais informações sobre arquivos SNMP e MIB.

Acessar arquivos MIB

Siga estas etapas para acessar os arquivos MIB.

Passos

1. Selecione **CONFIGURAÇÃO** > **Monitoramento** > **Agente SNMP**.
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 na Série E.
   - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com uma 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 do StorageGRID do arquivo MIB:

   a. Obtenha o OID da raiz do StorageGRID MIB:

   ```
   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` O comando tem muitas opções 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	ID do objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID .

Objetos MIB

Nome do objeto	ID do objeto (OID)	Descrição
Contagem de Alerta Ativo		O número de alertas ativos na activeAlertTable.
Tabela de Alerta Ativo		Uma tabela de alertas ativos no StorageGRID.
ID de alerta ativo		O ID do alerta. Único no conjunto atual de alertas ativos.
NomeAlertaAtivo		O nome do alerta.
instância de alerta ativo		O nome da entidade que gerou o alerta, normalmente o nome do nó.
activeAlertSeverity		A gravidade do alerta.
hora de início do alerta ativo		Data e hora em que o alerta foi disparado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ID de alerta ativo
- NomeAlertaAtivo
- instância de alerta ativo
- activeAlertSeverity
- hora de início do alerta ativo

Tipo de notificação	ID do objeto (OID)	Descrição
Alerta Menor Ativo		Um alerta com gravidade menor
AlertaMaiorAtivo		Um alerta com grande gravidade
AlertaCríticoAtivo		Um alerta com gravidade crítica

Informações sobre direitos autorais

Informações sobre marcas comerciais