Utilizar a monitorização SNMP

StorageGRID

NetApp
March 10, 2025

Índice

Utilizar a monitorização SNMP 1
Recursos 1
Suporte à versão SNMP 1
Limitações 2
Acessando o MIB 2
Configurando o agente SNMP 2
Atualizando o agente SNMP 11

Utilizar a monitorização SNMP

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

- "Configurando o agente SNMP"
- "Atualizando o agente SNMP"

Recursos

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece uma base de informações de gerenciamento (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.

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:

- **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** são semelhantes às armadilhas, 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 configurar um silêncio para o alerta. As notificações de alerta são enviadas por qualquer nó Admin configurado para ser o remetente preferido.
- Certos 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	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	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.

Acessando o MIB

Você pode acessar o arquivo de definição MIB no seguinte local em qualquer nó do StorageGRID:

/Usr/share/snmp/mibs/NetApp-StorageGRID-MIB.txt

Informações relacionadas

"Referência de alertas"

"Referência de alarmes (sistema legado)"

"Alarmes que geram notificações SNMP (sistema legado)"

"Silenciar notificações de alerta"

Configurando o agente SNMP

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.

- Você deve ter a permissão de acesso root.

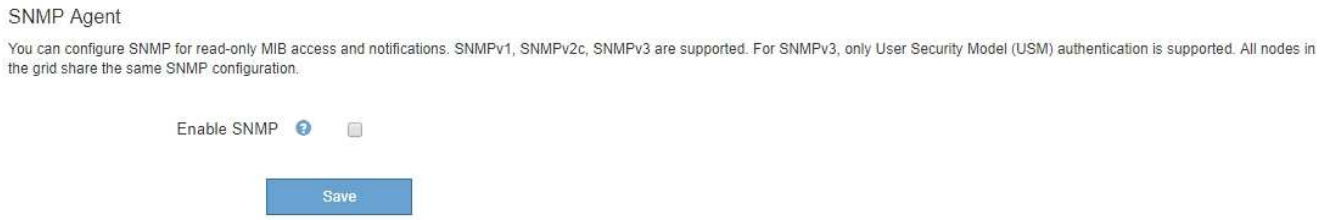
Sobre esta tarefa

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Você pode configurar o agente para uma ou mais versões.

Passos

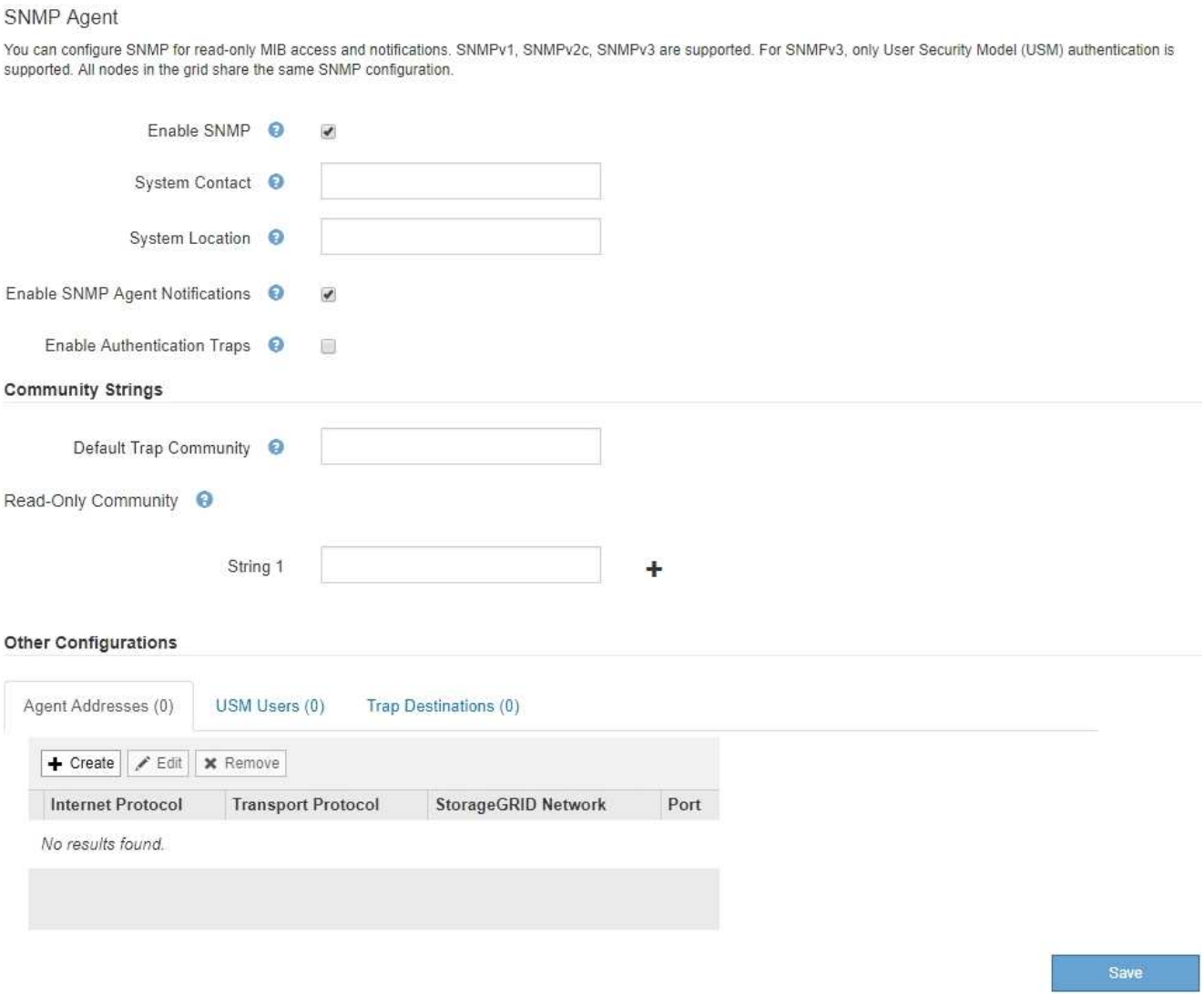
1. Selecione **Configuração Monitoramento Agente SNMP**.

   A página Agente SNMP é exibida.



2. Para ativar o agente SNMP em todos os nós de grade, marque a caixa de seleção **Ativar SNMP** .

   Os campos para configurar um agente SNMP são exibidos.



3. No campo **Contato do sistema**, insira o valor que você deseja que o StorageGRID forneça nas mensagens SNMP para o sysContact.

   Normalmente, o contacto do sistema é um endereço de correio eletrónico. O valor fornecido aplica-se a todos os nós do sistema StorageGRID. **O Contato do sistema** pode ter no máximo 255 carateres.

4. No campo **localização do sistema**, insira o valor que você deseja que o StorageGRID forneça nas mensagens SNMP para 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. O valor fornecido aplica-se a todos os nós do sistema StorageGRID. **A localização do sistema** pode ter no máximo 255 carateres.

5. Mantenha a caixa de seleção **Ativar notificações de agentes SNMP** selecionada se desejar que o agente SNMP do StorageGRID envie uma armadilha e informe notificações.

   Se esta caixa de verificação não estiver selecionada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

6. Marque a caixa de seleção **Enable Authentication traps** (Ativar traps de autenticação) se desejar que o agente SNMP do StorageGRID envie uma armadilha de autenticação se receber uma mensagem de protocolo autenticada incorretamente.
7. Se você usar SNMPv1 ou SNMPv2c, complete a seção cadeias de Comunidade.

   Os campos nesta seção são usados para autenticação baseada na comunidade em SNMPv1 ou SNMPv2c. Esses campos não se aplicam ao SNMPv3.

   a. No campo **Default Trap Community** (Comunidade de Trap padrão), insira opcionalmente a cadeia de carateres da comunidade padrão que você deseja usar para destinos de trap.

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

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

   b. Para **Comunidade somente leitura**, insira uma ou mais strings de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6. Clique no sinal de adição ➕para adicionar várias cadeias de carateres.

      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.

      Cada string de comunidade pode ter no máximo 32 carateres e não pode conter carateres de espaço em branco. Até cinco cordas são permitidas.

      > ⓘ Para garantir a segurança do seu sistema StorageGRID, não use "público" como a cadeia de carateres da comunidade. Se você não inserir uma string de comunidade, o agente SNMP usará a ID de grade do seu sistema StorageGRID como a string de comunidade.

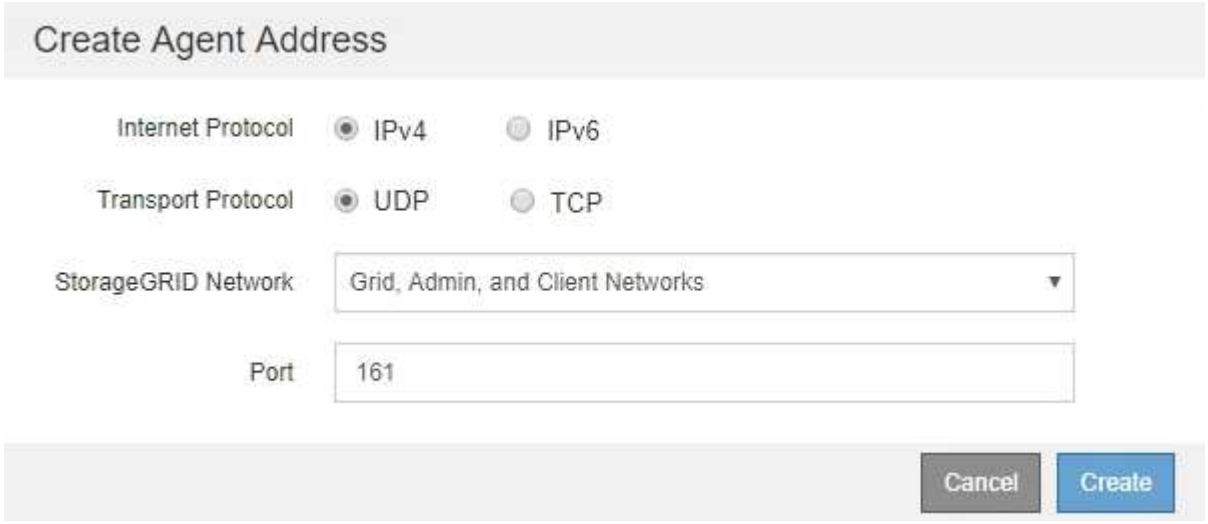
8. Opcionalmente, selecione a guia endereços de agentes na seção outras configurações .

Use esta guia para especificar um ou mais ""endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas. Cada endereço de agente inclui um protocolo de Internet, um protocolo de transporte, uma rede StorageGRID e, opcionalmente, uma porta.

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

a. Clique em **criar**.

   A caixa de diálogo criar endereço do agente é exibida.



b. Para **Internet Protocol**, selecione se este endereço usará IPv4 ou IPv6.

   Por padrão, o SNMP usa IPv4.

c. Para **Protocolo de Transporte**, selecione se este endereço usará UDP ou TCP.

   Por padrão, o SNMP usa UDP.

d. No campo **rede StorageGRID**, selecione em qual rede StorageGRID a consulta será recebida.
   - Rede, administrador e redes de clientes: O StorageGRID deve ouvir consultas SNMP em todas as três redes.
   - Rede de rede
   - Rede de administração
   - Rede de clientes

   > Para garantir que as comunicações do cliente com o StorageGRID permaneçam seguras, você não deve criar um endereço de agente para a rede do cliente.

e. No campo **Port**, insira 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.

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.

f. Clique em **criar**.

O endereço do agente é criado e adicionado à tabela.

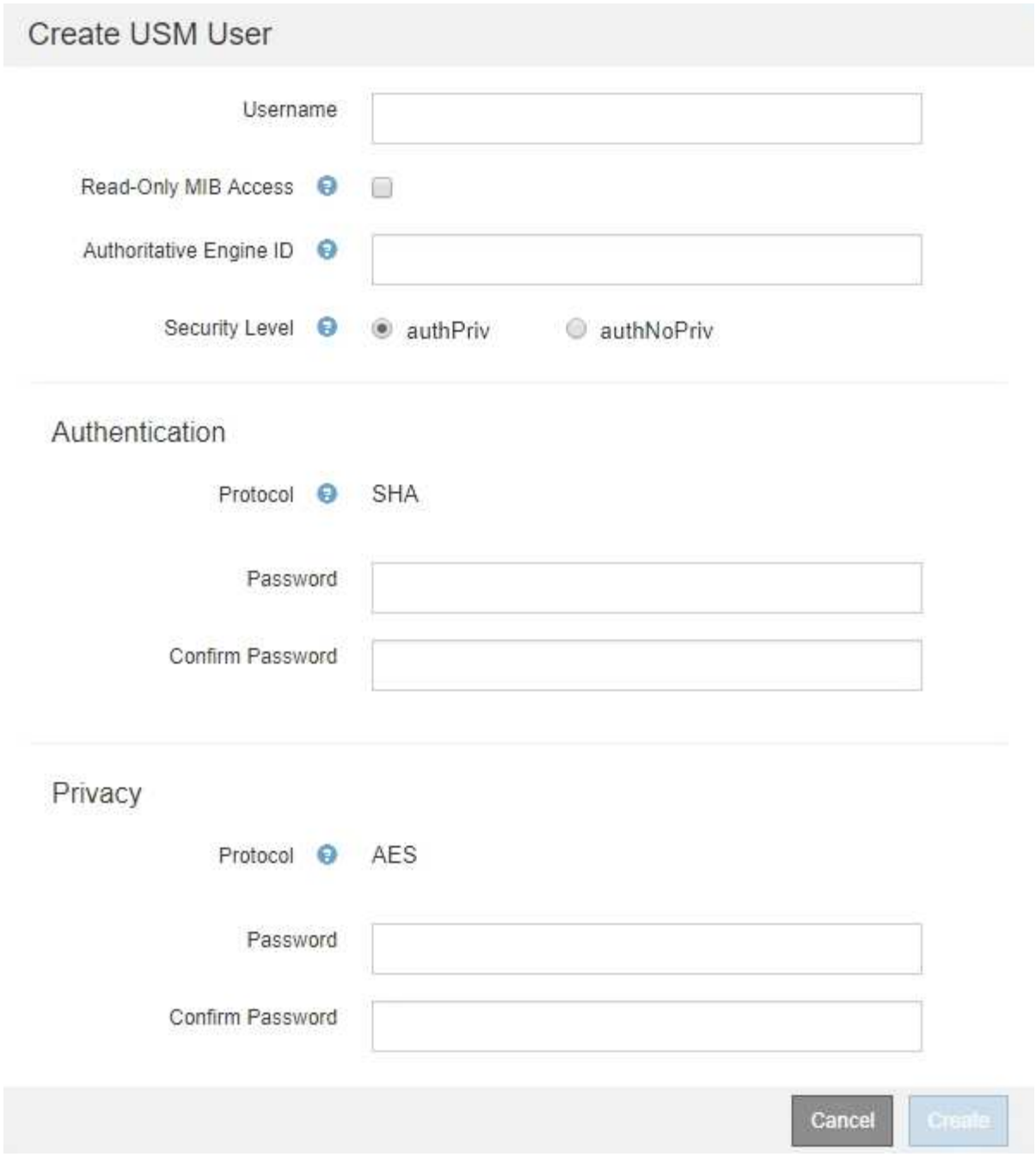
9. Se estiver a utilizar o SNMPv3, selecione o separador utilizadores USM na secção outras configurações.

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

Esta etapa não se aplica se você estiver usando apenas SNMPv1 ou SNMPv2c.

a. Clique em **criar**.

É apresentada a caixa de diálogo Create USM User (criar utilizador USM).



b. Introduza um **Nome de utilizador** exclusivo para este utilizador USM.

   Os nomes de usuário têm 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.

c. Marque a caixa de seleção **Acesso MIB somente leitura** se esse usuário tiver acesso somente leitura à MIB.

   Se você selecionar **Acesso MIB somente leitura**, o campo **ID do mecanismo autoritário** será desativado.

   Os utilizadores USM que têm acesso MIB apenas de leitura não podem ter IDs de motor.

d. Se este utilizador for utilizado num destino de informação, introduza o **ID de motor autoritário** para este utilizador.

> SNMPv3 informar destinos devem ter usuários com IDs de motor. SNMPv3 o destino do trap não pode ter utilizadores com IDs de motor.

O ID oficial do mecanismo pode ser de 5 a 32 bytes em hexadecimal.

e. Selecione um 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.

f. Introduza e confirme a palavra-passe que este utilizador utilizará para autenticação.

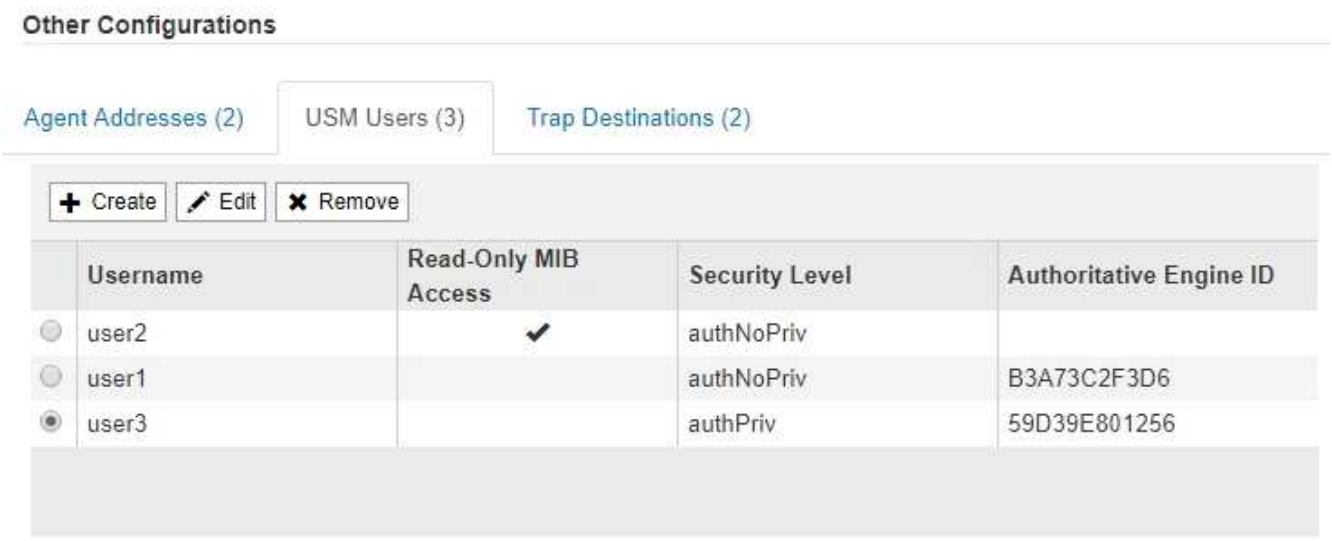
> O único protocolo de autenticação suportado é SHA (HMAC-SHA-96).

g. Se selecionou **authPriv**, introduza e confirme a palavra-passe que este utilizador utilizará para a privacidade.

> O único protocolo de privacidade suportado é AES.

h. Clique em **criar**.

O utilizador USM é criado e adicionado à tabela.

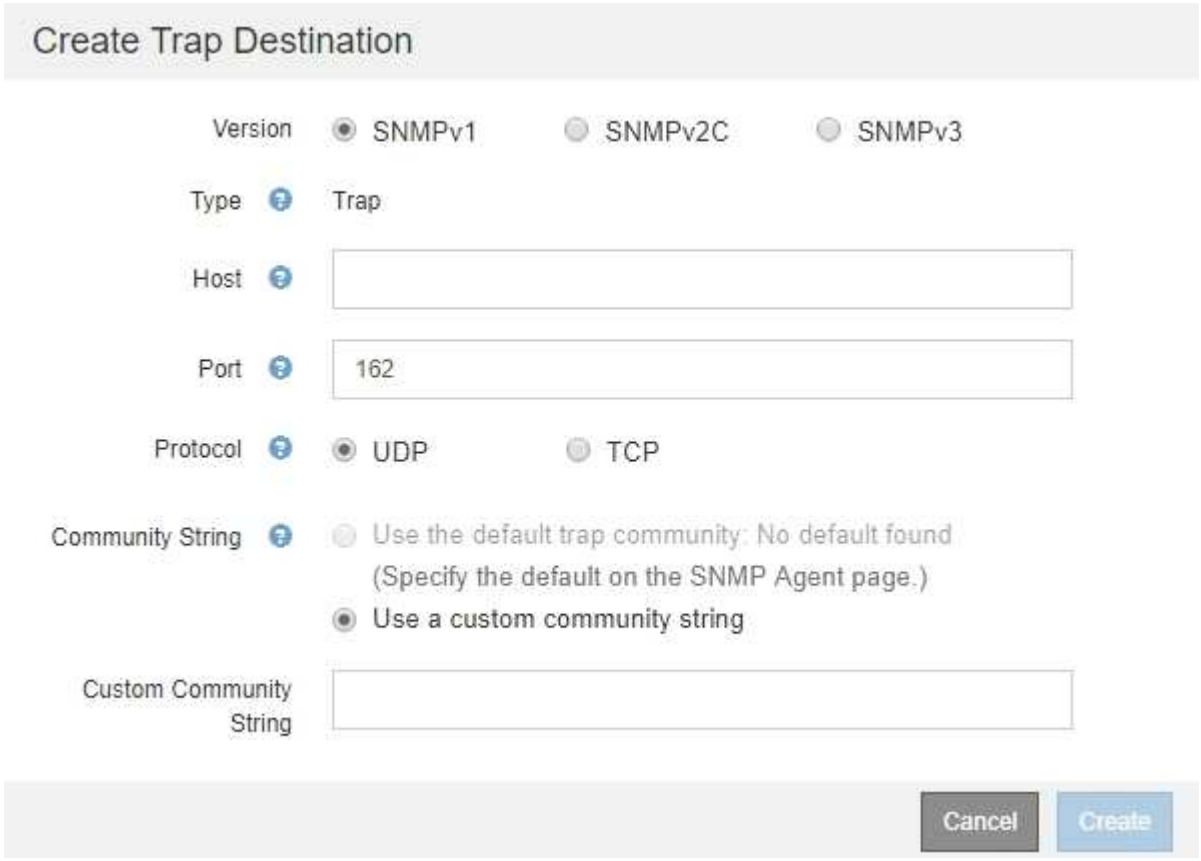


10. na seção outras configurações, selecione a guia Destinos de armadilha.

A guia Destinos de armadilha permite definir um ou mais destinos para notificações de intercetação StorageGRID ou informar. Quando você ativa o agente SNMP e clica em **Salvar**, o StorageGRID começa a enviar notificações para cada destino definido. As notificações são enviadas quando alertas e alarmes são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

a. Clique em **criar**.

A caixa de diálogo criar destino de armadilha é exibida.



b. No campo **Version** (versão), selecione qual versão SNMP será utilizada para esta notificação.

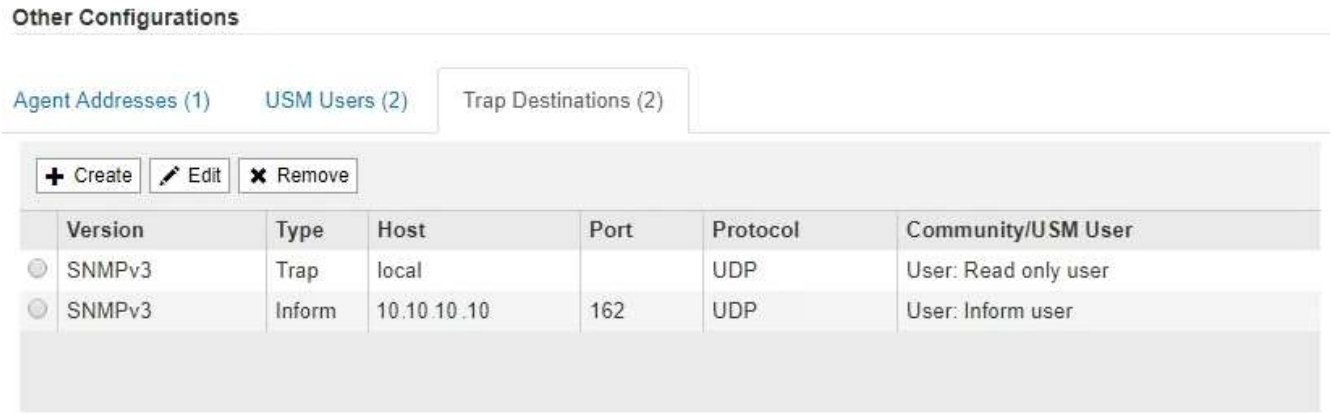
c. Preencha o formulário, com base na versão selecionada

Versão	Especifique esta informação
SNMPv1	**Nota:** para SNMPv1, o agente SNMP só pode enviar traps. As informações não são suportadas. i. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. ii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iii. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) iv. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, 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	i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Use a comunidade de trap padrão, se uma foi especificada na página Agente SNMP, 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.

Versão	Especifique esta informação
SNMPv3	i. Selecione se o destino será usado para armadilhas ou informações. ii. No campo **Host**, insira um endereço IPv4 ou IPv6 (ou FQDN) para receber a armadilha. iii. Para **Port**, use o padrão (162), a menos que você precise usar outro valor. (162 é a porta padrão para traps SNMP.) iv. Para **Protocolo**, use o padrão (UDP). TCP também é suportado. (UDP é o protocolo padrão de trap SNMP.) v. Selecione 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.

d. Clique em **criar**.

O destino da armadilha é criado e adicionado à tabela.



11. Quando tiver concluído a configuração do agente SNMP, clique em **Save**

A nova configuração do agente SNMP fica ativa.

Informações relacionadas

"Silenciar notificações de alerta"

Atualizando o agente SNMP

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

O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter a permissão de acesso root.

Sobre esta tarefa

Sempre que você atualizar a configuração do agente SNMP, esteja ciente de que você deve clicar em **Salvar** na parte inferior da página Agente SNMP para confirmar quaisquer alterações feitas em cada guia.

Passos

1. Selecione **Configuração Monitoramento Agente SNMP**.

   A página Agente SNMP é exibida.

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

   O agente SNMP está desativado para todos os nós de grade. Se você reativar o agente posteriormente, quaisquer configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize os valores inseridos para **Contato do sistema** e **localização do sistema**.
4. Opcionalmente, desmarque a caixa de seleção **Ativar notificações de agentes SNMP** se você não quiser mais que o agente SNMP do StorageGRID envie trap e informe notificações.

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

5. Opcionalmente, desmarque a caixa de seleção **Ativar traps de autenticação** se você não quiser mais que o agente SNMP do StorageGRID envie uma armadilha de autenticação quando receber uma mensagem de protocolo autenticada incorretamente.
6. Se você usar SNMPv1 ou SNMPv2c, atualize opcionalmente a seção cadeias de Comunidade.

   Os campos nesta seção são usados para autenticação baseada na comunidade em SNMPv1 ou SNMPv2c. Esses campos não se aplicam ao SNMPv3.

   > Se você quiser remover a cadeia de carateres padrão da comunidade, primeiro você deve garantir que todos os destinos de intercetação usem uma cadeia de carateres personalizada da comunidade.

7. Se quiser 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". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas. Cada endereço de agente inclui um protocolo de Internet, um protocolo de transporte, uma rede StorageGRID e uma porta.

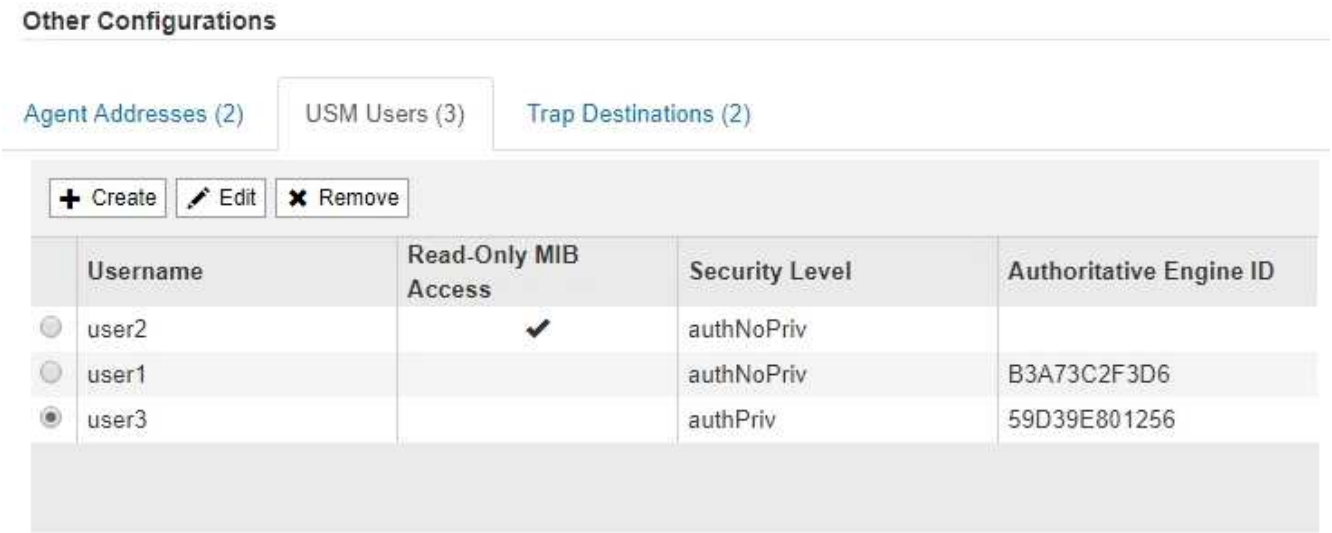
a. Para adicionar um endereço de agente, clique em **criar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.

b. Para editar um endereço de agente, selecione o botão de opção para o endereço e clique em **Editar**. Em seguida, consulte a etapa para obter endereços de agentes nas instruções para configurar o agente SNMP.

c. Para remover um endereço de agente, selecione o botão de opção para o endereço e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover esse endereço.

d. Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.

8. Se pretender atualizar 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.

a. Para adicionar um utilizador USM, clique em **criar**. Em seguida, consulte a etapa para usuários USM nas instruções para configurar o agente SNMP.

b. Para editar um utilizador USM, selecione o botão de opção do utilizador e clique em **Edit**. Em seguida,

consulte a etapa para usuários USM nas instruções para configurar o agente SNMP.

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.

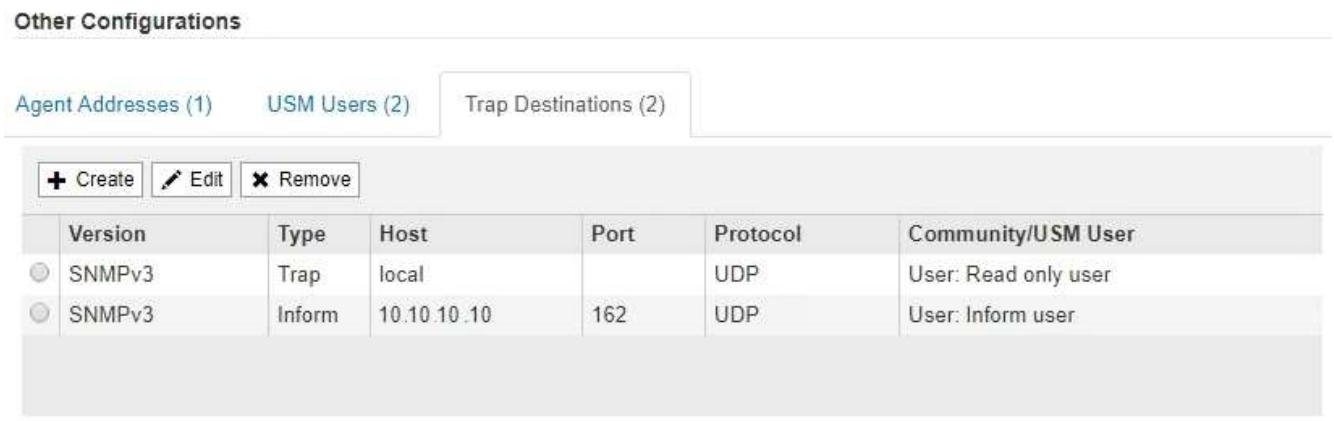
> Se você adicionar ou remover um ID de mecanismo autoritário de um usuário e esse usuário estiver selecionado atualmente para um destino, edite ou remova o destino, conforme descrito na etapa Destino de trap SNMP. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

c. Para remover um utilizador USM, selecione o botão de opção do utilizador e clique em **Remove**. Em seguida, clique em **OK** para confirmar que deseja remover esse usuário.

> Se o usuário removido estiver selecionado atualmente para um destino de armadilha, você deverá editar ou remover o destino, conforme descrito na etapa Destino de trap SNMP. Caso contrário, ocorre um erro de validação quando você salva a configuração do agente SNMP.

a. Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.

1. Se quiser atualizar destinos de intercetação, selecione a guia Destinos de intercetação na seção outras configurações.



A guia Destinos de armadilha permite definir um ou mais destinos para notificações de intercetação StorageGRID ou informar. Quando você ativa o agente SNMP e clica em **Salvar**, o StorageGRID começa a enviar notificações para cada destino definido. As notificações são enviadas quando alertas e alarmes são acionados. As notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifdown e coldstart).

a. Para adicionar um destino de armadilha, clique em **criar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.

b. Para editar um destino de armadilha, selecione o botão de opção do usuário e clique em **Editar**. Em seguida, consulte a etapa para destinos de intercetação nas instruções para configurar o agente SNMP.

c. Para remover um destino de armadilha, selecione o botão de opção para o destino e clique em **Remover**. Em seguida, clique em **OK** para confirmar que deseja remover este destino.

d. Para confirmar suas alterações, clique em **Salvar** na parte inferior da página Agente SNMP.

2. Quando tiver atualizado a configuração do agente SNMP, clique em **Save**.

Informações relacionadas

"Configurando o agente SNMP"

Informações sobre direitos autorais

Informações sobre marcas comerciais