Gerenciar alertas SNMP

SANtricity 11.9

NetApp
December 16, 2024

Índice

Gerenciar alertas SNMP

Configurar alertas SNMP

Para configurar alertas SNMP (Simple Network Management Protocol), você deve identificar pelo menos um servidor onde o monitor de eventos da matriz de armazenamento pode enviar traps SNMP. A configuração requer um nome de comunidade ou um nome de usuário e um endereço IP para o servidor.

Antes de começar

- Um servidor de rede deve ser configurado com um aplicativo de serviço SNMP. Você precisa do endereço de rede deste servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de intercetação para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de base de informações de gerenciamento (MIB) foi copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB define os dados que estão sendo monitorados e gerenciados.

  Se você não tiver o arquivo MIB, poderá obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte à NetApp".
  - Clique na guia **Downloads** e selecione **Downloads**.
  - Clique em **e-Series SANtricity os Controller Software**.
  - Selecione **Download Latest Release**.
  - Inicie sessão.
  - Aceite a declaração de precaução e o contrato de licença.
  - Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

Sobre esta tarefa

Esta tarefa descreve como identificar o servidor SNMP para destinos de intercetação e, em seguida, testar sua configuração.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Na primeira configuração, a guia SNMP exibe "Configurar Comunidades/usuários".

3. Selecione **Configurar Comunidades/usuários**.

   Abre-se a caixa de diálogo Selecionar versão SNMP.

4. Selecione a versão SNMP para os alertas, **SNMPv2c** ou **SNMPv3**.

   Dependendo da seleção, a caixa de diálogo Configurar Comunidades ou a caixa de diálogo Configurar usuários SNMPv3 será aberta.

5. Siga as instruções apropriadas para SNMPv2c (comunidades) ou SNMPv3 (usuários):
   - **SNMPv2c (comunidades)** — na caixa de diálogo Configurar Comunidades, insira uma ou mais strings de comunidade para os servidores de rede. Um nome de comunidade é uma cadeia de carateres que identifica um conjunto conhecido de estações de gerenciamento e é normalmente criado por um administrador de rede. Consiste apenas em carateres ASCII imprimíveis. Você pode adicionar até 256 comunidades. Quando terminar, clique em **Guardar**.
   - **SNMPv3 (usuários)** — na caixa de diálogo Configurar SNMPv3 usuários, clique em **Adicionar** e insira as seguintes informações:
     - **Nome do usuário** — Digite um nome para identificar o usuário, que pode ter até 31 carateres.
     - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
     - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
     - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres. Quando terminar, clique em **Adicionar** e, em seguida, clique em **Fechar**.
6. Na página Alertas com a guia SNMP selecionada, clique em **Adicionar destinos de armadilha**.

   A caixa de diálogo Adicionar destinos de armadilha é aberta.

7. Insira um ou mais destinos de armadilha, selecione seus nomes de comunidade ou de usuário associados e clique em **Adicionar**.
   - **Trap Destination** — Digite um endereço IPv4 ou IPv6 do servidor executando um serviço SNMP.
   - **Nome da comunidade ou Nome do usuário** — na lista suspensa, selecione o nome da comunidade (SNMPv2c) ou nome de usuário (SNMPv3) para esse destino de armadilha. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Send Authentication Failure Trap** — Selecione essa opção (a caixa de seleção) se você quiser alertar o destino da armadilha sempre que uma solicitação SNMP for rejeitada por causa de um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Add**, os destinos de intercetação e os nomes associados aparecem na guia **SNMP** da página **Alerts**.
8. Para se certificar de que uma armadilha é válida, selecione um destino de armadilha na tabela e clique em **destino de armadilha de teste** para enviar uma armadilha de teste para o endereço configurado.

Resultados

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertable.

Adicionar destinos de intercetação para alertas SNMP

Você pode adicionar até 10 servidores para enviar traps SNMP.

Antes de começar

- O servidor de rede que você deseja adicionar deve ser configurado com um aplicativo de serviço SNMP.

Você precisa do endereço de rede deste servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de intercetação para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).

- O arquivo de base de informações de gerenciamento (MIB) foi copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB define os dados que estão sendo monitorados e gerenciados.

  Se você não tiver o arquivo MIB, poderá obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte à NetApp".
  - Clique em **Downloads** e selecione **Downloads**.
  - Clique em **e-Series SANtricity os Controller Software**.
  - Selecione **Download Latest Release**.
  - Inicie sessão.
  - Aceite a declaração de precaução e o contrato de licença.
  - Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos de armadilha definidos atualmente aparecem na tabela.

3. Selecione **Add Trap Desinations**.

   A caixa de diálogo Adicionar destinos de armadilha é aberta.

4. Insira um ou mais destinos de armadilha, selecione seus nomes de comunidade ou de usuário associados e clique em **Adicionar**.
   - **Trap Destination** — Digite um endereço IPv4 ou IPv6 do servidor executando um serviço SNMP.
   - **Nome da comunidade ou Nome do usuário** — na lista suspensa, selecione o nome da comunidade (SNMPv2c) ou nome de usuário (SNMPv3) para esse destino de armadilha. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Send Authentication Failure Trap** — Selecione essa opção (a caixa de seleção) se você quiser alertar o destino da armadilha sempre que uma solicitação SNMP for rejeitada por causa de um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Add**, os destinos de intercetação e os nomes de comunidade ou de usuário associados aparecem na tabela.
5. Para se certificar de que uma armadilha é válida, selecione um destino de armadilha na tabela e clique em **destino de armadilha de teste** para enviar uma armadilha de teste para o endereço configurado.

Resultados

O monitor de eventos envia traps SNMP para o(s) servidor(es) sempre que ocorre um evento alertable.

Configurar variáveis MIB SNMP

Para alertas SNMP, você pode opcionalmente configurar variáveis de base de informações de gerenciamento (MIB) que aparecem em traps SNMP. Essas variáveis

podem retornar o nome do storage array, o local do array e uma pessoa de Contato.

Antes de começar

O arquivo MIB deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP.

Se não tiver um ficheiro MIB, pode obtê-lo da seguinte forma:

- Vá para "Suporte à NetApp".
- Clique em **Downloads** e selecione **Downloads**.
- Clique em **e-Series SANtricity os Controller Software**.
- Selecione **Download Latest Release**.
- Inicie sessão.
- Aceite a declaração de precaução e o contrato de licença.
- Role para baixo até ver o arquivo MIB para o tipo de controlador e clique no link para fazer o download do arquivo.

Sobre esta tarefa

Esta tarefa descreve como definir variáveis MIB para traps SNMP. Essas variáveis podem retornar os seguintes valores em resposta ao SNMP GetRequests:

- `sysName` (nome do storage array)
- `sysLocation` (local do storage array)
- `sysContact` (nome de um administrador)

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.
3. Selecione **Configurar variáveis MIB SNMP**.

   A caixa de diálogo Configurar variáveis MIB SNMP é aberta.

4. Introduza um ou mais dos seguintes valores e, em seguida, clique em **Guardar**.
   - **Name** — o valor para a variável MIB `sysName` . Por exemplo, insira um nome para a matriz de armazenamento.
   - **Localização** — o valor para a variável MIB `sysLocation` . Por exemplo, insira um local da matriz de armazenamento.
   - **Contact** — o valor da variável MIB `sysContact` . Por exemplo, insira um administrador responsável pelo storage array.

Resultados

Esses valores aparecem em mensagens de intercetação SNMP para alertas de storage array.

Edite comunidades para SNMPv2c armadilhas

Você pode editar nomes de comunidade para SNMPv2c armadilhas.

Antes de começar

Um nome de comunidade deve ser criado.

Passos

1. Selecione **Definir › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na tabela.

3. Selecione **Configurar Comunidades**.
4. Digite o novo nome da comunidade e clique em **Salvar**. Os nomes da comunidade podem consistir apenas em carateres ASCII imprimíveis.

Resultados

A guia SNMP da página Alertas exibe o nome da comunidade atualizado.

Edite as configurações do usuário para SNMPv3 traps

Você pode editar definições de usuário para SNMPv3 traps.

Antes de começar

Um usuário deve ser criado para o trap SNMPv3.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos e os nomes de utilizador da armadilha são apresentados na tabela.

3. Para editar uma definição de usuário, selecione o usuário na tabela e clique em **Configurar usuários**.
4. Na caixa de diálogo, clique em **Exibir/Editar configurações**.
5. Edite as seguintes informações:
   - **Nome do usuário** — altere o nome que identifica o usuário, que pode ter até 31 carateres.
   - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres.

Resultados

O separador SNMP da página Alertas apresenta as definições atualizadas.

Adicione comunidades para SNMPv2c armadilhas

Você pode adicionar até 256 nomes de comunidade para SNMPv2c armadilhas.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na tabela.

3. Selecione **Configurar Comunidades**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione **Adicionar outra comunidade**.
5. Digite o novo nome da comunidade e clique em **Salvar**.

Resultados

O novo nome da comunidade aparece na guia SNMP da página Alertas.

Adicione usuários para SNMPv3 traps

Você pode adicionar até 256 usuários para SNMPv3 armadilhas.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos e os nomes de utilizador da armadilha são apresentados na tabela.

3. Selecione **Configurar usuários**.

   A caixa de diálogo Configurar usuários SNMPv3 será aberta.

4. Selecione **Adicionar**.
5. Insira as informações a seguir e clique em **Adicionar**.
   - **Nome do usuário** — Digite um nome para identificar o usuário, que pode ter até 31 carateres.
   - **Engine ID** — Selecione o Engine ID, que é usado para gerar chaves de autenticação e criptografia para mensagens, e deve ser exclusivo no domínio administrativo. Na maioria dos casos, você deve selecionar **local**. Se você tiver uma configuração não padrão, selecione **Custom**; outro campo aparece onde você deve inserir o ID do mecanismo autorizado como uma cadeia hexadecimal, com um número par de carateres entre 10 e 32 carateres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, introduza uma palavra-passe de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 carateres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, introduza uma palavra-passe de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 carateres.

Remova comunidades para SNMPv2c armadilhas

Você pode remover um nome de comunidade para SNMPv2c armadilhas.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos da armadilha e os nomes da comunidade aparecem na página **Alertas**.

3. Selecione **Configurar Comunidades**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione o nome da comunidade que deseja excluir e clique no ícone **Remover** (X) na extrema direita.

   Se os destinos de intercetação estiverem associados a esse nome de comunidade, a caixa de diálogo confirmar Remover Comunidade mostrará os endereços de destino de intercetação afetados.

5. Confirme a operação e clique em **Remover**.

Resultados

O nome da comunidade e seu destino de armadilha associado são removidos da página Alertas.

Remova usuários para SNMPv3 armadilhas

Você pode remover um usuário para SNMPv3 traps.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os destinos de intercetação e os nomes de usuário aparecem na página Alertas.

3. Selecione **Configurar usuários**.

   A caixa de diálogo Configurar usuários SNMPv3 será aberta.

4. Selecione o nome de usuário que deseja excluir e clique em **Excluir**.
5. Confirme a operação e, em seguida, clique em **Delete**.

Resultados

O nome de usuário e seu destino de armadilha associado são removidos da página Alertas.

Eliminar destinos de armadilha

Você pode excluir um endereço de destino de armadilha para que o monitor de eventos da matriz de armazenamento não envie mais traps SNMP para esse endereço.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **SNMP**.

   Os endereços de destino da armadilha aparecem na tabela.

3. Selecione um destino de armadilha e clique em **Excluir** no canto superior direito da página.
4. Confirme a operação e, em seguida, clique em **Delete**.

   O endereço de destino não aparece mais na página Alertas.

Resultados

O destino da armadilha excluída não recebe mais traps SNMP do monitor de eventos da matriz de armazenamento.

Informações sobre direitos autorais

Informações sobre marcas comerciais