Alertas

SANtricity software

NetApp
March 17, 2026

Índice

Alertas

Saiba mais sobre alertas no SANtricity System Manager

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

O que são alertas?

Alerts notificam os administradores sobre eventos importantes que ocorrem no array de storage. Os eventos podem incluir problemas como falha de bateria, um componente passando de Optimal para Offline ou erros de redundância no controlador. Todos os eventos Critical são considerados "alertáveis", juntamente com alguns eventos Warning e Informational.

Saiba mais:

- "Como funcionam os alertas"
- "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 um trap SNMP para um servidor SNMP ou como uma mensagem para um servidor syslog. A configuração de alertas está disponível em **Configurações › Alertas**.

Saiba mais:

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

Informações relacionadas

Saiba mais sobre conceitos relacionados a alertas:

- "Visão geral do log de eventos"
- "Registros de data e hora inconsistentes"

Conceitos

Como funcionam os alertas no SANtricity System Manager

Os alertas notificam os administradores sobre eventos importantes que ocorrem no array de storage. Os alertas podem ser enviados por e-mail, SNMP traps 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 email.
- **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 array de storage detecta um problema, ele registra informações sobre esse problema no log de eventos (disponível em **Support › Event Log**). Por exemplo, os problemas podem incluir eventos como falha de bateria, um componente passando de Optimal para Offline ou erros de redundância no controlador.
3. Se o monitor de eventos determinar que o evento é "passível de alerta", ele então enviará uma notificação usando os métodos de alerta configurados (email, SNMP e/ou syslog). Todos os eventos críticos são considerados "passíveis de alerta", juntamente com alguns eventos de aviso e informativos.

Configuração de alertas

Você pode configurar alertas no assistente de Configuração Inicial (somente para alertas por e-mail) ou na página Alertas. Para verificar a configuração atual, acesse **Configurações › Alertas**.

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

- Não configurado.
- Configurado; pelo menos um método de alerta está definido. Para determinar quais métodos de alerta estão configurados, posicione o cursor sobre o bloco.

Informações de alertas

Os alertas podem incluir os seguintes tipos de informação:

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

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

Aprenda sobre a terminologia de alertas no software SANtricity

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

Componente	Descrição
Monitor de eventos	O monitor de eventos reside no array de storage e é executado como uma tarefa em segundo plano. Quando o monitor de eventos detecta anomalias no array de storage, ele registra informações sobre os problemas no log de eventos. Os problemas podem incluir eventos como falha de bateria, um componente passando de Ideal para Offline ou erros de redundância no controlador. Se o monitor de eventos determinar que o evento é "alertável", ele então enviará uma notificação usando os métodos de alerta configurados (email, SNMP e/ou syslog). Todos os eventos Críticos são considerados "alertáveis", juntamente com alguns eventos de Aviso e Informativos.

Componente	Descrição
Servidor de e-mail	O servidor de e-mail é usado para enviar e receber alertas por e-mail. O servidor utiliza Simple Mail Transfer Protocol (SMTP).
SNMP	Simple Network Management Protocol (SNMP) é um protocolo padrão da Internet usado para gerenciar e compartilhar informações entre dispositivos em redes IP.
Trap SNMP	Um SNMP trap é uma notificação enviada a um servidor SNMP. O trap contém informações sobre problemas significativos com o array de storage.
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	O nome de comunidade é uma sequência de caracteres que funciona como uma senha para o(s) servidor(es) de rede em um ambiente SNMP.
Arquivo MIB	O arquivo MIB (Management Information Base) define os dados que estão sendo monitorados e gerenciados no array de storage. Ele deve ser copiado e compilado no servidor com o aplicativo de serviço SNMP. Este arquivo MIB está disponível com o System Manager no site de suporte.
Variáveis MIB	As variáveis da Base de Informações de Gerenciamento (MIB) podem retornar valores como o nome do array de storage, a localização do array e uma pessoa de contato em resposta ao SNMP GetRequests.
Syslog	Syslog é um protocolo usado por dispositivos de rede para enviar mensagens de eventos a um servidor de log.
UDP	O Protocolo de Datagrama do Usuário (UDP) é um protocolo da camada de transporte que especifica um número de porta de origem e um número de porta de destino nos cabeçalhos dos pacotes.

Gerenciar alertas de email

Configurar o servidor de e-mail e os destinatários de alertas no SANtricity System Manager

Para configurar alertas por e-mail, você deve especificar o endereço do servidor de e-mail e os endereços de e-mail dos destinatários dos alertas. Até 20 endereços de e-mail são permitidos.

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 precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

- O endereço de e-mail a ser usado como remetente do alerta deve estar disponível. Este é o endereço que aparece no campo "De" da mensagem de alerta. Um endereço de remetente é obrigatório no protocolo SMTP; sem ele, ocorre um erro.
- Os endereços de e-mail dos destinatários do alerta devem estar disponíveis. O destinatário normalmente é um endereço para um administrador de rede ou administrador de storage. Você pode inserir até 20 endereços de e-mail.

Sobre esta tarefa

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

Os alertas por e-mail também podem ser configurados no assistente de configuração inicial.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.

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

3. Selecione **Configurar Mail Server**.

   A caixa de diálogo Configurar Servidor de Correio é aberta.

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

     Para usar um nome de domínio totalmente qualificado, você precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

   - **Endereço do remetente do e-mail** — insira um endereço de e-mail válido para ser usado como remetente do e-mail. Este endereço aparece no campo "De" da mensagem de e-mail.
   - **Criptografia** — Se desejar criptografar as mensagens, selecione **SMTPS** ou **STARTTLS** para o tipo de criptografia e, em seguida, selecione o número da porta para as mensagens criptografadas. Caso contrário, selecione **None**.
   - **Nome de usuário e senha** — Se necessário, insira um nome de usuário e uma senha para autenticação com o remetente de saída e o servidor de e-mail.
   - **Incluir informações de contato no email** — Para incluir as informações de contato do remetente na mensagem de alerta, selecione esta opção e insira um nome e um número de telefone.

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

5. Selecione **Add Emails**.

   A caixa de diálogo Adicionar Emails é aberta.

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

   Os endereços de e-mail aparecem na página Alerts.

7. Se quiser garantir que os endereços de e-mail são válidos, clique em **Test All Emails** para enviar mensagens de teste aos destinatários.

Resultados

Após configurar os alertas por e-mail, o monitor de eventos envia mensagens de e-mail aos destinatários especificados sempre que ocorre um evento passível de alerta.

Editar endereços de e-mail para alertas no SANtricity System Manager

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

Antes de começar

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

Passos

1. Selecione o menu: configurações [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. Digite um novo endereço e clique no ícone **Salvar** (marca de seleção).

   Se você quiser cancelar as alterações, selecione o ícone **Cancel** (X).

Resultados

A guia Email da página de Alertas exibe os endereços de email atualizados.

Adicionar endereços de e-mail para alertas no SANtricity System Manager

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.
3. Selecione **Add Emails**.

   A caixa de diálogo Adicionar Emails é aberta.

4. No campo vazio, insira um novo endereço de e-mail. Se desejar adicionar mais de um endereço, selecione **Adicionar outro e-mail** para abrir outro campo.
5. Clique em **Add**.

Resultados

A guia Email da página de Alertas exibe os novos endereços de email.

Excluir o servidor de e-mail ou os endereços de e-mail para alertas no SANtricity System Manager

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.
3. Na tabela, faça uma das seguintes ações:
   - Para remover um servidor de e-mail para que 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 **Excluir** no canto superior direito da tabela ficará disponível para seleção.
4. Clique em **Excluir** e confirme a operação.

Editar servidor de e-mail para alertas no SANtricity System Manager

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

Antes de começar

O endereço do servidor de e-mail que você está alterando precisa 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 precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Email**.
3. Selecione **Configurar Mail Server**.

   A caixa de diálogo Configurar Servidor de Correio é aberta.

4. Edite o endereço do servidor de e-mail, as informações do remetente e as informações de contato.
   - **Endereço do servidor de e-mail** — Edite o domínio totalmente qualificado, o endereço IPv4 ou o endereço IPv6 do servidor de e-mail.

     > Para usar um nome de domínio totalmente qualificado, você precisa configurar um servidor DNS em ambos os controladores. Você pode configurar um servidor DNS na página Hardware.

- **Endereço do remetente do e-mail** — Edite o endereço de e-mail que será usado como remetente do e-mail. Este endereço aparece no campo "De" da mensagem de e-mail.
- **Incluir informações de contato no email** — Para editar as informações de contato do remetente, selecione esta opção e, em seguida, edite o nome e o número de telefone.

5. Clique em **Salvar**.

Gerenciar alertas SNMP

Configurar alertas SNMP no SANtricity System Manager

Para configurar alertas do Protocolo Simples de Gerenciamento de Rede (SNMP), você deve identificar pelo menos um servidor para o qual o monitor de eventos do array de storage possa enviar traps SNMP. A configuração requer um nome de comunidade ou nome de usuário e um endereço IP para o servidor.

Antes de começar

- É necessário configurar um servidor de rede com um aplicativo de serviço SNMP. Você precisa do endereço de rede desse servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de trap para esse endereço. É possível usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de management information base (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.

  Caso não possua o arquivo MIB, você pode obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte da NetApp".
  - Clique na guia **Downloads** e, em seguida, selecione **Downloads**.
  - Clique em **E-Series SANtricity OS Controller Software**.
  - Selecione **Download Latest Release**.
  - Faça login.
  - Aceite a declaração de cautela e o contrato de licença.
  - Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o arquivo.

Sobre esta tarefa

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Na configuração inicial, a guia SNMP exibe "Configure Communities/Users."

3. Selecione **Configurar comunidades/usuários**.

   A caixa de diálogo Selecionar versão SNMP é aberta.

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

   Dependendo da sua seleção, a caixa de diálogo Configurar Comunidades ou a caixa de diálogo Configurar Usuários SNMPv3 é 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 string que identifica um conjunto conhecido de estações de gerenciamento e geralmente é criada por um administrador de rede. Consiste apenas em caracteres ASCII imprimíveis. Você pode adicionar até 256 comunidades. Quando terminar, clique em **Salvar**.
   - **SNMPv3 (usuários)** — Na caixa de diálogo Configurar SNMPv3 Users, clique em **Add** e insira as seguintes informações:
     - **Nome de usuário** — Digite um nome para identificar o usuário, que pode ter até 31 caracteres.
     - **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
     - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
     - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres. Quando terminar, clique em **Adicionar** e depois em **Fechar**.
6. Na página de Alertas, com a aba SNMP selecionada, clique em **Add Trap Destinations**.

   A caixa de diálogo Adicionar Destinos de Trap é aberta.

7. Insira um ou mais destinos de trap, selecione os nomes de comunidade ou nomes de usuário associados e clique em **Adicionar**.
   - **Destino da armadilha** — Insira um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP.
   - **Nome da comunidade ou nome de usuário** — No menu suspenso, selecione o nome da comunidade (SNMPv2c) ou o nome de usuário (SNMPv3) para este destino de trap. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Enviar Trap de Falha de Autenticação** — selecione esta opção (a caixa de seleção) se desejar alertar o destino do trap sempre que uma solicitação SNMP for rejeitada devido a um nome de comunidade ou nome de usuário não reconhecido. Após clicar em **Adicionar**, os destinos do trap e os nomes associados aparecem na guia **SNMP** da página **Alertas**.
8. Para garantir que um trap seja válido, selecione um destino de trap na tabela e clique em **Testar Destino do Trap** para enviar um trap de teste para o endereço configurado.

Resultados

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

Adicionar destinos de trap para alertas SNMP no SANtricity System Manager

Você pode adicionar até 10 servidores para enviar traps SNMP.

Antes de começar

- O servidor de rede que você deseja adicionar deve estar configurado com um aplicativo de serviço SNMP. Você precisa do endereço de rede desse servidor (um endereço IPv4 ou IPv6), para que o monitor de eventos possa enviar mensagens de trap para esse endereço. Você pode usar mais de um servidor (até 10 servidores são permitidos).
- O arquivo de management information base (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.

  Caso não possua o arquivo MIB, você pode obtê-lo no site de suporte da NetApp:

  - Vá para "Suporte da NetApp".
  - Clique em **Downloads** e depois selecione **Downloads**.
  - Clique em **E-Series SANtricity OS Controller Software**.
  - Selecione **Download Latest Release**.
  - Faça login.
  - Aceite a declaração de cautela e o contrato de licença.
  - Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o arquivo.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos de trap atualmente definidos aparecem na tabela.

3. Selecione **Add Trap Desinations**.

   A caixa de diálogo Adicionar Destinos de Trap é aberta.

4. Insira um ou mais destinos de trap, selecione os nomes de comunidade ou nomes de usuário associados e clique em **Adicionar**.
   - **Destino da armadilha** — Insira um endereço IPv4 ou IPv6 do servidor que executa um serviço SNMP.
   - **Nome da comunidade ou nome de usuário** — No menu suspenso, selecione o nome da comunidade (SNMPv2c) ou o nome de usuário (SNMPv3) para este destino de trap. (Se você definiu apenas um, o nome já aparece neste campo.)
   - **Enviar Trap de Falha de Autenticação** — Selecione esta opção (a caixa de seleção) se desejar alertar o destino do trap sempre que uma solicitação SNMP for rejeitada devido a um nome de comunidade ou nome de usuário não reconhecido. Depois de clicar em **Adicionar**, os destinos do trap e os nomes de comunidade ou nomes de usuário associados aparecem na tabela.
5. Para garantir que um trap seja válido, selecione um destino de trap na tabela e clique em **Testar Destino do Trap** para enviar um trap de teste para o endereço configurado.

Resultados

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

Configurar variáveis MIB do SNMP no SANtricity System Manager

Para alertas SNMP, você pode opcionalmente configurar variáveis da Base de Informações de Gerenciamento (MIB) que aparecem nos traps SNMP. Essas variáveis podem retornar o nome do array de storage, a localização 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 você não tiver um arquivo MIB, poderá obtê-lo da seguinte forma:

- Vá para "Suporte da NetApp".
- Clique em **Downloads** e depois selecione **Downloads**.
- Clique em **E-Series SANtricity OS Controller Software**.
- Selecione **Download Latest Release**.
- Faça login.
- Aceite a declaração de cautela e o contrato de licença.
- Role a página para baixo até ver o arquivo MIB para o seu tipo de controlador e, em seguida, clique no link para baixar o 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 para o array de storage)
- `sysLocation` (localização do array de storage)
- `sysContact` (nome de um administrador)

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.
3. Selecione **Configurar variáveis MIB SNMP**.

   A caixa de diálogo Configurar variáveis MIB SNMP é aberta.

4. Insira um ou mais dos seguintes valores e clique em **Save**.
   - **Nome** — O valor para a variável MIB `sysName`. Por exemplo, insira um nome para o array de storage.
   - **Localização** — O valor da variável MIB `sysLocation`. Por exemplo, insira a localização do array de storage.
   - **Contato** — O valor para a variável MIB `sysContact`. Por exemplo, insira um administrador responsável pelo array de storage.

Resultados

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

Editar comunidades para traps SNMPv2c em SANtricity System Manager

Você pode editar nomes de comunidades para traps SNMPv2c.

Antes de começar

Um nome de comunidade deve ser criado.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na tabela.

3. Selecione **Configurar Communities**.
4. Digite o novo nome da comunidade e clique em **Save**. Os nomes das comunidades podem conter apenas caracteres ASCII imprimíveis.

Resultados

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

${post_edited_translations.segment}

${post_edited_translations.segment}

Antes de começar

${post_edited_translations.segment}

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na tabela.

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.

Resultados

${post_edited_translations.segment}

Adicionar comunidades para traps SNMPv2c no SANtricity System Manager

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na tabela.

3. Selecione **Configurar Communities**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione **Add another community**.
5. Digite o novo nome da comunidade e clique em **Save**.

Resultados

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

Adicionar usuários para traps SNMPv3 no SANtricity System Manager

Você pode adicionar até 256 usuários para SNMPv3 traps.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na tabela.

3. Selecione **Configurar Users**.

   A caixa de diálogo Configurar usuários SNMPv3 é aberta.

4. Selecione **Add**.
5. Insira as seguintes informações e clique em **Add**.
   - **Nome de usuário** — Digite um nome para identificar o usuário, que pode ter até 31 caracteres.
   - **ID do mecanismo** — Selecione o ID do mecanismo, 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 **Personalizado**; outro campo aparecerá onde você deverá inserir o ID do mecanismo autorizado como uma string hexadecimal, com um número par de caracteres entre 10 e 32 caracteres.
   - **Credenciais de autenticação** — Selecione um protocolo de autenticação, que garante a identidade dos usuários. Em seguida, insira uma senha de autenticação, que é necessária quando o protocolo de autenticação é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.
   - **Credenciais de privacidade** — Selecione um protocolo de privacidade, que é usado para criptografar o conteúdo das mensagens. Em seguida, insira uma senha de privacidade, que é necessária quando

o protocolo de privacidade é definido ou alterado. A senha deve ter entre 8 e 128 caracteres.

Remova comunidades para traps SNMPv2c no SANtricity System Manager

Você pode remover um nome de comunidade para traps SNMPv2c.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes das comunidades aparecem na página **Alerts**.

3. Selecione **Configurar Communities**.

   A caixa de diálogo Configurar Comunidades é aberta.

4. Selecione o nome da comunidade que deseja excluir e clique no ícone **Remover** (X) no canto direito.

   Se destinos de captura estiverem associados a esse nome de comunidade, a caixa de diálogo Confirmar Remoção da Comunidade exibirá os endereços de destino de captura afetados.

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

Resultados

O nome da comunidade e seu destino de trap associado foram removidos da página de Alertas.

Remover usuários para traps SNMPv3 em SANtricity System Manager

Você pode remover um usuário para traps SNMPv3.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os destinos das armadilhas e os nomes de usuário aparecem na página de Alerts.

3. Selecione **Configurar Users**.

   A caixa de diálogo Configurar usuários SNMPv3 é aberta.

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

Resultados

O nome de usuário e o destino de trap associados são removidos da página de Alertas.

Excluir destinos de trap no SANtricity System Manager

Você pode excluir um endereço de destino de trap para que o monitor de eventos do array de storage não envie mais traps SNMP para esse endereço.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **SNMP**.

   Os endereços de destino das armadilhas aparecem na tabela.

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

   O endereço de destino não aparece mais na página de Alertas.

Resultados

O destino de trap excluído não recebe mais traps SNMP do monitor de eventos do array de storage.

Gerenciar alertas do syslog

Configurar o servidor syslog para alertas no SANtricity System Manager

Para configurar alertas do syslog, você deve inserir o endereço de um servidor syslog e uma porta UDP. Até cinco servidores syslog são permitidos.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Esse endereço pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Essa porta normalmente é 514.

Sobre esta tarefa

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.

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

3. Clique em **Adicionar Syslog Servers**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

4. Insira as informações de um ou mais servidores syslog (máximo de cinco) e clique em **Adicionar**.
   - **Endereço do servidor** — Insira um 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 para os endereços do servidor, selecione **Test All Syslog Servers**.

Resultados

O monitor de eventos envia alertas para o servidor syslog sempre que ocorre um evento que exige alerta. Para configurar ainda mais as definições do syslog para logs de auditoria, consulte "Configurar servidor syslog

para logs de auditoria".

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

Edite os servidores syslog para alertas no SANtricity System Manager

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

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.
3. Na tabela, selecione um endereço de servidor syslog e clique no ícone **Editar** (lápis) no canto direito.

   A linha se torna um campo editável.

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

Resultados

O endereço do servidor atualizado aparece na tabela.

Adicione servidores syslog para alertas no SANtricity System Manager

Você pode adicionar no máximo cinco servidores para alertas do syslog.

Antes de começar

- O endereço do servidor syslog deve estar disponível. Esse endereço pode ser um domínio totalmente qualificado, um endereço IPv4 ou um endereço IPv6.
- O número da porta UDP do servidor syslog deve estar disponível. Essa porta normalmente é 514.

Passos

1. Selecione o menu: configurações [Alertas].
2. Selecione a guia **Syslog**.
3. Selecione **Add Syslog Servers**.

   A caixa de diálogo Adicionar Servidor syslog é aberta.

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

   - **Endereço do servidor Syslog** — Insira um 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.

Excluir servidores syslog para alertas no SANtricity System Manager

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

Passos

1. Selecione o menu: configurações [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 exclusão do servidor syslog é aberta.

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

Resultados

O servidor que você removeu não recebe mais alertas do monitor de eventos.

Perguntas frequentes sobre alertas do storage system para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

E se os alertas estiverem desativados?

Se você deseja que os administradores recebam notificações sobre eventos importantes que ocorrem no array de storage, é necessário configurar um método de alerta.

Para arrays de storage gerenciados com SANtricity System Manager, você configura alertas na página de Alertas. As notificações de alerta podem ser enviadas por e-mail, traps SNMP ou mensagens syslog. Além disso, alertas por e-mail podem ser configurados no 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 do Simple Network Management Protocol (SNMP) ou por mensagens de syslog.

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

Por que os registros de data e hora são inconsistentes entre o array de storage e os alertas?

Quando o array de storage envia alertas, ele não corrige o fuso horário do servidor ou host de destino que recebe os alertas. Em vez disso, o array de storage usa a hora local (GMT) para criar o registro de data e hora usado para o registro do alerta. Como resultado, você pode observar inconsistências entre os registros de data e hora do array de storage e do servidor ou host que recebe um alerta.

Como o array de storage não corrige o fuso horário ao enviar alertas, o registro de data e hora nos alertas é relativo ao GMT, que tem um deslocamento de fuso horário zero. Para calcular um registro de data e hora apropriado para o seu fuso horário local, você deve determinar o seu deslocamento de hora em relação ao GMT e então adicionar ou subtrair esse valor dos registros de data e hora.

Informações sobre direitos autorais

Informações sobre marcas comerciais