Gerenciar conexões de suporte

Element Software

NetApp
November 21, 2024

Índice

Gerenciar conexões de suporte

Acessando nós de storage usando SSH para solução de problemas básica

A partir do elemento 12,5, você pode usar a conta do sistema sfreeign somente nos nós de storage para solução de problemas básica. Você também pode ativar e abrir o acesso a túnel de suporte remoto para o suporte do NetApp para solução de problemas avançada.

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

> A menos que seja aconselhado pelo suporte NetApp, quaisquer alterações a este sistema não são suportadas, anulando o seu contrato de suporte e pode resultar em instabilidade ou inacessibilidade de dados.

Antes de começar

- **Permissões de gravação**: Verifique se você tem permissões de gravação no diretório de trabalho atual.
- **(Opcional) gere o seu próprio par de chaves**: Execute `ssh-keygen` a partir da distribuição Windows 10, MacOS ou Linux. Esta é uma ação única para criar um par de chaves de usuário e pode ser reutilizada para futuras sessões de solução de problemas. Você pode querer usar certificados associados a contas de funcionários, o que também funcionaria nesse modelo.
- **Ativar capacidade SSH no nó de gerenciamento**: Para habilitar a funcionalidade de acesso remoto no modo de gerenciamento, "este tópico"consulte . Para os serviços de gerenciamento 2,18 e posteriores, o recurso de acesso remoto é desativado no nó de gerenciamento por padrão.
- **Ativar capacidade SSH no cluster de armazenamento**: Para ativar a funcionalidade de acesso remoto nos nós do cluster de armazenamento, "este tópico"consulte .
- **Configuração do firewall**: Se o nó de gerenciamento estiver atrás de um servidor proxy, as seguintes portas TCP serão necessárias no arquivo sshd.config:

Porta de TCP	Descrição	Direção da ligação
443	Chamadas de API/HTTPS para reencaminhamento de portas via túnel de suporte aberto para a interface da Web	Nó de gerenciamento para nós de storage
22	Acesso SSH ao login	Nó de gerenciamento para nós de storage ou de nós de storage para nó de gerenciamento

Opções de resolução de problemas

- Solucionar problemas de um nó de cluster
- Solucione problemas de um nó de cluster com o suporte do NetApp
- Solucionar problemas de um nó que não faz parte do cluster

Solucionar problemas de um nó de cluster

Você pode executar a solução de problemas básica usando a conta do sistema spreadonly:

Passos

1. SSH para o nó de gerenciamento usando suas credenciais de login de conta que você selecionou ao instalar a VM do nó de gerenciamento.
2. No nó de gerenciamento, vá para `/sf/bin`.
3. Encontre o script apropriado para o seu sistema:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   > O SignSshKeys.ps1 depende do PowerShell 7 ou posterior e o SignSshKeys.py depende do Python 3.6.0 ou posterior e do "solicita o módulo".
   >
   > O `SignSshKeys` script grava `user` os arquivos , `user.pub` e `user-cert.pub` no diretório de trabalho atual, que são usados posteriormente 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 keychain SSH. O script permite o acesso SSH usando a conta do sistema sfrreadonly em todos os nós do cluster.

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

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

      > Você pode usar o parâmetro de formulário abreviado ou completo.

      - **--ip | -i [endereço ip]**: Endereço IP do nó de destino para a API ser executada.
      - **--user | -u [username]**: Usuário de cluster usado para executar a chamada API.
      - **(Opcional) --duração | -d [horas]**: A duração de uma chave assinada deve permanecer válida como um inteiro em horas. O padrão é 24 horas.
      - **(Opcional) --publickey | -k [caminho da chave pública]**: O caminho para uma chave pública, se o usuário optar por fornecer uma.

   b. Compare sua entrada com o seguinte comando de exemplo. Neste exemplo, `10.116.139.195` é o 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. Executar o comando.

5. SSH para os IPs do nó:

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

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

6. (Opcional) desative "funcionalidade de acesso remoto" novamente após a conclusão da solução de problemas.

> O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração ativada por SSH persiste no nó de gerenciamento por meio de atualizações e atualizações até que seja desabilitada manualmente.

Solucione problemas de um nó de cluster com o suporte do NetApp

O suporte da NetApp pode executar uma solução de problemas avançada com uma conta de sistema que permite que um técnico execute diagnósticos de elementos mais profundos.

Passos

1. SSH para o nó de gerenciamento usando suas credenciais de login de conta que você selecionou ao instalar a VM do nó de gerenciamento.
2. Execute o comando rst com o número da porta enviado pelo suporte NetApp para abrir o túnel de suporte:

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

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

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

   > O SignSshKeys.ps1 depende do PowerShell 7 ou posterior e o SignSshKeys.py depende do Python 3.6.0 ou posterior e do "solicita o módulo".
   >
   > O `SignSshKeys` script grava `user` os arquivos , `user.pub` e `user-cert.pub` no diretório de trabalho atual, que são usados posteriormente 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 keychain SSH com a `--sfadmin` bandeira. O script habilita o SSH em todos os nós.

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

Para SSH quanto `--sfadmin` a um nó em cluster, você deve gerar o keychain SSH usando um `--user supportAdmin` com acesso no cluster.

Para configurar `supportAdmin` o acesso para contas de administrador de cluster, você pode usar a IU ou APIs do Element:

- "Configure o acesso "supportAdmin" usando a IU do Element"
- Configure `supportAdmin` o acesso usando APIs e adicionando `"supportAdmin"` como o `"access"` tipo na solicitação de API:
  - "Configure o acesso "supportAdmin" para uma nova conta"
  - "Configure o acesso "supportAdmin" para uma conta existente"

    Para obter o `clusterAdminID`, você pode usar a "ListClusterAdmins" API.

Para adicionar `supportAdmin` acesso, você deve ter Privileges administrador de cluster ou administrador.

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

   Você pode usar o parâmetro de formulário abreviado ou completo.

   - **--ip | -i [endereço ip]**: Endereço IP do nó de destino para a API ser executada.
   - **--user | -u [username]**: Usuário de cluster usado para executar a chamada API.
   - **(Opcional) --duração | -d [horas]**: A duração de uma chave assinada deve permanecer válida como um 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 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 solução de problemas:

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

c. Executar o comando.

6. SSH para os IPs do nó:

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

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

```
rst --killall
```

8. (Opcional) desative "funcionalidade de acesso remoto" novamente após a conclusão da solução de problemas.

> O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração ativada por SSH persiste no nó de gerenciamento por meio de atualizações e atualizações até que seja desabilitada manualmente.

Solucionar problemas de um nó que não faz parte do cluster

Você pode executar a solução de problemas básica de um nó que ainda não foi adicionado a um cluster. Você pode usar a conta do sistema sfradonly para esse fim 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 essa tarefa.

1. A partir de uma máquina Windows, Linux ou Mac que tenha um cliente SSH instalado, execute o script apropriado para o seu sistema fornecido pelo suporte da NetApp.
2. SSH para o IP do nó:

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

3. (Opcional) desative "funcionalidade de acesso remoto" novamente após a conclusão da solução de problemas.

> O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração ativada por SSH persiste no nó de gerenciamento por meio de atualizações e atualizações até que seja desabilitada manualmente.

Encontre mais informações

- "Plug-in do NetApp Element para vCenter Server"
- "Página de recursos do NetApp HCI"

Inicie uma sessão remota de suporte do NetApp

Se você precisar de suporte técnico para o seu sistema de storage all-flash SolidFire, o suporte NetApp pode se conetar remotamente ao seu sistema. Para iniciar uma sessão e obter acesso remoto, o suporte da NetApp pode abrir uma conexão SSH (Secure Shell) reversa ao seu ambiente.

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

Antes de começar

- Para os serviços de gerenciamento 2,18 e posteriores, o recurso de acesso remoto é desativado no nó de gerenciamento por padrão. Para ativar a funcionalidade de acesso remoto, "Gerencie a funcionalidade SSH no nó de gerenciamento"consulte .
- Se o nó de gerenciamento estiver atrás de um servidor proxy, as seguintes portas TCP serão necessárias

no arquivo sshd.config:

Porta de TCP	Descrição	Direção da ligação
443	Chamadas de API/HTTPS para reencaminhamento de portas via túnel de suporte aberto para a interface da Web	Nó de gerenciamento para nós de storage
22	Acesso SSH ao login	Nó de gerenciamento para nós de storage ou de nós de storage para nó de gerenciamento

Passos

- Faça login no nó de gerenciamento e abra uma sessão de terminal.
- Em um prompt, digite o seguinte:

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

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

```
rst --killall
```

- (Opcional) Desativar "funcionalidade de acesso remoto" novamente.

> O SSH permanece habilitado no nó de gerenciamento se você não o desabilitar. A configuração ativada por SSH persiste no nó de gerenciamento por meio de atualizações e atualizações até que seja desabilitada manualmente.

Encontre mais informações

- "Plug-in do NetApp Element para vCenter Server"
- "Documentação do software SolidFire e Element"

Gerencie a funcionalidade SSH no nó de gerenciamento

Você pode desativar, reativar ou determinar o status da capacidade SSH no nó de gerenciamento (mNode) usando a API REST. O recurso SSH que fornece "Acesso à sessão do túnel de suporte remoto (RST) do suporte da NetApp" é desativado por padrão nos nós de gerenciamento que executam serviços de gerenciamento 2,18 ou posterior.

A partir dos Serviços de Gerenciamento 2.20.69, você pode ativar e desativar a capacidade SSH no nó de gerenciamento usando a IU do Controle de nuvem híbrida da NetApp.

O que você vai precisar

- **Permissões de controle de nuvem híbrida da NetApp**: Você tem permissões como administrador.
- **Permissões de administrador de cluster**: Você tem permissões como administrador no cluster de armazenamento.

- **Element software**: 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 de serviços de gestão**:
  - Para usar a IU do Controle de nuvem híbrida da NetApp, você atualizou o "pacote de serviços de gerenciamento" para a versão 2.20.69 ou posterior.
  - Para usar a IU da API REST, você atualizou o "pacote de serviços de gerenciamento" para a versão 2,17.

Opções

- Desative ou ative o recurso SSH no nó de gerenciamento usando a IU do Controle de nuvem híbrida do NetApp

Você pode executar qualquer uma das seguintes tarefas depois de "autenticar":

- Desative ou ative o recurso SSH no nó de gerenciamento usando APIs
- Determine o status do recurso SSH no nó de gerenciamento usando APIs

Desative ou ative o recurso SSH no nó de gerenciamento usando a IU do Controle de nuvem híbrida do NetApp

Você pode desativar ou reativar a capacidade SSH no nó de gerenciamento. O recurso SSH que fornece "Acesso à sessão do túnel de suporte remoto (RST) do suporte da NetApp" é desativado por padrão nos nós de gerenciamento que executam serviços de gerenciamento 2,18 ou posterior. A desativação do SSH não termina nem desliga sessões de cliente SSH existentes para o nó de gerenciamento. Se você desabilitar o SSH e optar por reativá-lo posteriormente, poderá fazê-lo usando a IU do Controle de nuvem híbrida da NetApp.

Para ativar ou desativar o acesso de suporte usando SSH para um cluster de armazenamento, você deve usar o "Página de configurações do cluster da IU do Element".

Passos

1. No Painel, selecione o menu de opções no canto superior direito e selecione **Configurar**.
2. Na tela **Support Access for Management Node**, alterne o switch para ativar o SSH do nó de gerenciamento.
3. Depois de concluir a solução de problemas, na tela **Support Access for Management Node**, alterne o switch para desativar o SSH do nó de gerenciamento.

Desative ou ative o recurso SSH no nó de gerenciamento usando APIs

Você pode desativar ou reativar a capacidade SSH no nó de gerenciamento. O recurso SSH que fornece "Acesso à sessão do túnel de suporte remoto (RST) do suporte da NetApp" é desativado por padrão nos nós de gerenciamento que executam serviços de gerenciamento 2,18 ou posterior. A desativação do SSH não termina nem desliga sessões de cliente SSH existentes para o nó de gerenciamento. Se você desabilitar 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 `${TOKEN}` portador usado pelo comando API quando "autorizar"você . O portador `${TOKEN}` está na resposta de ondulação.

ETAPAS DA IU DA API REST

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

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

2. Selecione **autorizar** e preencha o seguinte:
   a. Introduza o nome de utilizador e a palavra-passe do cluster.
   b. Introduza a ID do cliente como `mnode-client`.
   c. Selecione **autorizar** para iniciar uma sessão.
   d. Feche a janela.
3. Na IU da API REST, selecione **PUT /settings/ssh**.
   a. Selecione **Experimente**.
   b. Defina o parâmetro **Enabled** como `false` para desativar SSH ou `true` para reativar a capacidade SSH que foi anteriormente desativada.
   c. Selecione **Executar**.

Determine o status do recurso SSH no nó de gerenciamento usando APIs

Você pode determinar se a capacidade SSH está ou não ativada no nó de gerenciamento usando uma API de serviço de nó de gerenciamento. O SSH é desativado por padrão nos nós de gerenciamento que executam serviços de gerenciamento 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 `${TOKEN}` portador usado pelo comando API quando "autorizar"você . O portador `${TOKEN}` está na resposta de ondulação..

ETAPAS DA IU DA API REST

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

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

2. Selecione **autorizar** e preencha o seguinte:
   a. Introduza o nome de utilizador e a palavra-passe do cluster.
   b. Introduza a ID do cliente como `mnode-client`.
   c. Selecione **autorizar** para iniciar uma sessão.
   d. Feche a janela.
3. Na IU da API REST, selecione **GET /settings/ssh**.
   a. Selecione **Experimente**.
   b. Selecione **Executar**.

Encontre mais informações

- "Plug-in do NetApp Element para vCenter Server"
- "Documentação do software SolidFire e Element"

Informações sobre direitos autorais

Informações sobre marcas comerciais