



Gerenciar conexões de suporte

Element Software

NetApp

November 12, 2025

This PDF was generated from https://docs.netapp.com/pt-br/element-software-128/mnode/task_mnode_enable_node_troubleshooting_sessions.html on November 12, 2025. Always check docs.netapp.com for the latest.

Índice

Gerenciar conexões de suporte	1
Acessando nós de armazenamento usando SSH para solução de problemas básicos	1
Solucionar problemas em um nó de cluster	2
Solucione problemas em um nó de cluster com o suporte da NetApp	3
Solucionar problemas em um nó que não faz parte do cluster	5
Inicie uma sessão de suporte remoto da NetApp	5
Encontre mais informações	6
Gerenciar a funcionalidade SSH no nó de gerenciamento	6
Desative ou ative a funcionalidade SSH no nó de gerenciamento usando a interface de usuário do NetApp Hybrid Cloud Control.	7
Desative ou ative a funcionalidade SSH no nó de gerenciamento usando APIs.	7
Determine o status da capacidade SSH no nó de gerenciamento usando APIs.	8

Gerenciar conexões de suporte

Acessando nós de armazenamento usando SSH para solução de problemas básicos

A partir do Element 12.5, você pode usar a conta de sistema `sfsreadonly` nos nós de armazenamento para solução de problemas básicos. Você também pode habilitar e abrir o acesso remoto por túnel de suporte para o Suporte da NetApp para solução de problemas avançados.

A conta de sistema `sfsreadonly` permite o acesso para executar comandos básicos de solução de problemas do sistema Linux e da rede, incluindo `ping`.



A menos que seja instruído pelo Suporte da NetApp, quaisquer alterações neste sistema não são suportadas, anulando seu contrato de suporte e podendo resultar em instabilidade ou inacessibilidade dos dados.

Antes de começar

- **Permissões de escrita:** Verifique se você tem permissões de escrita no diretório de trabalho atual.
- **(Opcional) Gere seu próprio par de chaves:** Execute `ssh-keygen` do Windows 10, MacOS ou distribuição Linux. Esta é uma ação única para criar um par de chaves de usuário, que pode ser reutilizado em futuras sessões de resolução de problemas. Você pode usar certificados associados a contas de funcionários, o que também funcionaria nesse modelo.
- **Habilite a funcionalidade SSH no nó de gerenciamento:** Para habilitar a funcionalidade de acesso remoto no modo de gerenciamento, consulte ["este tópico"](#). Para os serviços de gerenciamento 2.18 e posteriores, a capacidade de acesso remoto está desativada no nó de gerenciamento por padrão.
- **Habilite a funcionalidade SSH no cluster de armazenamento:** Para habilitar a funcionalidade de acesso remoto nos nós do cluster de armazenamento, consulte ["este tópico"](#).
- **Configuração do firewall:** Se o seu nó de gerenciamento estiver atrás de um servidor proxy, as seguintes portas TCP são necessárias no arquivo `sshd.config`:

Porta TCP	Descrição	Direção da conexão
443	Chamadas de API/HTTPS para encaminhamento reverso de portas via túnel de suporte aberto para a interface web.	Nó de gerenciamento para nós de armazenamento
22	Acesso de login SSH	do nó de gerenciamento para os nós de armazenamento ou dos nós de armazenamento para o nó de gerenciamento.

Opções de resolução de problemas

- [Solucionar problemas em um nó de cluster](#)
- [Solucione problemas em um nó de cluster com o suporte da NetApp.](#)
- [Solucionar problemas em um nó que não faz parte do cluster.](#)

Solucionar problemas em um nó de cluster

Você pode realizar a solução de problemas básicos usando a conta de sistema somente leitura (sfireadonly):

Passos

1. Acesse o nó de gerenciamento via SSH usando as credenciais de login da conta que você selecionou ao instalar a máquina virtual do nó de gerenciamento.
2. No nó de gerenciamento, acesse `/sf/bin`.
3. Encontre o script apropriado para o seu sistema:
 - `SignSshKeys.ps1`
 - `SignSshKeys.py`
 - `SignSshKeys.sh`



O arquivo `SignSshKeys.ps1` depende do PowerShell 7 ou posterior e o arquivo `SignSshKeys.py` depende do Python 3.6.0 ou posterior. ["módulo de solicitações"](#).

O `SignSshKeys` script escreve `user`, `user.pub`, e `user-cert.pub` arquivos no diretório de trabalho atual, que são posteriormente usados pelo `ssh` comando. No entanto, quando um arquivo de chave pública é fornecido ao script, apenas um `<public_key>` arquivo (com `<public_key>` substituído pelo prefixo do arquivo de chave pública passado para o script) é gravado no diretório.

4. Execute o script no nó de gerenciamento para gerar o chaveiro SSH. O script habilita o acesso SSH usando a conta de sistema `sfireadonly` em todos os nós do cluster.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

- a. Substitua o valor entre colchetes `[ ]` (incluindo os colchetes) para cada um dos seguintes parâmetros:



Você pode usar o parâmetro de forma abreviada ou completa.

- **--ip | -i [endereço IP]**: Endereço IP do nó de destino no qual a API será executada.
 - **--user | -u [nome de usuário]**: Usuário do cluster usado para executar a chamada da API.
 - **(Opcional) --duration | -d [horas]**: A duração em que uma chave assinada deve permanecer válida, como um número inteiro em horas. O padrão é 24 horas.
 - **(Opcional) --publickey | -k [caminho da chave pública]**: O caminho para uma chave pública, caso o usuário opte por fornecer uma.
- b. Compare sua entrada com o seguinte comando de exemplo. Neste exemplo, `10.116.139.195` é o endereço IP do nó de armazenamento, `admin` é o nome de usuário do cluster e a duração da validade da chave é de duas horas:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Execute o comando.

5. Conecte-se via SSH aos endereços IP dos nós:

```
ssh -i user sfreadonly@[node_ip]
```

Você poderá executar comandos básicos de solução de problemas de sistema e rede Linux, como: `ping` e outros comandos somente leitura.

6. (Opcional) Desativar "[funcionalidade de acesso remoto](#)" novamente após a conclusão da resolução de problemas.



O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração com SSH habilitado permanece no nó de gerenciamento durante atualizações e upgrades até ser desabilitada manualmente.

Solucione problemas em um nó de cluster com o suporte da NetApp.

O suporte da NetApp pode realizar diagnósticos avançados com uma conta de sistema que permite ao técnico executar diagnósticos mais aprofundados do Element.

Passos

1. Acesse o nó de gerenciamento via SSH usando as credenciais de login da conta que você selecionou ao instalar a máquina virtual do nó de gerenciamento.
2. Execute o primeiro comando com o número da porta enviado pelo Suporte da NetApp para abrir o túnel de suporte:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

O suporte da NetApp fará login no seu nó de gerenciamento usando o túnel de suporte.

3. No nó de gerenciamento, acesse `/sf/bin`.
4. Encontre o script apropriado para o seu sistema:
 - SignSshKeys.ps1
 - SignSshKeys.py
 - SignSshKeys.sh



O arquivo SignSshKeys.ps1 depende do PowerShell 7 ou posterior e o arquivo SignSshKeys.py depende do Python 3.6.0 ou posterior. "[módulo de solicitações](#)".

O SignSshKeys script escreve `user`, `user.pub`, e `user-cert.pub` arquivos no diretório de trabalho atual, que são posteriormente usados pelo `ssh` comando. No entanto, quando um arquivo de chave pública é fornecido ao script, apenas um `<public_key>` arquivo (com `<public_key>` substituído pelo prefixo do arquivo de chave pública passado para o script) é gravado no diretório.

5. Execute o script para gerar o chaveiro SSH com o `--sfadmin` bandeira. O script habilita o SSH em todos os nós.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Para acessar via SSH como `--sfadmin` Para um nó em cluster, você deve gerar o chaveiro SSH usando um `--user` com `supportAdmin` Acesso ao cluster.

Para configurar `supportAdmin` Para acessar as contas de administrador do cluster, você pode usar a interface do usuário do Element ou as APIs:



- "Configure o acesso "supportAdmin" usando a interface do usuário do Element."
- Configurar `supportAdmin` Acesso por meio de APIs e adição de "supportAdmin" como o "access" Digite na solicitação da API:
 - "Configure o acesso "supportAdmin" para uma nova conta."
 - "Configure o acesso "supportAdmin" para uma conta existente."

Para obter o `clusterAdminID`, você pode usar o "Lista de administradores do cluster" API.

Para adicionar `supportAdmin` Para acessar, você precisa ter privilégios de administrador de cluster ou administrador.

- a. Substitua o valor entre colchetes [] (incluindo os colchetes) para cada um dos seguintes parâmetros:



Você pode usar o parâmetro de forma abreviada ou completa.

- `--ip` | `-i` [endereço IP]: Endereço IP do nó de destino no qual a API será executada.
- `--user` | `-u` [nome de usuário]: Usuário do cluster usado para executar a chamada da API.
- (Opcional) `--duration` | `-d` [horas]: A duração em que uma chave assinada deve permanecer válida, como um número inteiro em horas. O padrão é 24 horas.

- b. Compare sua entrada com o seguinte comando de exemplo. Neste exemplo, `192.168.0.1` é o endereço IP do nó de armazenamento, `admin` é o nome de usuário do cluster, a duração da validade da chave é de duas horas, e `--sfadmin` Permite o acesso do nó de suporte da NetApp para resolução de problemas:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

- c. Execute o comando.

6. Conecte-se via SSH aos endereços IP dos nós:

```
ssh -i user sfadmin@[node_ip]
```

7. Para fechar o túnel de suporte remoto, digite o seguinte:

```
rst --killall
```

8. (Opcional) Desativar ["funcionalidade de acesso remoto"](#) novamente após a conclusão da resolução de problemas.



O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração com SSH habilitado permanece no nó de gerenciamento durante atualizações e upgrades até ser desabilitada manualmente.

Solucionar problemas em um nó que não faz parte do cluster.

Você pode realizar a solução de problemas básicos em um nó que ainda não foi adicionado a um cluster. Você pode usar a conta de sistema `sfreadonly` para essa finalidade, com ou sem a ajuda do suporte da NetApp . Se você tiver um nó de gerenciamento configurado, poderá usá-lo para SSH e executar o script fornecido para esta tarefa.

1. A partir de um computador Windows, Linux ou Mac que tenha um cliente SSH instalado, execute o script apropriado para o seu sistema, fornecido pelo Suporte da NetApp .
2. Conecte-se ao endereço IP do nó via SSH:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Opcional) Desativar ["funcionalidade de acesso remoto"](#) novamente após a conclusão da resolução de problemas.



O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração com SSH habilitado permanece no nó de gerenciamento durante atualizações e upgrades até ser desabilitada manualmente.

Encontre mais informações

- ["Plug-in NetApp Element para vCenter Server"](#)
- ["Documentação NetApp HCI"](#)

Inicie uma sessão de suporte remoto da NetApp.

Caso necessite de suporte técnico para o seu sistema de armazenamento all-flash SolidFire , o Suporte da NetApp pode conectar-se remotamente ao seu sistema. Para iniciar uma sessão e obter acesso remoto, o Suporte da NetApp pode abrir uma conexão SSH (Secure Shell) reversa em seu ambiente.

Você pode abrir uma porta TCP para uma conexão de túnel reverso SSH com o suporte da NetApp . Essa conexão permite que o suporte da NetApp faça login no seu nó de gerenciamento.

Antes de começar

- Para os serviços de gerenciamento 2.18 e posteriores, a capacidade de acesso remoto está desativada no nó de gerenciamento por padrão. Para ativar a funcionalidade de acesso remoto, consulte ["Gerenciar a](#)

[funcionalidade SSH no nó de gerenciamento](#) .

- Se o seu nó de gerenciamento estiver atrás de um servidor proxy, as seguintes portas TCP são necessárias no arquivo sshd.config:

Porta TCP	Descrição	Direção da conexão
443	Chamadas de API/HTTPS para encaminhamento reverso de portas via túnel de suporte aberto para a interface web.	Nó de gerenciamento para nós de armazenamento
22	Acesso de login SSH	do nó de gerenciamento para os nós de armazenamento ou dos nós de armazenamento para o nó de gerenciamento.

Passos

- Faça login no seu nó de gerenciamento e abra uma sessão de terminal.
- Quando solicitado, digite o seguinte:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Para fechar o túnel de suporte remoto, digite o seguinte:

```
rst --killall
```

- (Opcional) Desativar ["funcionalidade de acesso remoto"](#) de novo.



O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração com SSH habilitado permanece no nó de gerenciamento durante atualizações e upgrades até ser desabilitada manualmente.

Encontre mais informações

- ["Plug-in NetApp Element para vCenter Server"](#)
- ["Documentação do SolidFire e do Element Software"](#)

Gerenciar a funcionalidade SSH no nó de gerenciamento

Você pode desativar, reativar ou determinar o status da funcionalidade SSH no nó de gerenciamento (mNode) usando a API REST. Capacidade SSH que fornece ["Acesso à sessão do túnel de suporte remoto \(RST\) do Suporte NetApp"](#) Está desativado por padrão em nós de gerenciamento que executam serviços de gerenciamento versão 2.18 ou posterior.

A partir da versão 2.20.69 do Management Services, você pode habilitar e desabilitar a funcionalidade SSH no nó de gerenciamento usando a interface de usuário do NetApp Hybrid Cloud Control.

O que você vai precisar

- **Permissões do NetApp Hybrid Cloud Control:** Você tem permissões como administrador.
- **Permissões de administrador do cluster:** Você tem permissões de administrador no cluster de armazenamento.
- **Software Element:** Seu cluster está executando o software NetApp Element 11.3 ou posterior.
- **Nó de gerenciamento:** Você implantou um nó de gerenciamento executando a versão 11.3 ou posterior.
- **Atualizações sobre serviços de gestão:**
 - Para usar a interface de usuário do NetApp Hybrid Cloud Control, você atualizou seu ["pacote de serviços de gestão"](#) para a versão 2.20.69 ou posterior.
 - Para usar a interface de usuário da API REST, você atualizou seu ["pacote de serviços de gestão"](#) para a versão 2.17.

Opções

- [Desative ou ative a funcionalidade SSH no nó de gerenciamento usando a interface de usuário do NetApp Hybrid Cloud Control.](#)

Você pode realizar qualquer uma das seguintes tarefas depois de...["autenticar"](#) :

- [Desative ou ative a funcionalidade SSH no nó de gerenciamento usando APIs.](#)
- [Determine o status da capacidade SSH no nó de gerenciamento usando APIs.](#)

Desative ou ative a funcionalidade SSH no nó de gerenciamento usando a interface de usuário do NetApp Hybrid Cloud Control.

Você pode desativar ou reativar a funcionalidade SSH no nó de gerenciamento. Capacidade SSH que fornece ["Acesso à sessão do túnel de suporte remoto \(RST\) do Suporte NetApp"](#) Está desativado por padrão em nós de gerenciamento que executam serviços de gerenciamento versão 2.18 ou posterior. Desativar o SSH não encerra nem desconecta as sessões de clientes SSH existentes no nó de gerenciamento. Se você desativar o SSH e optar por reativá-lo posteriormente, poderá fazê-lo usando a interface de usuário do NetApp Hybrid Cloud Control.



Para habilitar ou desabilitar o acesso de suporte usando SSH para um cluster de armazenamento, você deve usar o ["Página de configurações do cluster Element UI"](#) .

Passos

1. No painel de controle, selecione o menu de opções no canto superior direito e selecione **Configurar**.
2. Na tela **Suporte de acesso para o nó de gerenciamento**, ative a opção para habilitar o SSH do nó de gerenciamento.
3. Após concluir a resolução de problemas, na tela **Acesso de suporte para o nó de gerenciamento**, alterne a chave para desativar o SSH do nó de gerenciamento.

Desative ou ative a funcionalidade SSH no nó de gerenciamento usando APIs.

Você pode desativar ou reativar a funcionalidade SSH no nó de gerenciamento. Capacidade SSH que fornece ["Acesso à sessão do túnel de suporte remoto \(RST\) do Suporte NetApp"](#) Está desativado por padrão em nós de gerenciamento que executam serviços de gerenciamento versão 2.18 ou posterior. Desativar o SSH não encerra nem desconecta as sessões de clientes SSH existentes no nó de gerenciamento. Se você desativar o SSH e optar por reativá-lo posteriormente, poderá fazê-lo usando a mesma API.

Comando API

Para serviços de gerenciamento 2.18 ou posterior:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Para serviços de gerenciamento 2.17 ou anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Você pode encontrar o portador `${TOKEN}` usado pelo comando da API quando você [autorizar](#). O portador `${TOKEN}` está na resposta do curl.

Etapas da interface do usuário da API REST

1. Acesse a interface de usuário da API REST para o serviço de API do nó de gerenciamento inserindo o endereço IP do nó de gerenciamento seguido por `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Selecione **Autorizar** e complete o seguinte:
 - a. Insira o nome de usuário e a senha do cluster.
 - b. Insira o ID do cliente como `mnode-client`.
 - c. Selecione **Autorizar** para iniciar uma sessão.
 - d. Fechar a janela.
3. Na interface de usuário da API REST, selecione **PUT /settings/ssh**.
 - a. Selecione **Experimentar**.
 - b. Defina o parâmetro **enabled** para `false` para desativar o SSH ou `true` Para reativar a funcionalidade SSH que havia sido desativada anteriormente.
 - c. Selecione **Executar**.

Determine o status da capacidade SSH no nó de gerenciamento usando APIs.

Você pode determinar se a funcionalidade SSH está habilitada ou não no nó de gerenciamento usando uma API de serviço do nó de gerenciamento. O SSH está desativado por padrão nos nós de gerenciamento que executam os serviços de gerenciamento versão 2.18 ou posterior.

Comando API

Para serviços de gerenciamento 2.18 ou posterior:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Para serviços de gerenciamento 2.17 ou anteriores:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



Você pode encontrar o portador `${TOKEN}` usado pelo comando da API quando você ["autorizar"](#). O portador `${TOKEN}` está na resposta do curl...

Etapas da interface do usuário da API REST

1. Acesse a interface de usuário da API REST para o serviço de API do nó de gerenciamento inserindo o endereço IP do nó de gerenciamento seguido por `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Selecione **Autorizar** e complete o seguinte:
 - a. Insira o nome de usuário e a senha do cluster.
 - b. Insira o ID do cliente como `mnode-client`.
 - c. Selecione **Autorizar** para iniciar uma sessão.
 - d. Fechar a janela.
3. Na interface de usuário da API REST, selecione **GET /settings/ssh**.
 - a. Selecione **Experimental**.
 - b. Selecione **Executar**.

Encontre mais informações

- ["Plug-in NetApp Element para vCenter Server"](#)
- ["Documentação do SolidFire e do Element Software"](#)

Informações sobre direitos autorais

Copyright © 2025 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 SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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.