



# Gerenciar portas iSCSI

## SANtricity software

NetApp  
March 17, 2026

# Índice

- Gerenciar portas iSCSI ..... 1
  - Configurar as portas iSCSI no SANtricity System Manager ..... 1
  - Configurar autenticação iSCSI no SANtricity System Manager ..... 3
  - Ative as configurações de descoberta iSCSI no SANtricity System Manager ..... 5
  - Visualize pacotes de estatísticas iSCSI no SANtricity System Manager ..... 6
  - Visualizar sessões iSCSI no SANtricity System Manager ..... 7
  - Encerrar sessão iSCSI no SANtricity System Manager ..... 10
  - Configurar iSER sobre portas InfiniBand no SANtricity System Manager ..... 10
  - Visualize estatísticas de iSER sobre InfiniBand no SANtricity System Manager ..... 11

# Gerenciar portas iSCSI

## Configurar as portas iSCSI no SANtricity System Manager

Se o seu controlador incluir uma conexão de host iSCSI, você pode configurar as configurações da porta iSCSI na página Hardware.

### Antes de começar

- Seu controlador deve incluir portas iSCSI; caso contrário, as configurações de iSCSI não estarão disponíveis.
- Você deve saber a velocidade da rede (a taxa de transferência de dados entre as portas e o host).



As configurações e funções do iSCSI só aparecem se o seu array de storage for compatível com iSCSI.

### Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com as portas iSCSI que você deseja configurar.

O menu de contexto do controlador é exibido.

4. Selecione **Configurar portas iSCSI**.





A opção **Configurar portas iSCSI** só aparece se o System Manager detectar portas iSCSI no controlador.

A caixa de diálogo Configurar portas iSCSI é aberta.

5. Na lista suspensa, selecione a porta que deseja configurar e clique em **Next**.
6. Selecione as configurações da porta de configuração e clique em **Next**.

Para visualizar todas as configurações de porta, clique no link **Mostrar mais configurações de porta** à direita da caixa de diálogo.

## Detalhes do campo

Configuração da porta	Descrição
Velocidade da porta Ethernet configurada (aparece apenas para determinados tipos de placas de interface de host)	Selecione a velocidade que corresponda à capacidade de velocidade do SFP na porta.
Modo Forward Error Correction (FEC) (Aparece apenas para determinados tipos de Host Interface Cards)	Se desejar, selecione um dos modos FEC para a porta do host especificada.   O modo Reed Solomon não suporta a velocidade de porta de 25 Gbps.
Habilitar IPv4 / Habilitar IPv6	Selecione uma ou ambas as opções para ativar o suporte para redes IPv4 e IPv6.   Se você quiser desativar o acesso à porta, desmarque ambas as caixas de seleção.
Porta de escuta TCP (Disponível ao clicar em <b>Mostrar mais configurações de porta.</b> )	Se necessário, insira um novo número de porta.  A porta de escuta é o número da porta TCP que o controlador usa para escutar logins iSCSI de iniciadores iSCSI do host. A porta de escuta padrão é 3260. Você deve inserir 3260 ou um valor entre 49152 e 65535.
Tamanho do MTU (Disponível clicando em <b>Mostrar mais configurações de porta.</b> )	Se necessário, insira um novo tamanho em bytes para o Maximum Transmission Unit (MTU).  O tamanho padrão da Unidade Máxima de Transmissão (MTU) é de 1500 bytes por quadro. Você deve inserir um valor entre 1500 e 9000.
Habilitar respostas ICMP PING	Selecione esta opção para ativar o Internet Control Message Protocol (ICMP). Os sistemas operacionais de computadores em rede usam esse protocolo para enviar mensagens. Essas mensagens ICMP determinam se um host está acessível e quanto tempo leva para enviar e receber pacotes desse host.

Se você selecionou **Habilitar IPv4**, uma caixa de diálogo é aberta para selecionar as configurações de IPv4 após você clicar em **Avançar**. Se você selecionou **Habilitar IPv6**, uma caixa de diálogo é aberta para selecionar as configurações de IPv6 após você clicar em **Avançar**. Se você selecionou ambas as opções, a caixa de diálogo para as configurações de IPv4 é aberta primeiro e, em seguida, após você clicar em **Avançar**, a caixa de diálogo para as configurações de IPv6 é aberta.

- Configure as definições de IPv4 e/ou IPv6, automática ou manualmente. Para ver todas as configurações de porta, clique no link **Mostrar mais configurações** à direita da caixa de diálogo.

## Detalhes do campo

Configuração da porta	Descrição
Obter configuração automaticamente	Selecione esta opção para obter a configuração automaticamente.
Especificar manualmente a configuração estática	Selecione esta opção e, em seguida, insira um endereço estático nos campos. (Se desejar, você pode copiar e colar endereços nos campos.) Para IPv4, inclua a máscara de sub-rede e o gateway. Para IPv6, inclua o endereço IP roteável e o endereço IP do roteador.
Ative o suporte a VLAN (Disponível ao clicar em <b>Mostrar mais configurações.</b> )	Selecione esta opção para ativar uma VLAN e insira seu ID. Uma VLAN é uma rede lógica que se comporta como se estivesse fisicamente separada de outras redes locais (LANs) físicas e virtuais suportadas pelos mesmos switches, pelos mesmos roteadores ou por ambos.
Ative a prioridade Ethernet (Disponível ao clicar em <b>Mostrar mais configurações.</b> )	<p>Selecione esta opção para ativar o parâmetro que determina a prioridade de acesso à rede. Use o controle deslizante para selecionar uma prioridade entre 1 (mais baixa) e 7 (mais alta).</p> <p>Em um ambiente de rede local (LAN) compartilhada, como Ethernet, várias estações podem disputar o acesso à rede. O acesso é feito por ordem de chegada. Duas estações podem tentar acessar a rede ao mesmo tempo, o que faz com que ambas recuem e esperem antes de tentar novamente. Esse processo é minimizado para Ethernet comutado, onde apenas uma estação é conectada a uma porta do switch.</p>

8. Clique em **Concluir**.

## Configurar autenticação iSCSI no SANtricity System Manager

Para maior segurança em uma rede iSCSI, você pode configurar autenticação entre controladores (alvos) e hosts (iniciadores).

System Manager usa o método Challenge Handshake Authentication Protocol (CHAP), que valida a identidade dos targets e initiators durante o link inicial. A autenticação é baseada em uma chave de segurança compartilhada chamada *CHAP secret*.

### Antes de começar

Você pode definir o segredo CHAP para os iniciadores (iSCSI hosts) antes ou depois de definir o segredo CHAP para os alvos (controladores). Antes de seguir as instruções desta tarefa, você deve aguardar até que os hosts tenham feito uma conexão iSCSI primeiro e, em seguida, definir o segredo CHAP nos hosts individuais. Após as conexões serem feitas, os nomes IQN dos hosts e seus segredos CHAP são listados na caixa de diálogo para autenticação iSCSI (descrita nesta tarefa), e você não precisa digitá-los manualmente.

### Sobre esta tarefa

Você pode selecionar um dos seguintes métodos de autenticação:

- **Autenticação unidirecional** — Use esta configuração para permitir que o controlador autentique a identidade dos hosts iSCSI (autenticação unidirecional).
- **Two-way authentication** — Use esta configuração para permitir que tanto o controlador quanto os hosts iSCSI realizem autenticação (autenticação bidirecional). Esta configuração fornece um segundo nível de segurança, permitindo que o controlador autentique a identidade dos hosts iSCSI e, por sua vez, que os hosts iSCSI autentiquem a identidade do controlador.



As configurações e funções do iSCSI só são exibidas na página Configurações se o seu array de storage for compatível com iSCSI.

## Passos

1. Selecione o menu: configurações [Sistema].
2. Em Configurações iSCSI, clique em **Configurar autenticação**.

A caixa de diálogo Configurar autenticação é exibida, mostrando o método atualmente configurado. Ela também mostra se algum host possui segredos CHAP configurados.

3. Selecione uma das seguintes opções:
  - **Sem autenticação** — Se você não deseja que o controlador autentique a identidade dos iSCSI hosts, selecione esta opção e clique em **Concluir**. A caixa de diálogo será fechada e você terá concluído a configuração.
  - **One-way autenticação** — Para permitir que o controlador autentique a identidade dos hosts iSCSI, selecione esta opção e clique em **Next** para exibir a caixa de diálogo Configurar Target CHAP.
  - **Two-way authentication** — Para permitir que tanto o controlador quanto os hosts iSCSI realizem autenticação, selecione esta opção e clique em **Avançar** para exibir a caixa de diálogo Configurar CHAP de destino.
4. Para autenticação unidirecional ou bidirecional, insira ou confirme o segredo CHAP do controlador (o alvo). O segredo CHAP deve ter entre 12 e 57 caracteres ASCII imprimíveis.



Se o segredo CHAP do controlador já tiver sido configurado anteriormente, os caracteres no campo são mascarados. Se necessário, você pode substituir os caracteres existentes (os novos caracteres não são mascarados).

5. Faça uma das seguintes ações:
  - Se você estiver configurando autenticação *unidirecional*, clique em **Concluir**. A caixa de diálogo será fechada e a configuração estará finalizada.
  - Se você estiver configurando autenticação *bidirecional*, clique em **Avançar** para exibir a caixa de diálogo Configurar CHAP do Iniciador.
6. Para autenticação bidirecional, insira ou confirme um segredo CHAP para qualquer um dos hosts iSCSI (os iniciadores), que pode ter entre 12 e 57 caracteres ASCII imprimíveis. Se você não quiser configurar autenticação bidirecional para um host específico, deixe o campo Segredo CHAP do Iniciador em branco.



Se o segredo CHAP de um host já tiver sido configurado anteriormente, os caracteres no campo são mascarados. Se necessário, você pode substituir os caracteres existentes (os novos caracteres não são mascarados).

7. Clique em **Concluir**.

## Resultados

A autenticação ocorre durante a sequência de login iSCSI entre os controladores e os hosts iSCSI, a menos que você tenha especificado nenhuma autenticação.

## Ative as configurações de descoberta iSCSI no SANtricity System Manager

Você pode habilitar configurações relacionadas à descoberta de dispositivos de armazenamento em uma rede iSCSI.

As Configurações de Descoberta de Destino permitem que você registre as informações iSCSI do array de storage usando o protocolo Internet Storage Name Service (iSNS) e também determine se deve permitir sessões de descoberta sem nome.

### Antes de começar

Se o servidor iSNS usar um endereço IP estático, esse endereço deverá estar disponível para o registro no iSNS. Tanto IPv4 quanto IPv6 são suportados.

### Sobre esta tarefa

Você pode habilitar as seguintes configurações relacionadas à descoberta iSCSI:

- **Habilitar o servidor iSNS para registrar um alvo** — Quando habilitado, o array de storage registra seu Nome Qualificado iSCSI (IQN) e informações de porta no servidor iSNS. Essa configuração permite a descoberta iSNS, para que um iniciador possa recuperar o IQN e as informações de porta do servidor iSNS.
- **Habilitar sessões de descoberta sem nome** — Quando as sessões de descoberta sem nome estão habilitadas, o iniciador (host iSCSI) não precisa fornecer o IQN do alvo (controlador) durante a sequência de login para uma conexão do tipo descoberta. Quando desabilitadas, os hosts precisam fornecer o IQN para estabelecer uma sessão de descoberta com o controlador. No entanto, o IQN do alvo é sempre necessário para uma sessão normal (com suporte a E/S). Desabilitar essa configuração pode impedir que hosts iSCSI não autorizados se conectem ao controlador usando apenas seu endereço IP.



As configurações e funções do iSCSI só são exibidas na página Configurações se o seu array de storage for compatível com iSCSI.

### Passos

1. Selecione o menu: configurações [Sistema].
2. Em **configurações iSCSI**, clique em **Exibir/Editar configurações de descoberta de destino**.

A caixa de diálogo Configurações de Descoberta de Destino é exibida. Abaixo do campo **Ativar servidor iSNS...**, a caixa de diálogo indica se o controlador já está registrado.

3. Para registrar o controlador, selecione **Habilitar servidor iSNS para registrar meu destino** e, em seguida, selecione uma das seguintes:
  - **Obter configuração automaticamente do servidor DHCP** — Selecione esta opção se você quiser configurar o servidor iSNS usando um servidor DHCP (Dynamic Host Configuration Protocol). Esteja ciente de que, se você usar esta opção, todas as portas iSCSI no controlador também devem ser configuradas para usar DHCP. Se necessário, atualize as configurações da porta iSCSI do controlador para habilitar esta opção.



Para que o servidor DHCP forneça o endereço do servidor iSNS, você deve configurar o servidor DHCP para usar a Opção 43 — “Vendor Specific Information.” Esta opção precisa conter o endereço IPv4 do servidor iSNS nos bytes de dados 0xa-0xd (10-13).

- **Especificar configuração estática manualmente** — Selecione esta opção se você quiser inserir um endereço IP estático para o servidor iSNS. (Se desejar, você pode cortar e colar endereços nos campos.) No campo, insira um endereço IPv4 ou um endereço IPv6. Se você configurou ambos, IPv4 é o padrão. Insira também uma porta TCP de escuta (use o padrão 3205 ou insira um valor entre 49152 e 65535).

4. `#{post_edited_translations.segment}`

- `#{post_edited_translations.segment}`
- Quando desabilitado, as sessões de descoberta são impedidas, a menos que o iniciador forneça o IQN de destino. Desabilitar sessões de descoberta sem nome fornece segurança adicional.

5. Clique em **Salvar**.

## Resultados

Uma barra de progresso aparece enquanto o System Manager tenta registrar o controlador com o servidor iSNS. Este processo pode levar até cinco minutos.

# Visualize pacotes de estatísticas iSCSI no SANtricity System Manager

Você pode visualizar dados sobre as conexões iSCSI com seu array de storage.

## Sobre esta tarefa

System Manager exibe esses tipos de estatísticas iSCSI. Todas as estatísticas são somente leitura e não podem ser definidas.



Os tipos de estatísticas exibidos no System Manager são baseados nas estatísticas disponíveis para o seu array de storage.

- **Ethernet MAC estatísticas** — Fornece estatísticas para o controle de acesso à mídia (MAC). MAC também fornece um mecanismo de endereçamento chamado endereço físico ou endereço MAC. O endereço MAC é um endereço exclusivo atribuído a cada adaptador de rede. O endereço MAC ajuda a entregar pacotes de dados a um destino dentro da sub-rede.
- **Estatísticas Ethernet TCP/IP** — Fornece estatísticas para o TCP/IP, que é o Transmission Control Protocol (TCP) e o Internet Protocol (IP) para o dispositivo iSCSI. Com o TCP, aplicativos em hosts em rede podem criar conexões entre si, pelas quais podem trocar dados em pacotes. O IP é um protocolo orientado a dados que comunica dados através de uma inter-rede comutação de pacotes. As estatísticas IPv4 e as estatísticas IPv6 são exibidas separadamente.
- **Ethernet Kernel statistics** — Fornece estatísticas para os drivers do kernel da plataforma do dispositivo iSCSI. As estatísticas do kernel exibem dados de rede semelhantes aos da opção de estatísticas TCP/IP. No entanto, os dados das estatísticas do kernel são coletados dos drivers do kernel da plataforma, em vez de diretamente do hardware iSCSI.
- **Estatísticas do destino/iniciador local (protocolo)** — Exibe estatísticas do destino iSCSI, que fornece acesso em nível de bloco à sua mídia de armazenamento, e mostra as estatísticas iSCSI do array de storage quando usado como iniciador em operações de espelhamento assíncrono.
- **DCBX Operational States estatísticas** — Exibe os estados operacionais dos vários recursos do Data

Center Bridging Exchange (DCBX).

- **LLDP TLV estatísticas** — Exibe as estatísticas do Link Layer Discovery Protocol (LLDP) Type Length Value (TLV).
- **DCBX TLV estatísticas** — Exibe as informações que identificam as portas do host do array de storage em um ambiente de Data Center Bridging (DCB). Essas informações são compartilhadas com os pares da rede para fins de identificação e capacidade.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

#### Passos

1. Selecione menu: guia Suporte [Support Center > Diagnostics].
2. Selecione **Exibir pacotes de estatísticas iSCSI**.
3. Clique em uma aba para visualizar os diferentes conjuntos de estatísticas.
4. Para definir a linha de base, clique em **Set new baseline**.

A definição da linha de base estabelece um novo ponto de partida para a coleta das estatísticas. A mesma linha de base é usada para todas as estatísticas iSCSI.

## Visualizar sessões iSCSI no SANtricity System Manager

Você pode visualizar informações detalhadas sobre as conexões iSCSI com seu array de storage. As sessões iSCSI podem ocorrer com hosts ou arrays de storage remotos em uma relação de espelhamento assíncrono.

#### Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Visualizar/Encerrar sessões iSCSI**.

Uma lista das sessões iSCSI atuais aparece.

3. **Opcional:** Para ver informações adicionais sobre uma sessão iSCSI específica, selecione uma sessão e clique em **Ver detalhes**.

## Detalhes do campo

Item	Descrição
Identificador de sessão (SSID)	Uma sequência hexadecimal que identifica uma sessão entre um iniciador iSCSI e um destino iSCSI. O SSID é composto pelo ISID e pelo TPGT.
Session ID do iniciador (ISID)	A parte do iniciador do identificador de sessão. O iniciador especifica o ISID durante o login.
Grupo de portais alvo	O destino iSCSI.
Tag de grupo de portal de destino (TPGT)	A parte de destino do identificador de sessão. Um identificador numérico de 16 bits para um grupo de portais de destino iSCSI.
Nome do iniciador iSCSI	O nome exclusivo mundial do iniciador.
Rótulo do iniciador iSCSI	O rótulo do usuário definido no System Manager.
Alias do iniciador iSCSI	Um nome que também pode ser associado a um nó iSCSI. O alias permite que uma organização associe uma string amigável ao nome iSCSI. No entanto, o alias não substitui o nome iSCSI. O alias do iniciador iSCSI só pode ser definido no host, não no System Manager
Host	Um servidor que envia entrada e saída para o array de storage.
ID de conexão (CID)	Um nome único para uma conexão dentro da sessão entre o iniciador e o destino. O iniciador gera esse ID e o apresenta ao destino durante solicitações de login. O ID da conexão também é apresentado durante logouts que encerram conexões.
Identificador da porta	A porta do controlador associada à conexão.
Endereço IP do iniciador	O endereço IP do iniciador.
Parâmetros de login negociados	Os parâmetros que são transacionados durante o login da sessão iSCSI.
Método de autenticação	A técnica para autenticar usuários que desejam acessar a rede iSCSI. Os valores válidos são <b>CHAP</b> e <b>None</b> .
Método de resumo do cabeçalho	A técnica para exibir os possíveis valores de cabeçalho para a sessão iSCSI. HeaderDigest e DataDigest podem ser <b>None</b> ou <b>CRC32C</b> . O valor padrão para ambos é <b>None</b> .

Item	Descrição
Método de resumo de dados	A técnica para exibir os possíveis valores de dados para a sessão iSCSI. HeaderDigest e DataDigest podem ser <b>None</b> ou <b>CRC32C</b> . O valor padrão para ambos é <b>None</b> .
Conexões máximas	O maior número de conexões permitido para a sessão iSCSI. O número máximo de conexões pode ser de 1 a 4. O valor padrão é <b>1</b> .
Alias de destino	O rótulo associado ao destino.
Alias do iniciador	O rótulo associado ao iniciador.
Endereço IP de destino	O endereço IP do destino para a sessão iSCSI. Nomes DNS não são suportados.
R2T inicial	O status inicial de pronto para transferência. O status pode ser <b>Sim</b> ou <b>Não</b> .
Comprimento máximo de rajada	A carga máxima SCSI em bytes para esta sessão iSCSI. O comprimento máximo do burst pode ser de 512 a 262.144 (256 KB). O valor padrão é <b>262.144 (256 KB)</b> .
Primeira duração da rajada	A carga SCSI em bytes para dados não solicitados para esta sessão iSCSI. O comprimento da primeira rajada pode ser de 512 a 131.072 (128 KB). O valor padrão é <b>65.536 (64 KB)</b> .
Tempo de espera padrão	O número mínimo de segundos a aguardar antes de tentar estabelecer uma conexão após o término ou a reinicialização de uma conexão. O valor padrão para o tempo de espera pode variar de 0 a 3600. O padrão é <b>2</b> .
Tempo padrão de retenção	O número máximo de segundos que a conexão ainda é possível após o término ou a reinicialização da conexão. O tempo padrão de retenção pode ser de 0 a 3600. O valor padrão é <b>20</b> .
Máximo de R2T pendente	O número máximo de "prontos para transferência" pendentes para esta sessão iSCSI. O valor máximo de prontos para transferência pendentes pode ser de 1 a 16. O padrão é <b>1</b> .
Nível de recuperação de erros	O nível de recuperação de erros para esta sessão iSCSI. O valor do nível de recuperação de erros é sempre definido como <b>0</b> .
Comprimento máximo do segmento de dados recebidos	A quantidade máxima de dados que o iniciador ou o destino podem receber em qualquer unidade de dados de carga (PDU) iSCSI.
Nome do destino	O nome oficial do destino (não o pseudônimo). O nome do destino no formato <i>iqn</i> .

Item	Descrição
Nome do iniciador	O nome oficial do iniciador (não o alias). O nome do iniciador que usa o formato <i>iqn</i> ou <i>eui</i> .

4. **Opcional:** Para salvar o relatório em um arquivo, clique em **Save**.

O arquivo está salvo na pasta Downloads do seu navegador com o nome de arquivo `iscsi-session-connections.txt`.

## Encerrar sessão iSCSI no SANtricity System Manager

Você pode encerrar uma sessão iSCSI que não seja mais necessária. As sessões iSCSI podem ocorrer com hosts ou arrays de storage remotos em uma relação de espelhamento assíncrono.

### Sobre esta tarefa

Você pode querer encerrar uma sessão iSCSI pelos seguintes motivos:

- **Acesso não autorizado** — Se um iniciador iSCSI estiver conectado e não deveria ter acesso, você pode encerrar a sessão iSCSI para forçar o iniciador iSCSI a sair do array de storage. O iniciador iSCSI pode ter se conectado porque o método de autenticação None estava disponível.
- **Tempo de inatividade do sistema** — Se você precisar desligar um array de storage e perceber que os iniciadores iSCSI ainda estão conectados, você pode encerrar as sessões iSCSI para desconectá-los do array de storage.

### Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Visualizar/Encerrar sessões iSCSI**.

Uma lista das sessões iSCSI atuais aparece.

3. Selecione a sessão que você deseja encerrar.
4. Clique em **Encerrar sessão** e confirme que deseja realizar a operação.

## Configurar iSER sobre portas InfiniBand no SANtricity System Manager

Se o seu controlador incluir uma porta iSER sobre InfiniBand, você pode configurar a conexão de rede com o host.

### Antes de começar

- Seu controlador deve incluir uma porta iSER sobre InfiniBand; caso contrário, as configurações de iSER sobre InfiniBand não estarão disponíveis no System Manager.
- Você deve saber o endereço IP da conexão do host.

### Passos

1. Selecione **Hardware**.
2. Se a imagem mostrar as unidades, clique na guia **Controllers & Components**.

O gráfico muda para mostrar os controladores em vez das unidades de disco.

3. Clique no controlador com a porta iSER sobre InfiniBand que você deseja configurar.

O menu de contexto do controlador é exibido.

4. Selecione **Configurar iSER em InfiniBand ports**.

A caixa de diálogo Configurar iSER sobre InfiniBand portas é aberta.

5. Na lista suspensa, selecione a porta HIC que deseja configurar e insira o endereço IP do host.
6. Clique em **Configurar**.
7. Conclua a configuração e, em seguida, reinicie a porta iSER sobre InfiniBand clicando em **Sim**.

## Visualize estatísticas de iSER sobre InfiniBand no SANtricity System Manager

Se o controlador do seu array de storage incluir uma porta iSER sobre InfiniBand, você pode visualizar dados sobre as conexões do host.

### Sobre esta tarefa

System Manager exibe os seguintes tipos de estatísticas de iSER sobre InfiniBand. Todas as estatísticas são somente leitura e não podem ser definidas.

- **Estatísticas do alvo local (protocolo)** — Fornece estatísticas para o iSER sobre InfiniBand alvo, mostrando o acesso em nível de bloco à sua mídia de armazenamento.
- **iSER sobre estatísticas da interface InfiniBand** — Fornece estatísticas para todas as portas iSER na interface InfiniBand, incluindo estatísticas de desempenho e informações sobre erros de link associadas a cada porta do switch.

Você pode visualizar cada uma dessas estatísticas como estatísticas brutas ou como estatísticas de linha de base. Estatísticas brutas são todas as estatísticas que foram coletadas desde que os controladores foram iniciados. Estatísticas de linha de base são estatísticas de ponto no tempo que foram coletadas desde que você definiu o tempo de linha de base.

### Passos

1. Selecione o menu: configurações [Sistema].
2. Selecione **Exibir iSER em InfiniBand Estatísticas**.
3. Clique em uma aba para visualizar os diferentes conjuntos de estatísticas.
4. **Opcional:** Para definir a linha de base, clique em **Definir nova linha de base**.

A definição da linha de base estabelece um novo ponto de partida para a coleta das estatísticas. A mesma linha de base é usada para todas as estatísticas de iSER sobre InfiniBand.

## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.