Alertas

SANtricity 11.9

NetApp
December 16, 2024

Índice

Alertas 1
Visão geral dos alertas 1
Conceitos 1
Gerenciar alertas de e-mail 3
Gerenciar alertas SNMP 7
Gerenciar alertas syslog 14
FAQs 16

Alertas

Visão geral dos alertas

Você pode configurar o System Manager para enviar alertas de storage array por e-mail, traps SNMP e mensagens syslog.

O que são alertas?

Alertas notificar os administradores sobre eventos importantes que ocorrem no storage array. Os eventos podem incluir problemas como uma falha da bateria, um componente que se move do ideal para o Offline ou erros de redundância no controlador. Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação.

Saiba mais:

- "Como os alertas funcionam"
- "Terminologia de alertas"

Como faço para configurar alertas?

Você pode configurar alertas para serem enviados como uma mensagem para um ou mais endereços de e-mail, como uma intercetação SNMP para um servidor SNMP ou como uma mensagem para um servidor syslog. A configuração de alerta está disponível no **Configurações › Alertas**.

Saiba mais:

- "Configure o servidor de e-mail e os destinatários para alertas"
- "Configure o servidor syslog para alertas"
- "Configurar alertas SNMP"

Informações relacionadas

Saiba mais sobre conceitos relacionados a alertas:

- "Visão geral do log de eventos"
- "Carimbos de hora inconsistentes"

Conceitos

Como os alertas funcionam

Os alertas notificam os administradores sobre eventos importantes que ocorrem no storage array. Os alertas podem ser enviados por e-mail, traps SNMP e syslog.

O processo de alertas funciona da seguinte forma:

1. Um administrador configura um ou mais dos seguintes métodos de alerta no System Manager:

- **Email** — as mensagens são enviadas para endereços de e-mail.
- **SNMP** — traps SNMP são enviados para um servidor SNMP.
- **Syslog** — as mensagens são enviadas para um servidor syslog.

2. Quando o monitor de eventos do storage deteta um problema, ele grava informações sobre esse problema no log de eventos (disponível no **suporte › Log de eventos**). Por exemplo, os problemas podem incluir eventos como uma falha de bateria, um componente que se move do Optimal para o Offline ou erros de redundância no controlador.
3. Se o monitor de eventos determinar que o evento é "alertable", ele então envia uma notificação usando os métodos de alerta configurados (e-mail, SNMP e/ou syslog). Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação.

Configuração de alertas

Pode configurar alertas a partir do assistente de configuração inicial (apenas para alertas de e-mail) ou da página Alertas. Para verificar a configuração atual, vá para **Configurações › Alertas**.

O bloco Alertas exibe a configuração de alertas, que pode ser uma das seguintes opções:

- Não configurado.
- Configurado; pelo menos um método de alerta está configurado. Para determinar quais métodos de alerta estão configurados, aponte o cursor para o mosaico.

Informações de alertas

Os alertas podem incluir os seguintes tipos de informações:

- Nome do storage array.
- Tipo de erro de evento relacionado a uma entrada de log de eventos.
- Data e hora em que o evento ocorreu.
- Breve descrição do evento.

Os alertas de syslog seguem o padrão de mensagens RFC 5424.

Terminologia de alertas

Saiba como os termos de alertas se aplicam ao storage array.

Componente	Descrição
Monitor de eventos	O monitor de eventos reside no storage array e é executado como uma tarefa em segundo plano. Quando o monitor de eventos deteta anomalias no storage array, ele grava informações sobre os problemas no log de eventos. Os problemas podem incluir eventos como uma falha da bateria, um componente que se move do ideal para o Offline ou erros de redundância no controlador. Se o monitor de eventos determinar que o evento é "alertable", ele então envia uma notificação usando os métodos de alerta configurados (e-mail, SNMP e/ou syslog). Todos os eventos críticos são considerados "alertable", juntamente com alguns eventos de aviso e informação.

Componente	Descrição
Servidor de correio	O servidor de e-mail é usado para enviar e receber alertas de e-mail. O servidor utiliza o Simple Mail Transfer Protocol (SMTP).
SNMP	O SNMP (Simple Network Management Protocol) é um protocolo padrão da Internet usado para gerenciar e compartilhar informações entre dispositivos em redes IP.
Trap SNMP	Uma armadilha SNMP é uma notificação enviada para um servidor SNMP. A armadilha contém informações sobre problemas significativos com o storage array.
Destino de trap SNMP	Um destino de trap SNMP é um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP.
Nome da comunidade	Um nome de comunidade é uma cadeia de carateres que atua como uma senha para o(s) servidor(es) de rede em um ambiente SNMP.
Ficheiro MIB	O arquivo de base de informações de gerenciamento (MIB) define os dados que estão sendo monitorados e gerenciados no storage array. Ele deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB está disponível com o software System Manager no site de suporte.
Variáveis MIB	As variáveis do Management Information base (MIB) podem retornar valores como o nome do storage array, localização do array e uma pessoa de Contato em resposta ao SNMP GetRequest.
Syslog	Syslog é um protocolo usado por dispositivos de rede para enviar mensagens de eventos para um servidor de log.
UDP	O User Datagram Protocol (UDP) é um protocolo da camada de transporte que especifica um número de porta de origem e destino em seus cabeçalhos de pacotes.

Gerenciar alertas de e-mail

Configure o servidor de e-mail e os destinatários para alertas

Para configurar alertas de e-mail, você deve especificar um endereço de servidor de e-mail e os endereços de e-mail dos destinatários do alerta. São permitidos até 20 endereços de correio eletrónico.

Antes de começar

- O endereço do servidor de e-mail deve estar disponível. O endereço pode ser um endereço IPv4 ou IPv6, ou um nome de domínio totalmente qualificado.

Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

- O endereço de e-mail a ser usado como remetente de alerta deve estar disponível. Este é o endereço que aparece no campo "de" da mensagem de alerta. Um endereço de remetente é necessário no protocolo SMTP; sem ele, um erro resulta.
- O(s) endereço(s) de e-mail do(s) destinatário(s) alerta(s) deve(m) estar disponível(s) Normalmente, o destinatário é um endereço para um administrador de rede ou administrador de armazenamento. Pode introduzir até 20 endereços de correio eletrónico.

Sobre esta tarefa

Esta tarefa descreve como configurar o servidor de e-mail, inserir endereços de e-mail para o remetente e destinatários e testar todos os endereços de e-mail inseridos na página Alertas.

Os alertas de e-mail também podem ser configurados a partir do assistente de configuração inicial.

Passos

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

   Se um servidor de e-mail ainda não estiver configurado, a guia e-mail exibirá "Configurar servidor de e-mail".

3. Selecione **Configure Mail Server**.

   A caixa de diálogo Configurar servidor de correio abre-se.

4. Insira as informações do servidor de e-mail e clique em **Salvar**.
   - **Endereço do servidor de correio** — Insira um nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6 do servidor de correio.

     Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

   - **Endereço do remetente de e-mail** — Digite um endereço de e-mail válido para ser usado como remetente do e-mail. Este endereço é exibido no campo "de" da mensagem de e-mail.
   - **Criptografia** — se você quiser criptografar mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para mensagens criptografadas. Caso contrário, selecione **nenhum**.
   - **Nome de usuário e senha** — se necessário, insira um nome de usuário e senha para autenticação com o remetente de saída e o servidor de e-mail.
   - **Inclua informações de Contato no e-mail** — para incluir as informações de Contato do remetente com a mensagem de alerta, selecione esta opção e insira um nome e número de telefone.

     Depois de clicar em **Salvar**, os endereços de e-mail aparecem na guia e-mail da página Alertas.

5. Selecione **Adicionar e-mails**.

A caixa de diálogo Adicionar e-mails é aberta.

6. Insira um ou mais endereços de e-mail para os destinatários do alerta e clique em **Adicionar**.

   Os endereços de e-mail aparecem na página Alertas.

7. Se você quiser garantir que os endereços de e-mail sejam válidos, clique em **testar todos os e-mails** para enviar mensagens de teste aos destinatários.

Resultados

Depois de configurar alertas por e-mail, o monitor de eventos envia mensagens de e-mail para os destinatários especificados sempre que ocorre um evento alertable.

Editar endereços de e-mail para alertas

Você pode alterar os endereços de e-mail dos destinatários que recebem alertas de e-mail.

Antes de começar

O endereço de e-mail que você pretende editar deve ser definido na guia e-mail da página Alertas.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Na tabela **Endereço de e-mail**, selecione o endereço que deseja alterar e clique no ícone **Editar** (lápis) na extrema direita.

   A linha se torna um campo editável.

4. Insira um novo endereço e clique no ícone **Salvar** (marca de seleção).

   Se pretender cancelar as alterações, selecione o ícone **Cancelar** (X).

Resultados

A guia e-mail da página Alertas exibe os endereços de e-mail atualizados.

Adicionar endereços de e-mail para alertas

Você pode adicionar até 20 destinatários para alertas de e-mail.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Selecione **Adicionar e-mails**.

   A caixa de diálogo Adicionar e-mails é aberta.

4. No campo vazio, insira um novo endereço de e-mail. Se quiser adicionar mais de um endereço, selecione **Adicionar outro email** para abrir outro campo.

5. Clique em **Add**.

Resultados

A guia e-mail da página Alertas exibe os novos endereços de e-mail.

Excluir servidor de e-mail ou endereços de e-mail para alertas

Você pode remover o servidor de e-mail definido anteriormente para que os alertas não sejam mais enviados para os endereços de e-mail ou remover endereços de e-mail individuais.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Na tabela, execute um dos seguintes procedimentos:
   - Para remover um servidor de e-mail para que os alertas não sejam mais enviados para os endereços de e-mail, selecione a linha para o servidor de e-mail.
   - Para remover um endereço de e-mail para que os alertas não sejam mais enviados para esse endereço, selecione a linha do endereço de e-mail que deseja excluir. O botão **Delete** no canto superior direito da tabela fica disponível para seleção.
4. Clique em **Delete** e confirme a operação.

Edite o servidor de e-mail para alertas

Você pode alterar o endereço do servidor de e-mail e o endereço do remetente usado para alertas de e-mail.

Antes de começar

O endereço do servidor de correio que está a alterar tem de estar disponível. O endereço pode ser um endereço IPv4 ou IPv6, ou um nome de domínio totalmente qualificado.

Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Email**.
3. Selecione **Configure Mail Server**.

   A caixa de diálogo Configurar servidor de correio abre-se.

4. Edite o endereço do servidor de correio, as informações do remetente e as informações de contacto.
   - **Endereço do servidor de correio** — edite o nome de domínio totalmente qualificado, endereço IPv4 ou endereço IPv6 do servidor de correio.

Para usar um nome de domínio totalmente qualificado, você deve configurar um servidor DNS em ambos os controladores. Pode configurar um servidor DNS a partir da página hardware.

- **Endereço do remetente de e-mail** — edite o endereço de e-mail a ser usado como remetente do e-mail. Este endereço é exibido no campo "de" da mensagem de e-mail.
- **Inclua informações de Contato no e-mail** — para editar as informações de Contato do remetente, selecione esta opção e edite o nome e o número de telefone.

5. Clique em **Salvar**.

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.

Gerenciar alertas syslog

Configure o servidor syslog para alertas

Para configurar alertas syslog, você deve inserir um endereço de servidor syslog e uma porta UDP. São permitidos até cinco servidores syslog.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Este endereço pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Esta porta é tipicamente 514.

Sobre esta tarefa

Esta tarefa descreve como inserir o endereço e a porta para o servidor syslog e, em seguida, testar o endereço digitado.

Passos

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

   Se um servidor syslog ainda não estiver definido, a página Alertas exibirá "Adicionar servidores Syslog".

3. Clique em **Add Syslog Servers**.

   A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Insira informações para um ou mais servidores syslog (máximo de cinco) e clique em **Adicionar**.

- **Endereço do servidor** — Digite um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- **Porta UDP** — normalmente, a porta UDP para syslog é 514. A tabela exibe os servidores syslog configurados.

5. Para enviar um alerta de teste aos endereços do servidor, selecione **testar todos os servidores Syslog**.

Resultados

O monitor de eventos envia alertas para o servidor syslog sempre que ocorre um evento alertable. Para configurar ainda mais as configurações do syslog para logs de auditoria, "Configure o servidor syslog para logs de auditoria" consulte .

Se vários servidores syslog estiverem configurados, todos os servidores syslog configurados receberão um log de auditoria.

Editar servidores syslog para alertas

Você pode editar o endereço do servidor usado para receber alertas syslog.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Na tabela, selecione um endereço de servidor syslog e clique no ícone **Editar** (lápis) na extrema direita.

   A linha se torna um campo editável.

4. Edite o endereço do servidor e o número da porta UDP e clique no ícone **Salvar** (marca de seleção).

Resultados

O endereço do servidor atualizado é exibido na tabela.

Adicione servidores syslog para alertas

Você pode adicionar um máximo de cinco servidores para alertas syslog.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Este endereço pode ser um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Esta porta é tipicamente 514.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Selecione **Adicionar servidores Syslog**.

   A caixa de diálogo Add Syslog Server (Adicionar servidor Syslog) é aberta.

4. Selecione **Adicionar outro servidor syslog**.
5. Insira informações para o servidor syslog e clique em **Adicionar**.

- **Endereço do servidor Syslog** — Insira um nome de domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- **Porta UDP** — normalmente, a porta UDP para syslog é 514.

Você pode configurar até cinco servidores syslog.

Resultados

Os endereços do servidor syslog aparecem na tabela.

Exclua servidores syslog para alertas

Você pode excluir um servidor syslog para que ele não receba mais alertas.

Passos

1. Selecione **Definições › Alertas**.
2. Selecione a guia **Syslog**.
3. Selecione um endereço de servidor syslog e clique em **Remover** no canto superior direito.

   A caixa de diálogo confirmar servidor Syslog será aberta.

4. Confirme a operação e, em seguida, clique em **Delete**.

Resultados

O servidor removido não recebe mais alertas do monitor de eventos.

FAQs

E se os alertas estiverem desativados?

Se você quiser que os administradores recebam notificações sobre eventos importantes que ocorrem no storage array, configure um método de alerta.

Para storages gerenciados com o Gerenciador de sistemas do SANtricity, você configura alertas na página Alertas. As notificações de alerta podem ser enviadas por e-mail, traps SNMP ou mensagens syslog. Além disso, os alertas de e-mail podem ser configurados a partir do Assistente de configuração inicial.

Como configuro alertas SNMP ou syslog?

Além dos alertas por e-mail, você pode configurar alertas para serem enviados por traps SNMP (Simple Network Management Protocol) ou por mensagens syslog.

Para configurar alertas SNMP ou syslog, vá para **Configurações › Alertas**.

Por que os carimbos de data/hora são inconsistentes entre a matriz e os alertas?

Quando o storage array envia alertas, ele não corrige o fuso horário do servidor de destino ou host que recebe os alertas. Em vez disso, o storage array usa a hora local (GMT) para criar o carimbo de data/hora usado para o Registro de alerta. Como

resultado, você pode ver inconsistências entre os carimbos de data/hora do storage array e o servidor ou host recebendo um alerta.

Como o storage array não corrige o fuso horário ao enviar alertas, o carimbo de data/hora nos alertas é GMT-Relative, que tem um deslocamento de fuso horário de zero. Para calcular um carimbo de data/hora apropriado ao seu fuso horário local, você deve determinar o deslocamento da hora do GMT e, em seguida, adicionar ou subtrair esse valor dos carimbos de data/hora.

Informações sobre direitos autorais

Informações sobre marcas comerciais