Gerenciamento de clusters com a CLI

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciamento de clusters com a CLI

Visão geral da administração com a CLI

Você pode administrar sistemas ONTAP com a interface de linha de comando (CLI). Você pode usar as interfaces de gerenciamento do ONTAP, acessar o cluster, gerenciar nós e muito mais.

Você deve usar esses procedimentos nas seguintes circunstâncias:

- Você quer entender a gama de recursos de administrador do ONTAP.
- Você deseja usar a CLI, não o System Manager ou uma ferramenta de script automatizado.

Informações relacionadas

Para obter detalhes sobre a sintaxe e o uso da CLI, consulte "Referência do comando ONTAP"a documentação.

Administradores de clusters e SVM

Administradores de clusters e SVM

Os administradores de cluster administram todo o cluster e as máquinas virtuais de armazenamento (SVMs, anteriormente conhecidas como VServers) que ele contém. Os administradores do SVM administram apenas seus próprios SVMs de dados.

Os administradores de cluster podem administrar todo o cluster e seus recursos. Eles também podem configurar SVMs de dados e delegar a administração da SVM aos administradores do SVM. Os recursos específicos que os administradores de cluster têm dependem de suas funções de controle de acesso. Por padrão, um administrador de cluster com o nome de conta "'admin'" ou nome de função tem todos os recursos para gerenciar o cluster e SVMs.

Os administradores do SVM podem administrar apenas seus próprios recursos de rede e storage SVM, como volumes, protocolos, LIFs e serviços. As funcionalidades específicas que os administradores do SVM têm dependem das funções de controle de acesso atribuídas pelos administradores de cluster.

A interface de linha de comando (CLI) do ONTAP continua a usar o termo *SVM* na saída, e `vserver` como um nome de comando ou parâmetro não foi alterado.

Gerencie o acesso ao System Manager

Você pode ativar ou desativar o acesso de um navegador da Web ao System Manager. Você também pode visualizar o log do System Manager.

Você pode controlar o acesso de um navegador da Web ao System Manager usando `vserver services web modify -name sysmgr -vserver` *`cluster_name`* `-enabled` [`true`|`false`].

O log do System Manager é gravado `/mroot/etc/log/mlog/sysmgr.log` nos arquivos do nó que hospeda o LIF de gerenciamento de cluster no momento em que o System Manager é acessado. Você pode visualizar os arquivos de log usando um navegador. O log do Gerenciador de sistema também está incluído

nas mensagens do AutoSupport.

O que é o servidor de gerenciamento de cluster

O servidor de gerenciamento de cluster, também chamado de *admin*SVM, é uma implementação especializada de máquina virtual de storage (SVM) que apresenta o cluster como uma única entidade gerenciável. Além de servir como o domínio administrativo de mais alto nível, o servidor de gerenciamento de clusters possui recursos que não pertencem logicamente a um SVM de dados.

O servidor de gerenciamento de cluster está sempre disponível no cluster. Você pode acessar o servidor de gerenciamento de cluster por meio do console ou do LIF de gerenciamento de cluster.

Após a falha de sua porta de rede doméstica, o LIF de gerenciamento de cluster automaticamente faz failover para outro nó no cluster. Dependendo das caraterísticas de conetividade do protocolo de gerenciamento que você está usando, você pode ou não notar o failover. Se você estiver usando um protocolo sem conexão (por exemplo, SNMP) ou tiver uma conexão limitada (por exemplo, HTTP), é provável que você não perceba o failover. No entanto, se você estiver usando uma conexão de longo prazo (por exemplo, SSH), então você terá que se reconetar ao servidor de gerenciamento de cluster após o failover.

Quando você cria um cluster, todas as caraterísticas do LIF de gerenciamento de cluster são configuradas, incluindo seu endereço IP, máscara de rede, gateway e porta.

Diferentemente de um SVM ou nó de dados, um servidor de gerenciamento de cluster não tem volume raiz ou volumes de usuário de host (embora possa hospedar volumes do sistema). Além disso, um servidor de gerenciamento de cluster só pode ter LIFs do tipo de gerenciamento de cluster.

Se você executar o `vserver show` comando, o servidor de gerenciamento de cluster aparecerá na lista de saída para esse comando.

Tipos de SVMs

Um cluster consiste em quatro tipos de SVMs, que ajudam a gerenciar o cluster e seus recursos e acesso a dados aos clientes e aplicações.

Um cluster contém os seguintes tipos de SVMs:

- SVM admin

  O processo de configuração do cluster cria automaticamente o administrador SVM para o cluster. O SVM admin representa o cluster.

- SVM de nó

  Um nó SVM é criado quando o nó se junta ao cluster e o nó SVM representa os nós individuais do cluster.

- SVM do sistema (avançado)

  Um SVM do sistema é criado automaticamente para comunicações no nível do cluster em um espaço IPspace.

- Data SVM

Um data SVM representa os dados que atendem SVMs. Após a configuração do cluster, um administrador de cluster deve criar SVMs de dados e adicionar volumes a essas SVMs para facilitar o acesso aos dados a partir do cluster.

Um cluster precisa ter pelo menos um SVM de dados para servir dados a seus clientes.

Salvo especificação em contrário, o termo SVM se refere a um SVM de dados (fornecimento de dados).

Na CLI, os SVMs são exibidos como VServers.

Acessar o cluster usando a CLI (somente administradores de cluster)

Acesse o cluster usando a porta serial

Você pode acessar o cluster diretamente de um console conetado à porta serial de um nó.

Passos

1. No console, pressione Enter.

   O sistema responde com o aviso de início de sessão.

2. No prompt de login, execute um dos seguintes procedimentos:

Para acessar o cluster com…	Digite o seguinte nome de conta…
A conta de cluster predefinida	**`admin`**
Uma conta de usuário administrativa alternativa	*`username`*

   O sistema responde com o aviso de palavra-passe.

3. Introduza a palavra-passe da conta de utilizador administrativo ou administrativo e, em seguida, prima Enter.

Acesse o cluster usando SSH

Você pode emitir solicitações SSH para um cluster ONTAP para executar tarefas administrativas. O SSH está ativado por predefinição.

Antes de começar

- Você deve ter uma conta de usuário configurada para usar `ssh` como método de acesso.

  O `-application` parâmetro dos `security login` comandos especifica o método de acesso para uma conta de usuário. Saiba mais sobre `security login` o "Referência do comando ONTAP"na .

- Se você usar uma conta de usuário de domínio do ative Directory (AD) para acessar o cluster, um túnel de

autenticação para o cluster deve ter sido configurado por meio de uma VM de armazenamento habilitada para CIFS e sua conta de usuário de domínio do AD também deve ter sido adicionada ao cluster `ssh` como método de acesso e `domain` como método de autenticação.

Sobre esta tarefa

- Você deve usar um cliente OpenSSH 5,7 ou posterior.
- Apenas o protocolo SSH v2 é suportado; o SSH v1 não é suportado.
- O ONTAP suporta um máximo de 64 sessões de SSH simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- O ONTAP suporta apenas os algoritmos de criptografia AES e 3DES (também conhecidos como *cifras*) para SSH.

  O AES é suportado com 128, 192 e 256 bits no comprimento da chave. 3DES tem 56 bits no comprimento da chave como no DES original, mas é repetido três vezes.

- Quando o modo FIPS está ativado, os clientes SSH devem negociar com algoritmos de chave pública Elliptic Curve Digital Signature Algorithm (ECDSA) para que a conexão seja bem-sucedida.
- Se você quiser acessar a CLI do ONTAP a partir de um host do Windows, você pode usar um utilitário de terceiros, como o PuTTY.
- Se você usar um nome de usuário do Windows AD para fazer login no ONTAP, use as mesmas letras maiúsculas ou minúsculas que foram usadas quando o nome de usuário e o nome de domínio do AD foram criados no ONTAP.

  Os nomes de usuários DE ANÚNCIOS e nomes de domínio não diferenciam maiúsculas de minúsculas. No entanto, os nomes de usuário do ONTAP são sensíveis a maiúsculas e minúsculas. A incompatibilidade de casos entre o nome de utilizador criado no ONTAP e o nome de utilizador criado no AD resulta numa falha de início de sessão.

Opções de autenticação SSH

- A partir do ONTAP 9.3, você pode "Ative a autenticação multifator SSH" para contas de administrador locais.

  Quando a autenticação multifator SSH está ativada, os usuários são autenticados usando uma chave pública e uma senha.

- A partir do ONTAP 9.4, você pode "Ative a autenticação multifator SSH" para usuários remotos LDAP e NIS.
- A partir do ONTAP 9.13,1, você pode opcionalmente adicionar validação de certificado ao processo de autenticação SSH para melhorar a segurança de login. Para fazer isso, "Associar um certificado X,509 à chave pública"uma conta usa. Se você fizer login usando SSH com uma chave pública SSH e um certificado X,509, o ONTAP verificará a validade do certificado X,509 antes de autenticar com a chave pública SSH. O login SSH é recusado se esse certificado estiver expirado ou revogado e a chave pública SSH for desativada automaticamente.
- A partir do ONTAP 9.14,1, os administradores do ONTAP podem "Adicione a autenticação de dois fatores do Cisco Duo ao processo de autenticação SSH"melhorar a segurança de login. Após o primeiro login

depois de ativar a autenticação Cisco Duo, os usuários precisarão Registrar um dispositivo para servir como autenticador para sessões SSH.

- A partir do ONTAP 9.15,1, os administradores podem "Configurar autorização dinâmica"fornecer autenticação adaptativa adicional aos usuários SSH com base na pontuação de confiança do usuário.

Passos

1. A partir de um host com acesso à rede do cluster ONTAP, digite o `ssh` comando em um dos seguintes formatos:
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

Se você estiver usando uma conta de usuário de domínio do AD, você deve especificar *username* no formato *domainname**AD_accountname* (com backslashes duplos após o nome de domínio) ou "*domainname**AD_accountname*" (entre aspas duplas e com uma única barra invertida após o nome de domínio).

hostname_or_IP É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

command Não é necessário para sessões interativas SSH.

Exemplos de solicitações SSH

Os exemplos a seguir mostram como a conta de usuário chamada "joe" pode emitir uma solicitação SSH para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Os exemplos a seguir mostram como a conta de usuário chamada "john" do domínio chamado "domain1" pode emitir uma solicitação SSH para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

O exemplo a seguir mostra como a conta de usuário chamada "joe" pode emitir uma solicitação SSH MFA para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Informações relacionadas

"Autenticação de administrador e RBAC"

Segurança de login SSH

A partir do ONTAP 9.5, você pode exibir informações sobre logins anteriores, tentativas malsucedidas de fazer login e alterações no Privileges desde o último login bem-sucedido.

As informações relacionadas à segurança são exibidas quando você faz login com sucesso como um usuário de administrador SSH. Você é alertado sobre as seguintes condições:

- A última vez que o nome da sua conta foi iniciado.

- O número de tentativas de login mal sucedidas desde o último login bem-sucedido.
- Se a função mudou desde o último login (por exemplo, se a função da conta de administrador mudou de "admin" para "backup".)
- Se os recursos de adição, modificação ou exclusão da função foram modificados desde o último login.

Se alguma das informações apresentadas for suspeita, deverá contactar imediatamente o seu departamento de segurança.

Para obter essas informações quando você fizer login, os seguintes pré-requisitos devem ser atendidos:

- Sua conta de usuário SSH deve ser provisionada no ONTAP.
- Seu login de segurança SSH deve ser criado.
- Sua tentativa de login deve ser bem-sucedida.

Restrições e outras considerações para segurança de login SSH

As seguintes restrições e considerações se aplicam às informações de segurança de login SSH:

- As informações estão disponíveis apenas para logins baseados em SSH.
- Para contas de administrador baseadas em grupo, como contas LDAP/NIS e AD, os usuários podem exibir as informações de login SSH se o grupo do qual são membros for provisionado como uma conta de administrador no ONTAP.

  No entanto, alertas sobre alterações na função da conta de usuário não podem ser exibidos para esses usuários. Além disso, os usuários pertencentes a um grupo AD que tenha sido provisionado como uma conta de administrador no ONTAP não podem exibir a contagem de tentativas de login mal sucedidas que ocorreram desde a última vez em que fizeram login.

- As informações mantidas para um usuário são excluídas quando a conta de usuário é excluída do ONTAP.
- As informações não são exibidas para conexões a aplicativos que não sejam SSH.

Exemplos de informações de segurança de login SSH

Os exemplos a seguir demonstram o tipo de informação exibida após o login.

- Esta mensagem é apresentada após cada início de sessão bem-sucedido:

```
Last Login : 7/19/2018 06:11:32
```

- Estas mensagens são apresentadas se não tiverem sido efetuadas tentativas de início de sessão sem êxito desde o último início de sessão bem-sucedido:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Estas mensagens são apresentadas se não tiverem sido efetuadas tentativas de início de sessão sem êxito e o seu Privileges tiver sido modificado desde o último início de sessão bem-sucedido:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Ative o acesso Telnet ou RSH ao cluster

Como prática recomendada de segurança, Telnet e RSH são desativados por padrão. Para permitir que o cluster aceite solicitações Telnet ou RSH, você deve ativar o serviço na política de serviço de gerenciamento padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões simultâneas de Telnet ou RSH por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança RSH ou Telnet está ativado:

   ```
   security protocol show
   ```

   a. Se o protocolo de segurança RSH ou Telnet estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança RSH ou Telnet não estiver ativado, use o seguinte comando para ativá-lo:

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

2. Confirme se o `management-rsh-server` serviço ou `management-telnet-server` existe nas LIFs de gerenciamento:

   ```
   network interface show -services management-rsh-server
   ```

   ou

   ```
   network interface show -services management-telnet-server
   ```

   a. Se o `management-rsh-server` serviço ou `management-telnet-server` existir, avance para o passo seguinte.

   b. Se o `management-rsh-server` serviço ou `management-telnet-server` não existir, use o seguinte comando para adicioná-lo:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   ```
   network interface service-policy add-service -vserver cluster1 -policy
   default-management -service management-telnet-server
   ```

ONTAP 9 1.9 ou anterior

Sobre esta tarefa

O ONTAP impede que você altere políticas de firewall predefinidas, mas você pode criar uma nova política clonando a política de firewall de gerenciamento predefinida `mgmt` e habilitando o Telnet ou o RSH sob a nova política.

Passos

1. Entre no modo de privilégio avançado:

   ```
   set advanced
   ```

2. Ativar um protocolo de segurança (RSH ou Telnet):

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. Crie uma nova política de firewall de gerenciamento com base na `mgmt` política de firewall de gerenciamento:

```
system services firewall policy clone -policy mgmt -destination-policy
policy-name
```

4. Ativar Telnet ou RSH na nova política de firewall de gerenciamento:

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   Para permitir todos os endereços IP, você deve especificar `-ip-list 0.0.0.0/0`

5. Associe a nova política ao LIF de gerenciamento de clusters:

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

Acesse o cluster usando Telnet

Você pode emitir solicitações Telnet para o cluster para executar tarefas administrativas. O Telnet está desativado por padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Antes de começar

As condições a seguir devem ser atendidas antes que você possa usar o Telnet para acessar o cluster:

- Você deve ter uma conta de usuário local de cluster configurada para usar Telnet como método de acesso.

  O `-application` parâmetro dos `security login` comandos especifica o método de acesso para uma conta de usuário. Para obter mais informações, consulte as `security login` páginas de manual.

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões Telnet simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de ligações em curso for superior a 10 por segundo, o serviço é temporariamente desativado durante 60 segundos.

- Se você quiser acessar a CLI do ONTAP a partir de um host do Windows, você pode usar um utilitário de terceiros, como o PuTTY.
- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança Telnet está ativado:

   `security protocol show`

   a. Se o protocolo de segurança Telnet estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança Telnet não estiver ativado, use o seguinte comando para ativá-lo:

      `security protocol modify -application telnet -enabled true`

2. Confirme se o `management-telnet-server` serviço existe nas LIFs de gerenciamento:

   `network interface show -services management-telnet-server`

   a. Se o `management-telnet-server` serviço existir, avance para o passo seguinte.

   b. Se o `management-telnet-server` serviço não existir, use o seguinte comando para adicioná-lo:

      `network interface service-policy add-service -vserver cluster1 -policy default-management -service management-telnet-server`

ONTAP 9 1.9 ou anterior

Antes de começar

As condições a seguir devem ser atendidas antes que você possa usar o Telnet para acessar o cluster:

- O Telnet já deve estar habilitado na política de firewall de gerenciamento usada pelas LIFs de gerenciamento de cluster ou nó para que as solicitações Telnet possam passar pelo firewall.

  Por padrão, o Telnet está desativado. O `system services firewall policy show` comando com o `-service telnet` parâmetro exibe se o Telnet foi habilitado em uma política de firewall. Para obter mais informações, consulte as `system services firewall policy` páginas de manual.

- Se você usar conexões IPv6, o IPv6 já deve estar configurado e habilitado no cluster e as políticas de firewall já devem ser configuradas com endereços IPv6.

  O `network options ipv6 show` comando exibe se o IPv6 está ativado. O `system services firewall policy show` comando exibe políticas de firewall.

Passos

1. Em um host de administração, digite o seguinte comando:

   `telnet hostname_or_IP`

   `hostname_or_IP` É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

Exemplo de uma solicitação Telnet

O exemplo a seguir mostra como o usuário chamado "joe", que foi configurado com acesso Telnet, pode emitir uma solicitação Telnet para acessar um cluster cujo LIF de gerenciamento de cluster é 10.72.137.28:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Aceda ao cluster utilizando o RSH

Você pode emitir solicitações RSH ao cluster para executar tarefas administrativas. O RSH não é um protocolo seguro e está desativado por padrão.

Telnet e RSH não são protocolos seguros; você deve considerar o uso de SSH para acessar o cluster. O SSH fornece um shell remoto seguro e sessão de rede interativa. Para obter mais informações, "Acesse o cluster usando SSH"consulte .

Antes de começar

As seguintes condições devem ser cumpridas antes de poder utilizar o RSH para aceder ao cluster:

- Tem de ter uma conta de utilizador local de cluster configurada para utilizar o RSH como método de acesso.

  O `-application` parâmetro dos `security login` comandos especifica o método de acesso para uma conta de usuário. Para obter mais informações, consulte as `security login` páginas de manual.

Sobre esta tarefa

- O ONTAP suporta um máximo de 50 sessões de RSH simultâneas por nó.

  Se o LIF de gerenciamento de cluster reside no nó, ele compartilha esse limite com o LIF de gerenciamento de nós.

  Se a taxa de conexões de entrada for superior a 10 por segundo, o serviço será temporariamente desativado por 60 segundos.

- Os comandos RSH requerem Privileges avançado.

ONTAP 9.10,1 ou posterior

Passos

1. Confirme se o protocolo de segurança RSH está ativado:

   `security protocol show`

   a. Se o protocolo de segurança RSH estiver ativado, avance para o passo seguinte.

   b. Se o protocolo de segurança RSH não estiver ativado, utilize o seguinte comando para o ativar:

      `security protocol modify -application rsh -enabled true`

2. Confirme se o `management-rsh-server` serviço existe nas LIFs de gerenciamento:

   `network interface show -services management-rsh-server`

   a. Se o `management-rsh-server` serviço existir, avance para o passo seguinte.

   b. Se o `management-rsh-server` serviço não existir, use o seguinte comando para adicioná-lo:

      `network interface service-policy add-service -vserver cluster1 -policy default-management -service management-rsh-server`

ONTAP 9 1.9 ou anterior

Antes de começar

As seguintes condições devem ser cumpridas antes de poder utilizar o RSH para aceder ao cluster:

- O RSH já deve estar habilitado na política de firewall de gerenciamento que é usada pelos LIFs de gerenciamento de cluster ou nó para que as solicitações RSH possam passar pelo firewall.

  Por predefinição, o RSH está desativado. O comando show de política de firewall de serviços do sistema com o `-service rsh` parâmetro exibe se o RSH foi ativado em uma política de firewall. Para obter mais informações, consulte as `system services firewall policy` páginas de manual.

- Se você usar conexões IPv6, o IPv6 já deve estar configurado e habilitado no cluster e as políticas de firewall já devem ser configuradas com endereços IPv6.

  O `network options ipv6 show` comando exibe se o IPv6 está ativado. O `system services firewall policy show` comando exibe políticas de firewall.

Passos

1. Em um host de administração, digite o seguinte comando:

   `rsh hostname_or_IP -l username:passwordcommand`

   `hostname_or_IP` É o nome do host ou o endereço IP do LIF de gerenciamento de cluster ou um LIF de gerenciamento de nós. Recomenda-se a utilização do LIF de gestão de clusters. Você pode usar um endereço IPv4 ou IPv6.

   `command` É o comando que você deseja executar sobre RSH.

Exemplo de uma solicitação RSH

O exemplo a seguir mostra como o usuário chamado "joe", que foi configurado com RSH Access, pode emitir uma solicitação RSH para executar o `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Use a interface da linha de comando ONTAP

Usando a interface de linha de comando ONTAP

A interface de linha de comando (CLI) do ONTAP fornece uma visualização baseada em comando da interface de gerenciamento. Você insere comandos no prompt do sistema de armazenamento e os resultados do comando são exibidos no texto.

O prompt de comando CLI é representado como `cluster_name::>`.

Se você definir o nível de privilégio (ou seja, o `-privilege` parâmetro `set` do comando) como `advanced`, o prompt incluirá um asterisco (*), por exemplo:

```
cluster_name::*>
```

Sobre os diferentes shells para a visão geral dos comandos CLI (somente administradores de cluster)

O cluster tem três shells diferentes para comandos CLI, o *clustershell*, o *nodeshell* e o *systemshell*. Os shells são para finalidades diferentes, e cada um deles tem um conjunto de comandos diferente.

- O clustershell é o shell nativo que é iniciado automaticamente quando você faz login no cluster.

  Ele fornece todos os comandos que você precisa para configurar e gerenciar o cluster. A ajuda CLI do clustershell (acionada pelo `?` prompt do clustershell) exibe comandos disponíveis do clustershell. O `man` *`command_name`* comando no clustershell exibe a página de manual para o comando clustershell especificado.

- O nodeshell é um shell especial para comandos que entram em efeito apenas no nível do nó.

  O nodeshell é acessível através do `system node run` comando.

  A ajuda da CLI nodeshell (acionada por `?` ou `help` no prompt nodeshell) exibe os comandos nodeshell

disponíveis. O `man command_name` comando no nodeshell exibe a página man para o comando nodeshell especificado.

Muitos comandos e opções de nodeshell comumente usados são tunneled ou aliased no clustershell e podem ser executados também a partir do clustershell.

- O systemshell é um shell de baixo nível que é usado apenas para fins de diagnóstico e solução de problemas.

  A estrutura do sistema e a conta "diag" associada destinam-se a fins de diagnóstico de baixo nível. Seu acesso requer o nível de privilégio de diagnóstico e é reservado apenas para o suporte técnico para executar tarefas de solução de problemas.

Acesso de comandos e opções nodeshell no clustershell

Os comandos e opções Nodeshell são acessíveis através do nodeshell:

`system node run –node nodename`

Muitos comandos e opções de nodeshell comumente usados são tunneled ou aliased no clustershell e podem ser executados também a partir do clustershell.

As opções Nodeshell que são suportadas no clustershell podem ser acessadas usando o `vserver options clustershell` comando. Para ver essas opções, você pode fazer um dos seguintes procedimentos:

- Consulte a CLI do clustershell com `vserver options -vserver nodename_or_clustername -option-name ?`
- Acesse a `vserver options` página man na CLI do clustershell com `man vserver options`

Se você inserir um comando nodeshell ou legacy ou opção no clustershell, e o comando ou opção tiver um comando conclustershell equivalente, o ONTAP informa você sobre o comando conclustershell a ser usado.

Se você inserir um comando nodeshell ou legacy ou uma opção que não é suportada no clustershell, o ONTAP informa o status "'não suportado'" para o comando ou opção.

Exibir comandos nodeshell disponíveis

Você pode obter uma lista de comandos nodeshell disponíveis usando a ajuda CLI do nodeshell.

Passos

1. Para acessar o nodeshell, digite o seguinte comando no prompt do sistema do clustershell:

   `system node run -node {nodename|local}`

   `local` é o nó usado para acessar o cluster.

   > O `system node run` comando tem um comando alias, `run`.

2. Digite o seguinte comando no nodeshell para ver a lista de comandos nodeshell disponíveis:

   `[commandname] help`

`_commandname_` é o nome do comando cuja disponibilidade você deseja exibir. Se você não incluir `_commandname_`, a CLI exibirá todos os comandos nodeshell disponíveis.

Você insere `exit` ou digita Ctrl-d para retornar à CLI do clustershell.

Exemplo de exibição de comandos nodeshell disponíveis

O exemplo a seguir acessa o nodeshell de um nó chamado node2 e exibe informações para o comando nodeshell `environment` :

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Métodos de navegação de diretórios de comando CLI

Os comandos na CLI são organizados em uma hierarquia por diretórios de comando. Você pode executar comandos na hierarquia inserindo o caminho completo do comando ou navegando pela estrutura do diretório.

Ao usar a CLI, você pode acessar um diretório de comandos digitando o nome do diretório no prompt e pressionando Enter. O nome do diretório é então incluído no texto do prompt para indicar que você está interagindo com o diretório de comando apropriado. Para ir mais fundo para a hierarquia de comandos, digite o nome de um subdiretório de comandos seguido de pressionar Enter. O nome do subdiretório é então incluído no texto do prompt e o contexto muda para esse subdiretório.

Você pode navegar através de vários diretórios de comando inserindo o comando inteiro. Por exemplo, você pode exibir informações sobre unidades de disco digitando o `storage disk show` comando no prompt. Você também pode executar o comando navegando por um diretório de comando de cada vez, como mostrado no exemplo a seguir:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Você pode abreviar comandos inserindo apenas o número mínimo de letras em um comando que torna o comando exclusivo para o diretório atual. Por exemplo, para abreviar o comando no exemplo anterior, você

pode digitar `st d sh`. Você também pode usar a tecla Tab para expandir comandos abreviados e exibir os parâmetros de um comando, incluindo valores de parâmetro padrão.

Você pode usar o `top` comando para ir para o nível superior da hierarquia de comandos e o `up` comando ou `..` comando para subir um nível na hierarquia de comandos.

Comandos e opções de comando precedidos por um asterisco (*) na CLI só podem ser executados no nível de privilégio avançado ou superior.

Regras para especificar valores na CLI

A maioria dos comandos inclui um ou mais parâmetros necessários ou opcionais. Muitos parâmetros exigem que você especifique um valor para eles. Existem algumas regras para especificar valores na CLI.

- Um valor pode ser um número, um especificador booleano, uma seleção de uma lista enumerada de valores predefinidos ou uma cadeia de texto.

  Alguns parâmetros podem aceitar uma lista separada por vírgulas de dois ou mais valores. Listas de valores separados por vírgulas não precisam estar entre aspas (" "). Sempre que você especificar texto, um espaço ou um caractere de consulta (quando não se entende como uma consulta ou texto começando com um símbolo menor ou maior), você deve incluir a entidade entre aspas.

- A CLI interpreta um ponto de interrogação ("?"") como o comando para exibir informações de ajuda para um determinado comando.
- Algum texto inserido na CLI, como nomes de comandos, parâmetros e determinados valores, não diferencia maiúsculas de minúsculas.

  Por exemplo, quando você insere valores de parâmetro para os `vserver cifs` comandos, a capitalização é ignorada. No entanto, a maioria dos valores de parâmetros, como os nomes de nós, máquinas virtuais de storage (SVMs), agregados, volumes e interfaces lógicas, são sensíveis a maiúsculas e minúsculas.

- Se você quiser limpar o valor de um parâmetro que recebe uma string ou uma lista, especifique um conjunto vazio de aspas ("") ou um traço ("-").
- O sinal de hash ("""), também conhecido como sinal de libra, indica um comentário para uma entrada de linha de comando; se usado, ele deve aparecer após o último parâmetro em uma linha de comando.

  A CLI ignora o texto entre o número "" e o fim da linha.

No exemplo a seguir, um SVM é criado com um comentário de texto. O SVM é então modificado para excluir o comentário:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

No exemplo a seguir, um comentário de linha de comando que usa o sinal de "" indica o que o comando faz.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Métodos de visualização do histórico de comandos e reemissão de comandos

Cada sessão CLI mantém um histórico de todos os comandos emitidos nela. Você pode ver o histórico de comandos da sessão em que está atualmente. Você também pode reemitir comandos.

Para visualizar o histórico de comandos, pode utilizar o `history` comando.

Para reemitir um comando, você pode usar o `redo` comando com um dos seguintes argumentos:

- Uma cadeia de carateres que corresponde a parte de um comando anterior

  Por exemplo, se o único `volume` comando executado for `volume show`, você poderá usar o `redo volume` comando para reexecutar o comando.

- O ID numérico de um comando anterior, conforme listado pelo `history` comando

  Por exemplo, você pode usar o `redo 4` comando para reemitir o quarto comando na lista de histórico.

- Um desvio negativo a partir do final da lista de histórico

  Por exemplo, você pode usar o `redo -2` comando para reemitir o comando que você executou dois comandos atrás.

Por exemplo, para refazer o comando que está em terceiro lugar do final do histórico de comandos, digite o seguinte comando:

```
cluster1::> redo -3
```

Atalhos de teclado para editar comandos CLI

O comando no prompt de comando atual é o comando ativo. O uso de atalhos de teclado permite que você edite o comando ativo rapidamente. Esses atalhos de teclado são semelhantes aos do shell UNIX tcsh e do editor Emacs.

A tabela a seguir lista os atalhos de teclado para editar comandos CLI. ""Ctrl-"" indica que você pressiona e mantém pressionada a tecla Ctrl enquanto digita o caractere especificado após ele. "'Esc-" indica que você pressiona e solta a tecla ESC e, em seguida, digita o caractere especificado após ela.

Se você quiser…	Use o seguinte atalho de teclado…
Mova o cursor para trás por um caractere	Ctrl-B
Seta para trás	Mova o cursor para a frente por um caractere
Ctrl-F	Seta para a frente
Mova o cursor para trás por uma palavra	ESC-B
Mova o cursor para a frente por uma palavra	ESC-F
Mova o cursor para o início da linha	Ctrl-A
Mova o cursor para o fim da linha	Ctrl-e
Remova o conteúdo da linha de comando do início da linha para o cursor e salve-o no buffer de corte. O buffer de corte age como memória temporária, semelhante ao que é chamado de *clipboard* em alguns programas.	Ctrl-U
Remova o conteúdo da linha de comando do cursor até o final da linha e salve-o no buffer de corte	Ctrl-K
Remova o conteúdo da linha de comando do cursor até o final da palavra a seguir e salve-o no buffer de corte	ESC-D
Remova a palavra antes do cursor e salve-a no buffer de corte	Ctrl-W
Yank o conteúdo do buffer de corte, e empurre-o para a linha de comando no cursor	Ctrl-Y
Exclua o caractere antes do cursor	Ctrl-H
Backspace	Exclua o caractere onde o cursor está
Ctrl-D	Limpe a linha
Ctrl-C	Limpe o ecrã

Se você quiser…	Use o seguinte atalho de teclado…
Ctrl-L	Substitua o conteúdo atual da linha de comando pela entrada anterior na lista de histórico. Com cada repetição do atalho de teclado, o cursor do histórico move-se para a entrada anterior.
Ctrl-P	ESC-P
Seta para cima	Substitua o conteúdo atual da linha de comando pela próxima entrada na lista de histórico. Com cada repetição do atalho de teclado, o cursor do histórico move-se para a próxima entrada.
Ctrl-N	ESC-N
Seta para baixo	Expanda um comando parcialmente inserido ou liste entrada válida da posição de edição atual
Separador	Ctrl-I
Exibir ajuda sensível ao contexto	?
Escapar do mapeamento especial para o ponto de interrogação (" ?'?`") character. For instance, to enter a question mark into a command's argument, press Esc and then the "`" caractere.	ESC-?
Iniciar saída TTY	Ctrl-Q
Parar a saída TTY	Ctrl-S

Utilização de níveis de privilégios administrativos

Os comandos e parâmetros do ONTAP são definidos em três níveis de privilégio: *Admin*, *Advanced* e *diagnostic*. Os níveis de privilégio refletem os níveis de habilidade necessários na execução das tarefas.

- **admin**

  A maioria dos comandos e parâmetros estão disponíveis neste nível. Eles são usados para tarefas comuns ou rotineiras.

- **avançado**

  Comandos e parâmetros neste nível são usados com pouca frequência, exigem conhecimentos avançados e podem causar problemas se usados de forma inadequada.

Você usa comandos ou parâmetros avançados apenas com o Conselho do pessoal de suporte.

- **diagnóstico**

  Comandos e parâmetros de diagnóstico são potencialmente disruptivos. Eles são usados apenas pelo pessoal de suporte para diagnosticar e corrigir problemas.

Defina o nível de privilégio na CLI

Você pode definir o nível de privilégio na CLI usando o `set` comando. As alterações nas configurações de nível de privilégio aplicam-se apenas à sessão em que você está. Elas não são persistentes em todas as sessões.

Passos

1. Para definir o nível de privilégio na CLI, use o `set` comando com o `-privilege` parâmetro.

Exemplo de definição do nível de privilégio

O exemplo a seguir define o nível de privilégio como avançado e depois como admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Defina as preferências de exibição na CLI

Você pode definir preferências de exibição para uma sessão CLI usando o `set` comando e `rows` o comando. As preferências definidas aplicam-se apenas à sessão em que se encontra. Elas não são persistentes em todas as sessões.

Sobre esta tarefa

Você pode definir as seguintes preferências de exibição da CLI:

- O nível de privilégio da sessão de comando
- Se as confirmações são emitidas para comandos potencialmente disruptivos
- Se `show` os comandos exibem todos os campos
- O caractere ou carateres a serem usados como separador de campo
- A unidade padrão ao relatar tamanhos de dados
- O número de linhas que a tela exibe na sessão atual da CLI antes que a interface interrompa a saída

  Se o número preferido de linhas não for especificado, ele será ajustado automaticamente com base na altura real do terminal. Se a altura real for indefinida, o número padrão de linhas é 24.

- O nó ou a máquina virtual de storage padrão (SVM)
- Se um comando contínuo deve parar se encontrar um erro

Passos

1. Para definir preferências de exibição da CLI, use o `set` comando.

   Para definir o número de linhas que a tela exibe na sessão atual da CLI, você também pode usar o `rows` comando.

   Para obter mais informações, consulte as páginas man para o `set` comando e `rows` comando.

Exemplo de configuração de preferências de exibição na CLI

O exemplo a seguir define uma vírgula para ser o separador de campos, define `GB` como a unidade padrão de tamanho de dados e define o número de linhas como 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Métodos de uso de operadores de consulta

A interface de gerenciamento suporta consultas e padrões de estilo UNIX e wildcards para permitir que você combine vários valores em argumentos de comando-parâmetro.

A tabela a seguir descreve os operadores de consulta suportados:

Operador	Descrição
*	Curinga que corresponde a todas as entradas. Por exemplo, o comando `volume show -volume *tmp*` exibe uma lista de todos os volumes cujos nomes incluem a cadeia de carateres `tmp`.
!	NÃO operador. Indica um valor que não deve ser correspondido; por exemplo, **`!vs0`** indica não corresponder ao valor `vs0`.
OU operador. Separa dois valores que devem ser comparados; por exemplo, `*vs0	vs2*` corresponde a vs0 ou VS2. Você pode especificar várias INSTRUÇÕES OU; por exemplo, `a

Operador	Descrição
b*	*c*` corresponde à entrada `a`, qualquer entrada que comece com `b`, e qualquer entrada que inclua `c`.
..	Operador de gama. Por exemplo, **`5..10`** corresponde a qualquer valor de `5` a `10`, inclusive.
*	Menos do que o operador. Por exemplo, **`<20`** corresponde a qualquer valor inferior `20` a .
>	Operador superior a. Por exemplo, **`>5`** corresponde a qualquer valor maior que `5`.
O que é que é	Menos ou igual ao operador. Por exemplo, ⇐**`5`** corresponde a qualquer valor menor ou igual a `5`.
>	Maior ou igual ao operador. Por exemplo, **`>=5`** corresponde a qualquer valor maior ou igual a `5`.
{`query`Selecione	Consulta alargada. Uma consulta estendida deve ser especificada como o primeiro argumento após o nome do comando, antes de quaisquer outros parâmetros. Por exemplo, o comando `volume modify {-volume *tmp*} -state offline` define offline todos os volumes cujos nomes incluem a cadeia de carateres `tmp`.

Se você quiser analisar carateres de consulta como literais, você deve incluir os carateres em aspas duplas (por exemplo, `"<10"` `"0..100"` , , `"*abc*"` ou `"a|b"`) para que os resultados corretos sejam retornados.

Você deve incluir nomes de arquivos brutos em aspas duplas para evitar a interpretação de carateres especiais. Isso também se aplica a carateres especiais usados pelo clustershell.

Você pode usar vários operadores de consulta em uma linha de comando. Por exemplo, o comando `volume show -size >1GB -percent-used <50 -vserver !vs1` exibe todos os volumes com mais de 1 GB de tamanho, menos de 50% utilizados e não na máquina virtual de armazenamento (SVM) chamada "'VS1".

Informações relacionadas

"Atalhos de teclado para editar comandos CLI"

Métodos de uso de consultas estendidas

Você pode usar consultas estendidas para corresponder e executar operações em

objetos que tenham valores especificados.

Você especifica consultas estendidas, anexando-as entre colchetes encaracolados ("colchetes"). Uma consulta estendida deve ser especificada como o primeiro argumento após o nome do comando, antes de quaisquer outros parâmetros. Por exemplo, para definir offline todos os volumes cujos nomes incluem a cadeia de carateres `tmp`, execute o comando no exemplo a seguir:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Consultas estendidas geralmente são úteis apenas com `modify` comandos e `delete`. Eles não têm nenhum significado em `create` ou `show` comandos.

A combinação de consultas e operações de modificação é uma ferramenta útil. No entanto, ele pode potencialmente causar confusão e erros se implementado incorretamente. Por exemplo, usar o comando (privilégio avançado) `system node image modify` para definir a imagem de software padrão de um nó automaticamente define a outra imagem de software para não ser a padrão. O comando no exemplo a seguir é efetivamente uma operação nula:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Este comando define a imagem padrão atual como a imagem não padrão e, em seguida, define a nova imagem padrão (a imagem não padrão anterior) para a imagem não padrão, resultando na retenção das configurações padrão originais. Para executar a operação corretamente, você pode usar o comando como indicado no exemplo a seguir:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Métodos de personalização da saída do comando show usando campos

Quando você usa o `-instance` parâmetro com um `show` comando para exibir detalhes, a saída pode ser longa e incluir mais informações do que você precisa. O `-fields` parâmetro de um `show` comando permite exibir apenas as informações especificadas.

Por exemplo, é provável que a execução `volume show -instance` resulte em várias telas de informações. Você pode usar `volume show -fields` *`fieldname[,fieldname…]`* para personalizar a saída de modo que ela inclua apenas o campo ou campos especificados (além dos campos padrão que são sempre exibidos). Você pode usar `-fields ?` para exibir campos válidos para um `show` comando.

O exemplo a seguir mostra a diferença de saída entre o `-instance` parâmetro e o `-fields` parâmetro:

```
cluster1::> volume show -instance

                                  Vserver Name: cluster1-1
                                   Volume Name: vol0
                                Aggregate Name: aggr0
                                   Volume Size: 348.3GB
                            Volume Data Set ID: -
                     Volume Master Data Set ID: -
                                  Volume State: online
                                   Volume Type: RW
                                  Volume Style: flex
                                           ...
                        Space Guarantee Style: volume
                     Space Guarantee in Effect: true
                                           ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

Sobre parâmetros posicionais

Você pode aproveitar a funcionalidade de parâmetro posicional da CLI do ONTAP para aumentar a eficiência na entrada de comandos. Você pode consultar um comando para identificar parâmetros que são posicionais para o comando.

O que é um parâmetro posicional

- Um parâmetro posicional é um parâmetro que não requer que você especifique o nome do parâmetro antes de especificar o valor do parâmetro.
- Um parâmetro posicional pode ser intercalado com parâmetros não posicionais na entrada do comando,

desde que observe sua sequência relativa com outros parâmetros posicionais no mesmo comando, como indicado na ***command_name ?*** saída.

- Um parâmetro posicional pode ser um parâmetro obrigatório ou opcional para um comando.
- Um parâmetro pode ser posicional para um comando, mas não posicional para outro.

> O uso da funcionalidade de parâmetro posicional em scripts não é recomendado, especialmente quando os parâmetros posicionais são opcionais para o comando ou têm parâmetros opcionais listados antes deles.

Identificar um parâmetro posicional

Você pode identificar um parâmetro posicional na ***command_name ?*** saída do comando. Um parâmetro posicional tem colchetes em torno do nome do parâmetro, em um dos seguintes formatos:

- [*-parameter_name parameter_value*] mostra um parâmetro necessário que é posicional.
- [*-parameter_name*[*parameter_value*] mostra um parâmetro opcional que é posicional.

Por exemplo, quando exibido como o seguinte na ***command_name ?*** saída, o parâmetro é posicional para o comando em que aparece:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

No entanto, quando exibido como o seguinte, o parâmetro é não posicional para o comando em que aparece:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Exemplos de uso de parâmetros posicionais

No exemplo a seguir, a ***volume create ?*** saída mostra que três parâmetros são posicionais para o comando: `-volume` `-aggregate` , E `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

No exemplo a seguir, o `volume create` comando é especificado sem tirar vantagem da funcionalidade do parâmetro posicional:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

Os exemplos a seguir usam a funcionalidade de parâmetro posicional para aumentar a eficiência da entrada de comando. Os parâmetros posicionais são intercalados com parâmetros não posicionais no `volume create` comando, e os valores dos parâmetros posicionais são especificados sem os nomes dos parâmetros. Os parâmetros posicionais são especificados na mesma sequência indicada pela **`volume create ?`** saída. Ou seja, o valor para `-volume` é especificado antes do `-aggregate` de , que por sua vez é especificado antes do de `-size`.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0

cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

Métodos de acesso a páginas man do ONTAP

As páginas de manual do ONTAP (man) explicam como usar os comandos do ONTAP CLI. Essas páginas estão disponíveis na linha de comando e também são publicadas em *referências de comando* específicas da versão.

Na linha de comando ONTAP, use o `man command_name` comando para exibir a página manual do comando especificado. Se você não especificar um nome de comando, o índice de página manual será exibido. Você pode usar o `man man` comando para exibir informações sobre o `man` próprio comando. Pode sair de uma página de manual introduzindo **`q`**.

Consulte o Referência de comando para a sua versão do ONTAP 9 para saber mais sobre os comandos ONTAP de nível de administrador e de nível avançado disponíveis na sua versão.

Gerenciar sessões de CLI

Você pode gravar uma sessão CLI em um arquivo com um limite de nome e tamanho especificado e, em seguida, fazer o upload do arquivo para um destino FTP ou HTTP. Você também pode exibir ou excluir arquivos nos quais você gravou sessões CLI anteriormente.

Grave uma sessão CLI

Um Registro de uma sessão CLI termina quando você interrompe a gravação ou termina a sessão CLI, ou quando o arquivo atinge o limite de tamanho especificado. O limite de tamanho padrão do arquivo é de 1 MB. O limite máximo de tamanho do arquivo é de 2 GB.

Gravar uma sessão CLI é útil, por exemplo, se você estiver solucionando um problema e quiser salvar informações detalhadas ou se quiser criar um Registro permanente de uso de espaço em um determinado momento.

Passos

1. Comece a gravar a sessão CLI atual em um arquivo:

   ```
   system script start
   ```

   Para obter mais informações sobre como usar o `system script start` comando, consulte a página de manual.

   O ONTAP começa a gravar sua sessão CLI no arquivo especificado.

2. Prossiga com sua sessão CLI.
3. Quando terminar, pare de gravar a sessão:

   ```
   system script stop
   ```

   Para obter mais informações sobre como usar o `system script stop` comando, consulte a página de manual.

   O ONTAP pára de gravar sua sessão CLI.

Comandos para gerenciar Registros de sessões CLI

Você usa os `system script` comandos para gerenciar Registros de sessões CLI.

Se você quiser…	Use este comando…
Comece a gravar a sessão CLI atual em um arquivo especificado	`system script start`

Se você quiser…	Use este comando…
Pare de gravar a sessão CLI atual	`system script stop`
Exibir informações sobre Registros de sessões CLI	`system script show`
Carregue um Registro de uma sessão CLI para um destino FTP ou HTTP	`system script upload`
Excluir um Registro de uma sessão CLI	`system script delete`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar o período de tempo limite automático das sessões CLI

O valor de tempo limite especifica por quanto tempo uma sessão CLI permanece inativa antes de ser terminada automaticamente. O valor de tempo limite da CLI é de todo o cluster. Ou seja, cada nó em um cluster usa o mesmo valor de tempo limite da CLI.

Por padrão, o período de tempo limite automático das sessões CLI é de 30 minutos.

Você usa os `system timeout` comandos para gerenciar o período de tempo limite automático das sessões CLI.

Se você quiser…	Use este comando…
Exibir o período de tempo limite automático para sessões CLI	`system timeout show`
Modifique o período de tempo limite automático para sessões CLI	`system timeout modify`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciamento de clusters (somente administradores de cluster)

Exibir informações sobre os nós em um cluster

Você pode exibir nomes de nós, se os nós estão íntegros e se eles estão qualificados para participar do cluster. No nível de privilégio avançado, você também pode exibir se um nó contém epsilon.

Passos

1. Para exibir informações sobre os nós em um cluster, use o `cluster show` comando.

Se você quiser que a saída mostre se um nó possui epsilon, execute o comando no nível de privilégio avançado.

Exemplos de exibição dos nós em um cluster

O exemplo a seguir exibe informações sobre todos os nós em um cluster de quatro nós:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

O exemplo a seguir exibe informações detalhadas sobre o nó chamado "'node1" no nível de privilégio avançado:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

Exibir atributos do cluster

Você pode exibir o identificador exclusivo de um cluster (UUID), nome, número de série, localização e informações de Contato.

Passos

1. Para exibir os atributos de um cluster, use o `cluster identity show` comando.

Exemplo de exibição de atributos de cluster

O exemplo a seguir exibe o nome, o número de série, a localização e as informações de Contato de um cluster.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

Modifique os atributos do cluster

Você pode modificar os atributos de um cluster, como o nome do cluster, o local e as informações de Contato, conforme necessário.

Sobre esta tarefa

Não é possível alterar o UUID de um cluster, que é definido quando o cluster é criado.

Passos

1. Para modificar atributos de cluster, use o `cluster identity modify` comando.

   O `-name` parâmetro especifica o nome do cluster. A `cluster identity modify` página man descreve as regras para especificar o nome do cluster.

   O `-location` parâmetro especifica a localização do cluster.

   O `-contact` parâmetro especifica as informações de Contato, como um nome ou endereço de e-mail.

Exemplo de renomeação de um cluster

O comando a seguir renomeia o cluster atual ("'cluster1') para "'cluster2'":

```
cluster1::> cluster identity modify -name cluster2
```

Exibir o status dos anéis de replicação do cluster

Você pode exibir o status dos anéis de replicação do cluster para ajudar a diagnosticar problemas em todo o cluster. Se o cluster tiver problemas, a equipe de suporte poderá solicitar que você execute esta tarefa para ajudar nos esforços de solução de problemas.

Passos

1. Para exibir o status dos anéis de replicação do cluster, use o `cluster ring show` comando no nível de privilégio avançado.

Exemplo de exibição do status de replicação do anel do cluster

O exemplo a seguir exibe o status do anel de replicação VLDB em um nó chamado node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

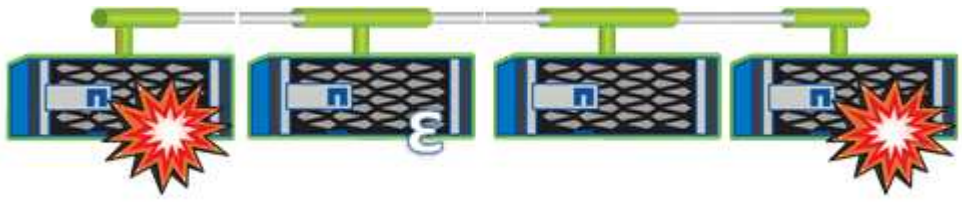
Sobre quórum e epsilon

O quórum e o epsilon são medidas importantes de integridade e função do cluster que, em conjunto, indicam como os clusters abordam potenciais desafios de comunicação e conetividade.

Quorum é uma pré-condição para um cluster totalmente funcional. Quando um cluster está no quórum, uma maioria simples dos nós é saudável e pode se comunicar uns com os outros. Quando o quorum é perdido, o cluster perde a capacidade de realizar operações normais de cluster. Apenas uma coleção de nós pode ter quórum de cada vez, porque todos os nós compartilham coletivamente uma única visualização dos dados. Portanto, se dois nós não-comunicantes forem permitidos modificar os dados de maneiras divergentes, não será mais possível reconciliar os dados em uma única visualização de dados.

Cada nó no cluster participa de um protocolo de votação que elege um nó *master*; cada nó restante é um *secondary*. O nó principal é responsável pela sincronização de informações no cluster. Quando o quórum é formado, ele é mantido por votação contínua. Se o nó mestre ficar offline e o cluster ainda estiver no quórum, um novo mestre será eleito pelos nós que permanecem online.

Como existe a possibilidade de um empate em um cluster que tem um número par de nós, um nó tem um peso de votação fracionário extra chamado *epsilon*. Se a conetividade entre duas partes iguais de um cluster grande falhar, o grupo de nós que contêm epsilon mantém quórum, assumindo que todos os nós estão saudáveis. Por exemplo, a ilustração a seguir mostra um cluster de quatro nós no qual dois dos nós falharam. No entanto, como um dos nós sobreviventes possui epsilon, o cluster permanece no quórum, embora não haja uma maioria simples de nós saudáveis.



O Epsilon é atribuído automaticamente ao primeiro nó quando o cluster é criado. Se o nó que mantém o epsilon não estiver saudável, assumir o seu parceiro de alta disponibilidade ou for assumido pelo parceiro de alta disponibilidade, o epsilon será reatribuído automaticamente a um nó saudável em um par de HA diferente.

Colocar um nó off-line pode afetar a capacidade do cluster de permanecer no quorum. Portanto, o ONTAP emite uma mensagem de aviso se você tentar uma operação que irá tirar o cluster do quórum ou então colocar uma interrupção longe de uma perda de quórum. Você pode desativar as mensagens de aviso de quórum usando o `cluster quorum-service options modify` comando no nível avançado de privilégio.

Em geral, assumindo uma conetividade confiável entre os nós do cluster, um cluster maior é mais estável do que um cluster menor. O requisito de quórum de uma maioria simples de metade dos nós mais o epsilon é mais fácil de manter em um cluster de 24 nós do que em um cluster de dois nós.

Um cluster de dois nós apresenta alguns desafios únicos para manter o quórum. Os clusters de dois nós usam *cluster HA*, no qual nenhum nó detém epsilon; em vez disso, ambos os nós são continuamente polled para garantir que, se um nó falhar, o outro tem acesso completo de leitura e gravação aos dados, bem como acesso a interfaces lógicas e funções de gerenciamento.

Quais são os volumes do sistema

Os volumes do sistema são volumes do FlexVol que contêm metadados especiais, como metadados para logs de auditoria de serviços de arquivo. Esses volumes ficam visíveis no cluster para que você possa considerar totalmente o uso do storage no cluster.

Os volumes de sistema pertencem ao servidor de gerenciamento de cluster (também chamado de administrador SVM) e são criados automaticamente quando a auditoria de serviços de arquivos é ativada.

Você pode visualizar volumes do sistema usando o `volume show` comando, mas a maioria das outras operações de volume não são permitidas. Por exemplo, você não pode modificar um volume de sistema usando o `volume modify` comando.

Este exemplo mostra quatro volumes de sistema no SVM admin, que foram criados automaticamente quando a auditoria de serviços de arquivo foi ativada para um SVM de dados no cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Gerenciar nós

Adicione nós ao cluster

Depois que um cluster é criado, você pode expandi-lo adicionando nós a ele. Você adiciona apenas um nó de cada vez.

O que você vai precisar

- Se você estiver adicionando nós a um cluster de vários nós, todos os nós existentes no cluster devem estar íntegros (indicado pela `cluster show`).
- Se estiver adicionando nós a um cluster sem switch de dois nós, você deverá converter seu cluster sem switch de dois nós para um cluster conetado ao switch usando um switch de cluster compatível com NetApp.

  A funcionalidade de cluster sem switch é suportada apenas em um cluster de dois nós.

- Se você estiver adicionando um segundo nó a um cluster de nó único, o segundo nó deve ter sido instalado e a rede de cluster deve ter sido configurada.
- Se o cluster tiver a configuração automática do SP ativada, a sub-rede especificada para o SP deve ter recursos disponíveis para permitir que o nó de junção use a sub-rede especificada para configurar automaticamente o SP.
- Você deve ter reunido as seguintes informações para o LIF de gerenciamento de nós do novo nó:
  - Porta
  - Endereço IP
  - Máscara de rede

- Gateway predefinido

Sobre esta tarefa

Os nós precisam estar em números pares para que possam formar pares de HA. Depois de começar a adicionar um nó ao cluster, você deve concluir o processo. O nó deve fazer parte do cluster antes de poder começar a adicionar outro nó.

Passos

1. Ligue o nó que você deseja adicionar ao cluster.

   O nó é inicializado e o assistente de configuração do nó é iniciado no console.

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. Saia do assistente de configuração do nó: `exit`

   O assistente de configuração do nó é encerrado e é apresentado um aviso de início de sessão, avisando que não concluiu as tarefas de configuração.

3. Inicie sessão na conta de administrador utilizando o `admin` nome de utilizador.
4. Inicie o assistente Configuração do cluster:

   `cluster setup`

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

Para obter mais informações sobre como configurar um cluster usando a GUI de configuração, consulte a "System Manager" ajuda on-line.

5. Pressione Enter para usar a CLI para concluir esta tarefa. Quando for solicitado a criar um novo cluster ou ingressar em um existente, digite **`join`**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

Se a versão do ONTAP em execução no novo nó for diferente da versão em execução no cluster existente, o sistema informará um `System checks Error: Cluster join operation cannot be performed at this time` erro. Este é o comportamento esperado. Para continuar, execute o `add-node -allow-mixed-version-join new_node_name` comando no nível de privilégio avançado a partir de um nó existente no cluster.

6. Siga as instruções para configurar o nó e associá-lo ao cluster:
   - Para aceitar o valor padrão de um prompt, pressione Enter.
   - Para inserir seu próprio valor para um prompt, digite o valor e pressione Enter.
7. Repita as etapas anteriores para cada nó adicional que você deseja adicionar.

Depois de terminar

Depois de adicionar nós ao cluster, ative o failover de storage para cada par de HA.

Informações relacionadas

"Clusters ONTAP de versão mista"

Remova os nós do cluster

Você pode remover nós indesejados de um cluster, um nó de cada vez. Depois de remover um nó, você também deve remover o parceiro de failover. Se você estiver removendo um nó, seus dados ficarão inacessíveis ou apagados.

Antes de começar

As condições a seguir devem ser satisfeitas antes de remover nós do cluster:

- Mais da metade dos nós no cluster precisa estar saudável.
- Todos os dados, volumes e agregados não-raiz foram transferidos ou removidos do nó.
  - Todos os dados no nó que você deseja remover devem ter sido evacuados. Isso pode incluir "limpando dados de um volume criptografado".
  - Todos os volumes que não são raiz "movido"foram de agregados pertencentes ao nó.
  - Todos os agregados que não são root foram "eliminado"do nó.
- Todas as LIFs e VLANs foram relocadas ou removidas do nó.
  - Os LIFs de dados foram "eliminado" ou "relocado" do nó.
  - As LIFs de gerenciamento de cluster foram "relocado"do nó e as portas iniciais foram alteradas.
  - Todos os LIFs entre clusters foram "removido". Ao remover LIFs entre clusters, é exibido um aviso que pode ser ignorado.
  - Todas as VLANs no nó foram "eliminado".
- O nó não está participando de nenhum relacionamento de failover.
  - O failover de storage "desativado"foi para o nó.
  - Todas as regras de failover de LIF foram "modificado" para remover portas no nó.
- Se o nó possuir discos FIPS (Federal Information Processing Standards) ou SEDs (Self-Encrypting Disks)"a criptografia de disco foi removida", retornando os discos para o modo desprotegido.
  - Você também pode querer "Higienizar unidades FIPS ou SEDs".
- Se você tiver LUNs no nó a ser removido, você deve "Modifique a lista de nós de relatório do mapa LUN seletivo (SLM)" antes de remover o nó.

  Se você não remover o nó e seu parceiro de HA da lista de nós de relatórios do SLM, o acesso às LUNs anteriormente no nó poderá ser perdido mesmo que os volumes que contêm as LUNs tenham sido movidos para outro nó.

Recomenda-se que você emita uma mensagem do AutoSupport para notificar o suporte técnico da NetApp de que a remoção do nó está em andamento.

> Não execute operações como `cluster remove-node` , `cluster unjoin` e `node rename` quando uma atualização automática do ONTAP estiver em andamento.

Sobre esta tarefa

- Se você estiver executando um cluster de versão mista, poderá remover o último nó de versão baixa usando um dos comandos de privilégio avançados que começam com ONTAP 9.3:
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`

- ONTAP 9 .4 e posterior: `cluster remove-node -skip-last-low-version-node-check`

- Se você desmarcar 2 nós de um cluster de 4 nós, o HA do cluster será automaticamente ativado nos dois nós restantes.

> Todos os dados do sistema e do usuário, de todos os discos conetados ao nó, devem ficar inacessíveis aos usuários antes de remover um nó do cluster. Se um nó foi desvinculado incorretamente de um cluster, entre em Contato com o suporte da NetApp para obter assistência com opções de recuperação.

Passos

1. Altere o nível de privilégio para avançado:

```
set -privilege advanced
```

2. Verifique se um nó no cluster contém epsilon:

```
cluster show -epsilon true
```

3. Se um nó no cluster contiver epsilon e esse nó for desvinculado, mova o epsilon para um nó que não será desconetado:
   a. Mova o epsilon do nó que vai ser desconetado

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

   b. Mova o epsilon para um nó que não vai ser desconetado:

```
cluster modify -node <node_name> -epsilon true
```

4. Identificar o nó principal atual:

```
cluster ring show
```

   O nó principal é o nó que contém processos como `mgmt` , `vldb`, , `vifmgr`, `bcomd` `crs` e .

5. Se o nó que você deseja remover for o nó principal atual, habilite outro nó no cluster a ser eleito como o nó mestre:
   a. Torne o nó principal atual inelegível para participar do cluster:

```
cluster modify -node <node_name> -eligibility false
```

   Isso fará com que o nó seja marcado como não saudável até que a elegibilidade seja restaurada na próxima etapa. Quando o nó mestre se torna inelegível, um dos nós restantes é eleito pelo quorum do

cluster como o novo mestre.

b. Torne o nó principal anterior elegível para participar novamente no cluster:

```
cluster modify -node <node_name> -eligibility true
```

6. Faça login no LIF de gerenciamento de nós remoto ou no LIF de gerenciamento de cluster em um nó diferente daquele que está sendo removido.
7. Remova o nó do cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9,3	`cluster unjoin`

ONTAP 9 .4 e mais tarde	Com nome do nó:
	`cluster remove-node -name <node_name>`
	Com IP do nó:
	`cluster remove-node -cluster_ip <node_ip>`

Se você tiver um cluster de versão mista e estiver removendo o último nó de versão inferior, use o `-skip -last-low-version-node-check` parâmetro com esses comandos.

O sistema informa-o do seguinte:

- Você também deve remover o parceiro de failover do nó do cluster.
- Depois que o nó é removido e antes que ele possa reingressar em um cluster, você deve usar a opção de menu de inicialização (4) Limpar configuração e inicializar todos os discos ou a opção (9) Configurar particionamento de unidade avançado para apagar a configuração do nó e inicializar todos os discos.

  Uma mensagem de falha é gerada se você tiver condições que devem ser endereçadas antes de remover o nó. Por exemplo, a mensagem pode indicar que o nó tem recursos compartilhados que você deve remover ou que o nó está em uma configuração de HA de cluster ou configuração de failover de storage que você deve desativar.

Se o nó for o mestre do quórum, o cluster perderá brevemente e retornará ao quórum. Essa perda de quorum é temporária e não afeta nenhuma operação de dados.

8. Se uma mensagem de falha indicar condições de erro, aborde essas condições e execute novamente o `cluster remove-node` comando ou `cluster unjoin`.

O nó é reinicializado automaticamente depois de removido com sucesso do cluster.

9. Se você estiver reutilizando o nó, apague a configuração do nó e inicialize todos os discos:
   a. Durante o processo de inicialização, pressione Ctrl-C para exibir o menu de inicialização quando solicitado a fazê-lo.
   b. Selecionar a opção do menu de arranque (4) Limpar a configuração e inicializar todos os discos.
10. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

11. Repita as etapas anteriores para remover o parceiro de failover do cluster.

Acesse os arquivos de log, despejo de memória e MIB de um nó usando um navegador da Web

O (`spi`serviço da Web Service Processor Infrastructure) está habilitado por padrão para permitir que um navegador da Web acesse os arquivos de log, despejo de núcleo e MIB de um nó no cluster. Os arquivos permanecem acessíveis mesmo quando o nó está inativo, desde que o nó seja assumido pelo parceiro.

O que você vai precisar

- O LIF de gerenciamento de clusters deve estar ativo.

  Você pode usar o LIF de gerenciamento do cluster ou de um nó para acessar o `spi` serviço da Web. No entanto, é recomendável usar o LIF de gerenciamento de cluster.

  O `network interface show` comando exibe o status de todas as LIFs no cluster.

- Você deve usar uma conta de usuário local para acessar o `spi` serviço da Web, as contas de usuário de domínio não são suportadas.
- Se a sua conta de usuário não tiver a função "admin" (que tem acesso ao `spi` serviço da Web por padrão), sua função de controle de acesso deve ter acesso ao `spi` serviço da Web.

  O `vserver services web access show` comando mostra quais funções têm acesso a quais serviços da Web.

- Se você não estiver usando a conta de usuário "'admin'" (que inclui o `http` método de acesso por padrão), sua conta de usuário deve ser configurada com o `http` método de acesso.

  O `security login show` comando mostra os métodos de acesso e login das contas de usuário e suas funções de controle de acesso.

- Se você quiser usar HTTPS para acesso seguro à Web, o SSL deve estar habilitado e um certificado digital deve ser instalado.

  O `system services web show` comando exibe a configuração do mecanismo de protocolo da Web no nível do cluster.

Sobre esta tarefa

O `spi` serviço da Web está ativado por predefinição e o serviço pode ser desativado manualmente (`vserver services web modify -vserver * -name spi -enabled false`).

A função "'admin'" tem acesso ao `spi` serviço web por padrão e o acesso pode ser desativado manualmente (`services web access delete -vserver` *`cluster_name`* `-name spi -role admin`).

Passos

1. Aponte o navegador da Web para o `spi` URL do serviço da Web em um dos seguintes formatos:
   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

   `cluster-mgmt-LIF` É o endereço IP do LIF de gerenciamento de cluster.
2. Quando solicitado pelo navegador, insira sua conta de usuário e senha.

   Depois que a conta for autenticada, o navegador exibirá links para os `/mroot/etc/log/` diretórios , `/mroot/etc/crash/` e `/mroot/etc/mib/` de cada nó no cluster.

Acesse o console do sistema de um nó

Se um nó estiver suspenso no menu de inicialização ou no prompt do ambiente de inicialização, você poderá acessá-lo somente pelo console do sistema (também chamado de *console serial*). Você pode acessar o console do sistema de um nó a partir de uma conexão SSH para o SP do nó ou para o cluster.

Sobre esta tarefa

Tanto o SP quanto o ONTAP oferecem comandos que permitem acessar o console do sistema. No entanto, a partir do SP, você pode acessar apenas o console do sistema de seu próprio nó. No cluster, você pode acessar o console do sistema de qualquer nó no cluster.

Passos

1. Acesse o console do sistema de um nó:

Se você está no…	Digite este comando…
CLI do SP do nó	`system console`
CLI do ONTAP	`system node run-console`

2. Inicie sessão na consola do sistema quando lhe for pedido que o faça.
3. Para sair do console do sistema, pressione Ctrl-D.

Exemplos de acesso ao console do sistema

O exemplo a seguir mostra o resultado da inserção `system console` do comando no prompt "'SP node2'". O console do sistema indica que o node2 está suspenso no prompt do ambiente de inicialização. O `boot_ontap` comando é inserido no console para inicializar o nó no ONTAP. Ctrl-D é então pressionado para sair do console e retornar ao SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(Ctrl-D é pressionado para sair do console do sistema.)

```
Connection to 123.12.123.12 closed.
SP node2>
```

O exemplo a seguir mostra o resultado de inserir o `system node run-console` comando do ONTAP para acessar o console do sistema do node2, que está pendurado no prompt do ambiente de inicialização. O `boot_ontap` comando é inserido no console para inicializar o node2 no ONTAP. Ctrl-D é então pressionado para sair do console e retornar ao ONTAP.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(Ctrl-D é pressionado para sair do console do sistema.)

```
Connection to 123.12.123.12 closed.
cluster1::>
```

Gerenciar volumes de raiz de nós e agregados de raiz

O volume raiz de um nó é um FlexVol volume instalado na fábrica ou pelo software de configuração. Ele é reservado para arquivos de sistema, arquivos de log e arquivos principais. O nome do diretório é `/mroot`, que é acessível somente através do systemshell pelo suporte técnico. O tamanho mínimo para o volume raiz de um nó depende do modelo da plataforma.

Regras que regem os volumes de raiz dos nós e a visão geral dos agregados de raiz

O volume raiz de um nó contém diretórios e arquivos especiais para esse nó. O agregado raiz contém o volume raiz. Algumas regras governam o volume raiz e o agregado raiz de um nó.

- As seguintes regras regem o volume raiz do nó:
  - A menos que o suporte técnico o instrua a fazê-lo, não modifique a configuração ou o conteúdo do volume raiz.
  - Não armazene dados do usuário no volume raiz.

    Armazenar dados de usuário no volume raiz aumenta o tempo de giveback de storage entre nós em um par de HA.

  - Você pode mover o volume raiz para outro agregado. [relocate-root]Consulte .
- O agregado raiz é dedicado apenas ao volume raiz do nó.

  O ONTAP impede que você crie outros volumes no agregado raiz.

"NetApp Hardware Universe"

Libere espaço no volume raiz de um nó

Uma mensagem de aviso aparece quando o volume raiz de um nó ficou cheio ou quase cheio. O nó não pode funcionar corretamente quando seu volume raiz está cheio. Você pode liberar espaço no volume raiz de um nó excluindo arquivos de despejo de núcleo, arquivos de rastreamento de pacotes e cópias Snapshot de volume raiz.

Passos

1. Exiba os arquivos de despejo de núcleo do nó e seus nomes:

   ```
   system node coredump show
   ```

2. Excluir arquivos indesejados de despejo de memória do nó:

   ```
   system node coredump delete
   ```

3. Acesse o nodeshell:

   `system node run -node` *`nodename`*

   `nodename` é o nome do nó cujo espaço de volume raiz você deseja liberar.

4. Mude para o nível de privilégio avançado nodeshell a partir do nodeshell:

priv set advanced

5. Exiba e exclua os arquivos de rastreamento de pacotes do nó através do nodeshell:
   a. Exibir todos os arquivos no volume raiz do nó:

      ls /etc

   b. Se algum arquivo de rastreamento de pacote (`*.trc`) estiver no volume raiz do nó, exclua-os individualmente:

      rm /etc/log/packet_traces/*file_name.trc*

6. Identifique e exclua as cópias Snapshot do volume raiz do nó através do nodeshell:
   a. Identifique o nome do volume raiz:

      vol status

      O volume raiz é indicado pela palavra "root" na coluna "Opções" da `vol status` saída do comando.

      No exemplo a seguir, o volume raiz é `vol0`:

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   a. Exibir cópias Snapshot do volume raiz:

      snap list root_vol_name

   b. Excluir cópias snapshot do volume raiz indesejadas:

      snap delete root_vol_namesnapshot_name

7. Saia do nodeshell e volte para a concha:

   exit

Realocar volumes raiz para novos agregados

O procedimento de substituição de raiz migra o agregado de raiz atual para outro conjunto de discos sem interrupção.

Sobre esta tarefa

O failover de armazenamento deve estar habilitado para realocar volumes raiz. Você pode usar o `storage failover modify -node *nodename* -enable true` comando para ativar o failover.

Você pode alterar o local do volume raiz para um novo agregado nos seguintes cenários:

- Quando os agregados de raiz não estão no disco que preferir
- Quando pretender reorganizar os discos ligados ao nó
- Quando estiver a efetuar uma substituição de prateleira das prateleiras de disco EOS

Passos

1. Defina o nível de privilégio como avançado:

   `set privilege advanced`

2. Realocar o agregado raiz:

   `system node migrate-root -node` *`nodename`* `-disklist` *`disklist`* `-raid-type` *`raid-type`*

   - **-node**

     Especifica o nó que possui o agregado raiz que você deseja migrar.

   - **-disklist**

     Especifica a lista de discos nos quais o novo agregado raiz será criado. Todos os discos precisam ser sobressalentes e de propriedade do mesmo nó. O número mínimo de discos necessário depende do tipo RAID.

   - **-raid-type**

     Especifica o tipo RAID do agregado raiz. O valor padrão é `raid-dp`.

3. Monitorize o progresso do trabalho:

   `job show -id` *`jobid`* `-instance`

Resultados

Se todas as pré-verificações forem bem-sucedidas, o comando iniciará uma tarefa de substituição de volume raiz e será encerrado. Espere que o nó seja reiniciado.

Iniciar ou parar uma visão geral do nó

Talvez seja necessário iniciar ou parar um nó por motivos de manutenção ou solução de problemas. Você pode fazer isso a partir da CLI do ONTAP, do prompt do ambiente de inicialização ou da CLI do SP.

O uso do comando SP CLI `system power off` ou `system power cycle` para desligar ou desligar um nó pode causar um desligamento inadequado do nó (também chamado de *desligamento anormal*) e não substitui um desligamento gracioso usando o comando ONTAP `system node halt`.

Reinicie um nó no prompt do sistema

Você pode reinicializar um nó no modo normal a partir do prompt do sistema. Um nó é configurado para inicializar a partir do dispositivo de inicialização, como uma placa CompactFlash do PC.

Passos

1. Se o cluster contiver quatro ou mais nós, verifique se o nó a ser reiniciado não possui epsilon:

   a. Defina o nível de privilégio como avançado:

      set -privilege advanced

   b. Determine qual nó contém o epsilon:

      cluster show

      O exemplo a seguir mostra que "'node1" contém epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. Se o nó a ser reinicializado contiver epsilon, remova o epsilon do nó:

      cluster modify -node *node_name* -epsilon false

   b. Atribua o epsilon a um nó diferente que permanecerá ativo:

      cluster modify -node *node_name* -epsilon true

   c. Voltar ao nível de privilégio de administrador:

      set -privilege admin

2. Use o `system node reboot` comando para reinicializar o nó.

   Se você não especificar o `-skip-lif-migration` parâmetro, o comando tentará migrar dados e LIFs de gerenciamento de cluster de forma síncrona para outro nó antes da reinicialização. Se a migração de LIF falhar ou expirar, o processo de reinicialização será abortado e o ONTAP exibirá um erro para indicar a falha de migração de LIF.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

   O nó inicia o processo de reinicialização. O prompt de login do ONTAP é exibido, indicando que o processo de reinicialização está concluído.

Inicie o ONTAP no prompt do ambiente de inicialização

Você pode inicializar a versão atual ou a versão de backup do ONTAP quando estiver no prompt do ambiente de inicialização de um nó.

Passos

1. Acesse o prompt do ambiente de inicialização a partir do prompt do sistema de armazenamento usando o `system node halt` comando.

   O console do sistema de armazenamento exibe o prompt do ambiente de inicialização.

2. No prompt do ambiente de inicialização, digite um dos seguintes comandos:

Para iniciar…	Digite…
A versão atual do ONTAP	`boot_ontap`
A imagem primária do ONTAP a partir do dispositivo de arranque	`boot_primary`
A imagem de cópia de segurança do ONTAP a partir do dispositivo de arranque	`boot_backup`

   Se você não tiver certeza sobre qual imagem usar, você deve usar `boot_ontap` na primeira instância.

Encerre um nó

Você pode encerrar um nó se ele ficar sem resposta ou se a equipe de suporte o direcionar para fazer isso como parte dos esforços de solução de problemas.

Passos

1. Se o cluster contiver quatro ou mais nós, verifique se o nó a ser desligado não possui epsilon:

   a. Defina o nível de privilégio como avançado:

      `set -privilege advanced`

   b. Determine qual nó contém o epsilon:

      `cluster show`

      O exemplo a seguir mostra que "'node1" contém epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. Se o nó a ser desligado mantiver o epsilon, remova o epsilon do nó:

```
cluster modify -node node_name -epsilon false
```

b. Atribua o epsilon a um nó diferente que permanecerá ativo:

```
cluster modify -node node_name -epsilon true
```

c. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

2. Use o `system node halt` comando para encerrar o nó.

   Se você não especificar o `-skip-lif-migration` parâmetro, o comando tentará migrar dados e LIFs de gerenciamento de cluster de forma síncrona para outro nó antes do desligamento. Se a migração de LIF falhar ou expirar o tempo, o processo de encerramento é cancelado e o ONTAP exibe um erro para indicar a falha de migração de LIF.

   Você pode acionar manualmente um despejo de memória com o desligamento usando ambos os `-dump` parâmetros.

   O exemplo a seguir desliga o nó chamado "'node1" para manutenção de hardware:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Gerencie um nó usando o menu de inicialização

Você pode usar o menu de inicialização para corrigir problemas de configuração em um nó, redefinir a senha de administrador, inicializar discos, redefinir a configuração do nó e restaurar as informações de configuração do nó de volta para o dispositivo de inicialização.

> Se um par de HA estiver usando "Criptografia de unidades SAS ou NVMe (SED, NSE, FIPS)", siga as instruções no "Retornar uma unidade FIPS ou SED para o modo desprotegido"tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Passos

1. Reinicie o nó para acessar o menu de inicialização usando o `system node reboot` comando no prompt do sistema.

   O nó inicia o processo de reinicialização.

2. Durante o processo de reinicialização, pressione Ctrl-C para exibir o menu de inicialização quando solicitado a fazê-lo.

   O nó exibe as seguintes opções para o menu de inicialização:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

Opção de menu de inicialização (2) a inicialização sem /etc/rc é obsoleta e não tem efeito no sistema.

3. Selecione uma das seguintes opções inserindo o número correspondente:

Para…	Selecione…
Continue a inicializar o nó no modo normal	1) bota normal
Altere a senha do nó, que também é a senha da conta "admin"	3) altere a senha

Para…	Selecione…
Inicialize os discos do nó e crie um volume raiz para o nó	4) limpe a configuração e inicialize todos os discos Esta opção de menu apaga todos os dados nos discos do nó e redefine a configuração do nó para as configurações padrão de fábrica. Selecione este item de menu apenas depois de o nó ter sido removido de um cluster (não associado) e não ser Unido a outro cluster. Para um nó com compartimentos de disco internos ou externos, o volume raiz nos discos internos é inicializado. Se não houver compartimentos de disco internos, o volume raiz nos discos externos será inicializado. Para um sistema que executa a virtualização FlexArray com compartimentos de disco internos ou externos, os LUNs do array não são inicializados. Todos os discos nativos em compartimentos internos ou externos são inicializados. Para um sistema que executa a virtualização FlexArray apenas com LUNS de array e sem compartimentos de disco internos ou externos, o volume raiz nos LUNS de storage array é inicializado, consulte "A instalar o FlexArray". Se o nó que você deseja inicializar tiver discos particionados para particionamento de dados raiz, os discos devem ser desparticionados antes que o nó possa ser inicializado, consulte **9) Configurar particionamento de unidade avançado** e "Gerenciamento de discos e agregados".
Execute operações de manutenção de disco e agregado e obtenha informações detalhadas sobre o agregado e o disco.	5) Inicialização do modo de manutenção Você sai do modo Manutenção usando o `halt` comando.
Restaure as informações de configuração do volume raiz do nó para o dispositivo de inicialização, como um cartão CompactFlash do PC	6) Atualizar flash a partir da configuração de backup O ONTAP armazena algumas informações de configuração de nós no dispositivo de inicialização. Quando o nó é reiniciado, as informações no dispositivo de inicialização são automaticamente gravadas no volume raiz do nó. Se o dispositivo de inicialização ficar corrompido ou precisar ser substituído, você deve usar essa opção de menu para restaurar as informações de configuração do volume raiz do nó de volta para o dispositivo de inicialização.

Para…	Selecione…
Instale um novo software no nó	7) instale primeiro novo software Se o software ONTAP no dispositivo de inicialização não incluir suporte para o storage array que você deseja usar para o volume raiz, você poderá usar essa opção de menu para obter uma versão do software compatível com seu storage array e instalá-lo no nó. Esta opção de menu é apenas para instalar uma versão mais recente do software ONTAP em um nó que não tem volume raiz instalado. *Não* Use esta opção de menu para atualizar o ONTAP.
Reinicie o nó	8) nó de reinicialização

Desparticionar todos os discos e remover suas informações de propriedade ou limpar a configuração e inicializar o sistema com discos inteiros ou particionados	9) Configurar particionamento de unidade avançado
	
	A partir do ONTAP 9.2, a opção particionamento de unidade avançado fornece recursos de gerenciamento adicionais para discos que são configurados para particionamento de dados raiz ou dados raiz. As seguintes opções estão disponíveis na opção de inicialização 9:
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

Exibir atributos do nó

Você pode exibir os atributos de um ou mais nós no cluster, por exemplo, o nome, proprietário, local, número do modelo, número de série, quanto tempo o nó está sendo executado, estado de integridade e elegibilidade para participar de um cluster.

Passos

1. Para exibir os atributos de um nó especificado ou sobre todos os nós em um cluster, use o `system node show` comando.

Exemplo de exibição de informações sobre um nó

O exemplo a seguir exibe informações detalhadas sobre o node1:

```
cluster1::> system node show -node node1
                           Node: node1
                          Owner: Eng IT
                       Location: Lab 5
                          Model: model_number
                  Serial Number: 12345678
                      Asset Tag: -
                         Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                      System ID: 0118051205
                         Vendor: NetApp
                         Health: true
                    Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

Modificar atributos de nó

Você pode modificar os atributos de um nó conforme necessário. Os atributos que você pode modificar incluem as informações de proprietário do nó, informações de localização, etiqueta de ativo e elegibilidade para participar do cluster.

Sobre esta tarefa

A elegibilidade de um nó para participar no cluster pode ser modificada no nível de privilégio avançado usando o `-eligibility` parâmetro do `system node modify` comando ou `cluster modify`. Se você definir a elegibilidade de um nó como `false`, o nó ficará inativo no cluster.

> Não é possível modificar a elegibilidade do nó localmente. Ele deve ser modificado de um nó diferente. A elegibilidade do nó também não pode ser modificada com uma configuração de HA do cluster.

> Você deve evitar definir a elegibilidade de um nó para `false`, exceto para situações como restaurar a configuração do nó ou manutenção prolongada do nó. O acesso a dados SAN e nas ao nó pode ser afetado quando o nó não é elegível.

Passos

1. Use o `system node modify` comando para modificar os atributos de um nó.

Exemplo de modificação de atributos de nó

O comando a seguir modifica os atributos do nó "'node1". O proprietário do nó está definido como "'Joe Smith'" e sua etiqueta de ativo está definida como "'js1234'":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

Renomeie um nó

Você pode alterar o nome de um nó conforme necessário.

Passos

1. Para renomear um nó, use o `system node rename` comando.

   O `-newname` parâmetro especifica o novo nome para o nó. A `system node rename` página man descreve as regras para especificar o nome do nó.

   Se você quiser renomear vários nós no cluster, você deve executar o comando para cada nó individualmente.

   O nome do nó não pode ser "'tudo'" porque "'tudo'" é um nome reservado ao sistema.

Exemplo de renomeação de um nó

O seguinte comando renomeia o nó "'node1" para "'node1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

Gerenciar clusters de nó único

Um cluster de nó único é uma implementação especial de um cluster executado em um nó autônomo. Os clusters de nó único não são recomendados porque não fornecem redundância. Se o nó ficar inativo, o acesso aos dados será perdido.

Para tolerância de falhas e operações ininterruptas, é altamente recomendável configurar seu cluster com "Alta disponibilidade (pares de HA)"o .

Se você optar por configurar ou atualizar um cluster de nó único, você deve estar ciente do seguinte:

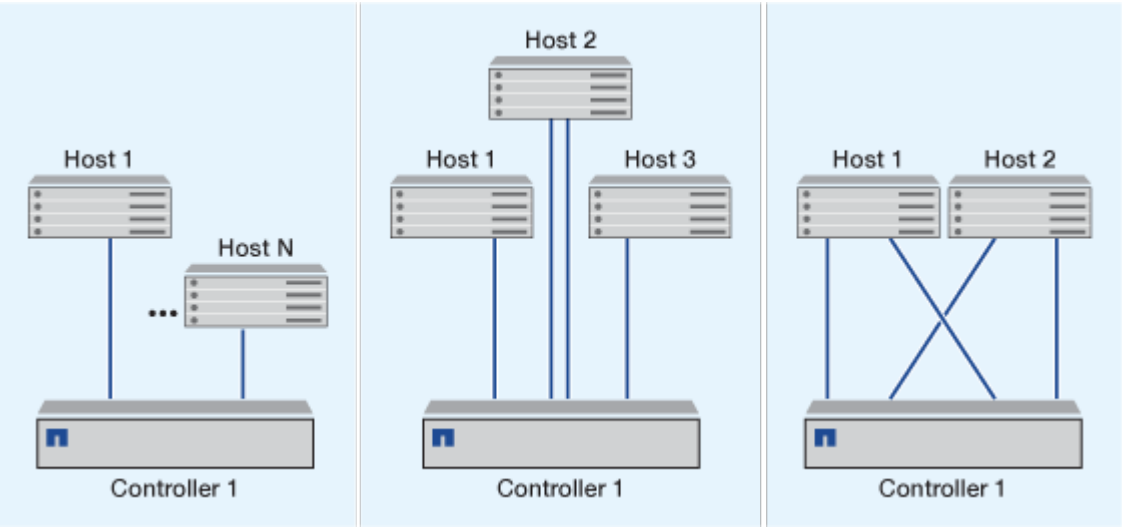
- A criptografia de volume raiz não é compatível com clusters de nó único.
- Se você remover nós para ter um cluster de nó único, modifique as portas do cluster para servir o tráfego de dados, modificando as portas do cluster para serem portas de dados e criando LIFs de dados nas portas de dados.
- Para clusters de nó único, você pode especificar o destino do backup de configuração durante a configuração do software. Após a configuração, essas configurações podem ser modificadas usando comandos ONTAP.
- Se houver vários hosts conetados ao nó, cada host pode ser configurado com um sistema operacional diferente, como Windows ou Linux. Se houver vários caminhos do host para o controlador, o ALUA deve estar habilitado no host.

Maneiras de configurar hosts SAN iSCSI com nós únicos

Você pode configurar hosts SAN iSCSI para se conetar diretamente a um único nó ou para se conetar através de um ou mais switches IP. O nó pode ter várias conexões iSCSI ao switch.

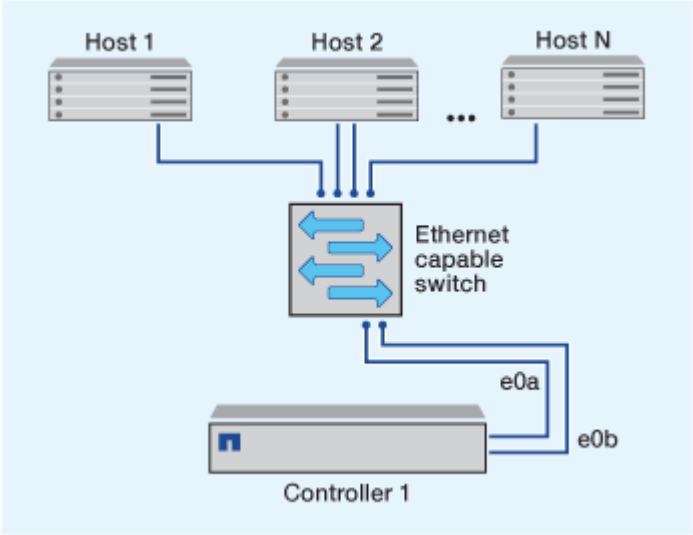
Configurações de nó único com conexão direta

Nas configurações de nó único com conexão direta, um ou mais hosts são conectados diretamente ao nó.



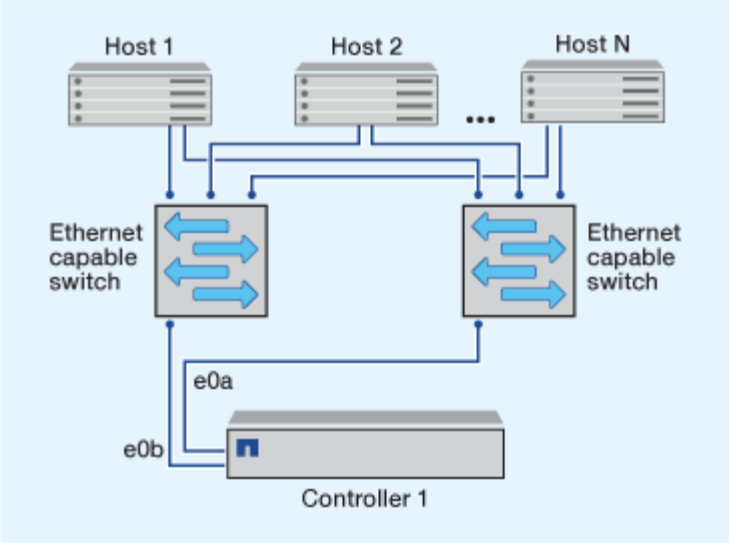
Configurações de nó único de rede única

Em configurações de nó único de rede única, um switch coneta um único nó a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.



Configurações de nó único multi-rede

Em configurações de nó único de várias redes, dois ou mais switches conetam um único nó a um ou mais hosts. Como existem vários switches, essa configuração é totalmente redundante.



Maneiras de configurar hosts SAN FC e FC-NVMe com nós únicos

É possível configurar hosts SAN FC e FC-NVMe com nós únicos por meio de uma ou mais malhas. O NPIV (N-Port ID Virtualization) é necessário e deve ser ativado em todos os switches FC na malha. Não é possível conectar diretamente hosts SAN FC ou FC-NMVE a nós únicos sem usar um switch FC.

Configurações de nó único de malha única

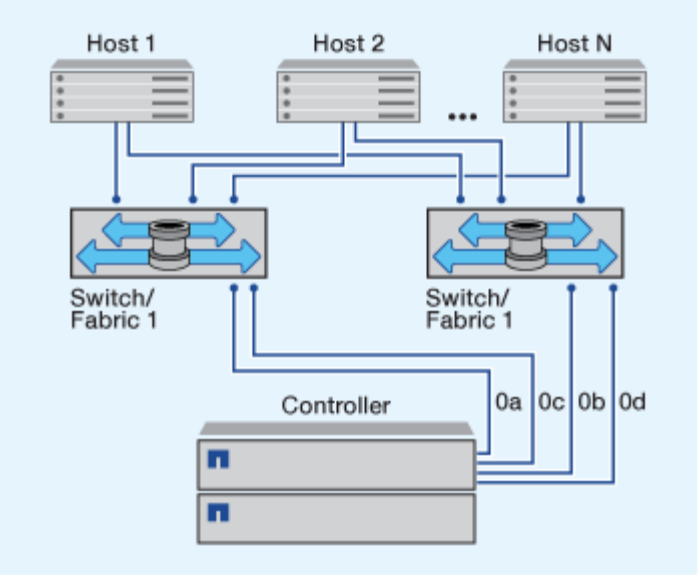
Nas configurações de nó único de estrutura única, há um switch que conecta um único nó a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.

Em configurações de nó único de malha única, o software de multipathing não é necessário se você tiver apenas um caminho único do host para o nó.

Configurações de nó único de MultiFabric

Nas configurações de nó único de várias estruturas, há dois ou mais switches que conectam um único nó a um ou mais hosts. Para simplificar, a figura a seguir mostra uma configuração de nó único de várias malhas com apenas duas malhas. No entanto, você pode ter duas ou mais malhas em qualquer configuração de várias malhas. Nesta figura, o controlador de armazenamento é montado no chassi superior e o chassi inferior pode estar vazio ou pode ter um módulo IOMX, como acontece neste exemplo.

As portas de destino FC (0a, 0C, 0b, 0d) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.



Informações relacionadas

"Relatório técnico da NetApp 4684: Implementando e configurando SANs modernas com NVMe-of"

Atualização do ONTAP para cluster de nó único

A partir do ONTAP 9.2, você pode usar a CLI do ONTAP para executar uma atualização automatizada de um cluster de nó único. Como os clusters de nó único não têm redundância, as atualizações são sempre disruptivas. As atualizações disruptivas não podem ser realizadas usando o System Manager.

Antes de começar

Você deve concluir as etapas de atualização"preparação".

Passos

1. Elimine o pacote de software ONTAP anterior:

```
cluster image package delete -version <previous_package_version>
```

2. Faça o download do pacote de software ONTAP de destino:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. Verifique se o pacote de software está disponível no repositório de pacotes de cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. Verifique se o cluster está pronto para ser atualizado:

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Monitorize o progresso da validação:

```
cluster image show-update-progress
```

6. Conclua todas as ações necessárias identificadas pela validação.
7. Opcionalmente, gere uma estimativa de atualização de software:

```
cluster image update -version <package_version_number> -estimate-only
```

A estimativa de atualização de software exibe detalhes sobre cada componente a ser atualizado e a duração estimada da atualização.

8. Execute a atualização de software:

```
cluster image update -version <package_version_number>
```

Se for encontrado um problema, a atualização será interrompida e solicitará que você tome medidas corretivas. Você pode usar o comando show-update-progress da imagem de cluster para exibir detalhes sobre quaisquer problemas e o andamento da atualização. Depois de corrigir o problema, você pode retomar a atualização usando o comando de retomada-atualização da imagem de cluster.

9. Apresentar o progresso da atualização do cluster:

```
cluster image show-update-progress
```

O nó é reinicializado como parte da atualização e não pode ser acessado durante a reinicialização.

10. Acionar uma notificação:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

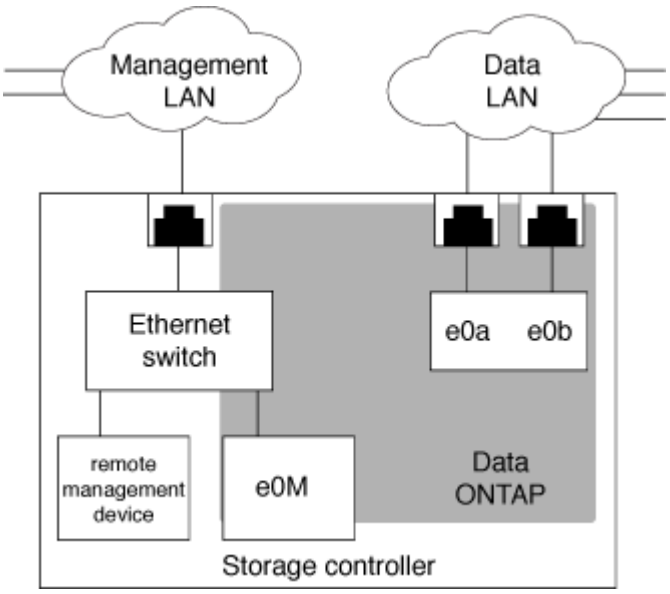
Se o cluster não estiver configurado para enviar mensagens, uma cópia da notificação será salva localmente.

Configure a rede SP/BMC

Isolar o tráfego de rede de gerenciamento

É uma prática recomendada configurar o SP/BMC e a interface de gerenciamento e0M em uma sub-rede dedicada ao tráfego de gerenciamento. A execução do tráfego de dados pela rede de gerenciamento pode causar degradação do desempenho e problemas de roteamento.

A porta Ethernet de gerenciamento na maioria dos controladores de armazenamento (indicada por um ícone de chave na parte traseira do chassi) é conetada a um switch Ethernet interno. O switch interno fornece conetividade ao SP/BMC e à interface de gerenciamento e0M, que você pode usar para acessar o sistema de armazenamento através de protocolos TCP/IP como Telnet, SSH e SNMP.



Se pretende utilizar o dispositivo de gestão remota e o e0M, tem de os configurar na mesma sub-rede IP. Como essas são interfaces de baixa largura de banda, a prática recomendada é configurar SP/BMC e e0M em uma sub-rede dedicada ao tráfego de gerenciamento.

Se não conseguir isolar o tráfego de gestão ou se a sua rede de gestão dedicada for invulgarmente grande, deve tentar manter o volume de tráfego de rede o mais baixo possível. O tráfego de broadcast ou multicast de

entrada excessiva pode degradar o desempenho do SP/BMC.

> Alguns controladores de storage, como o AFF A800, têm duas portas externas, uma para BMC e outra para e0M. Para esses controladores, não há nenhum requisito para configurar BMC e e0M na mesma sub-rede IP.

Considerações para a configuração de rede SP/BMC

Pode ativar a configuração automática de rede no nível do cluster para o SP (recomendado). Você também pode deixar a configuração automática de rede do SP desativada (o padrão) e gerenciar a configuração de rede do SP manualmente no nível do nó. Existem algumas considerações para cada caso.

> Este tópico aplica-se tanto ao SP como ao BMC.

A configuração automática de rede SP permite que o SP use recursos de endereço (incluindo o endereço IP, máscara de sub-rede e endereço de gateway) da sub-rede especificada para configurar sua rede automaticamente. Com a configuração automática de rede SP, não é necessário atribuir manualmente endereços IP para o SP de cada nó. Por padrão, a configuração automática de rede do SP está desativada; isso ocorre porque a ativação da configuração exige que a sub-rede a ser usada para a configuração seja definida primeiro no cluster.

Se você ativar a configuração automática de rede do SP, os seguintes cenários e considerações serão aplicados:

- Se o SP nunca tiver sido configurado, a rede SP é configurada automaticamente com base na sub-rede especificada para a configuração automática de rede SP.
- Se o SP foi configurado manualmente anteriormente ou se a configuração de rede SP existente for baseada em uma sub-rede diferente, a rede SP de todos os nós do cluster será reconfigurada com base na sub-rede especificada na configuração automática de rede SP.

  A reconfiguração pode resultar na atribuição de um endereço diferente ao SP, o que pode ter um impactos na configuração de DNS e na capacidade de resolver nomes de host do SP. Como resultado, você pode precisar atualizar sua configuração de DNS.

- Um nó que se une ao cluster usa a sub-rede especificada para configurar sua rede SP automaticamente.
- O `system service-processor network modify` comando não permite alterar o endereço IP do SP.

  Quando a configuração automática de rede SP está ativada, o comando permite-lhe ativar ou desativar a interface de rede SP.

  - Se a configuração automática de rede do SP tiver sido ativada anteriormente, a desativação da interface de rede do SP resulta na liberação do recurso de endereço atribuído e retornada à sub-rede.
  - Se você desabilitar a interface de rede SP e reativá-la, o SP poderá ser reconfigurado com um endereço diferente.

Se a configuração automática de rede do SP estiver desativada (o padrão), os seguintes cenários e considerações serão aplicados:

- Se o SP nunca tiver sido configurado, a configuração de rede do SP IPv4 é predefinida para utilizar DHCP IPv4 e IPv6 é desativada.

Um nó que une o cluster também usa DHCP IPv4 para sua configuração de rede SP por padrão.

- O `system service-processor network modify` comando permite configurar o endereço IP SP de um nó.

  É apresentada uma mensagem de aviso quando tenta configurar manualmente a rede SP com endereços atribuídos a uma sub-rede. Ignorar o aviso e prosseguir com a atribuição manual de endereços pode resultar em um cenário com endereços duplicados.

Se a configuração automática de rede do SP for desativada depois de ter sido ativada anteriormente, aplicam-se os seguintes cenários e considerações:

- Se a configuração automática de rede do SP tiver a família de endereços IPv4 desativada, a rede SP IPv4 é predefinida para utilizar DHCP e o `system service-processor network modify` comando permite modificar a configuração do SP IPv4 para nós individuais.
- Se a configuração automática de rede do SP tiver a família de endereços IPv6 desativada, a rede do SP IPv6 também será desativada e o `system service-processor network modify` comando permitirá ativar e modificar a configuração do SP IPv6 para nós individuais.

Ative a configuração automática de rede SP/BMC

É preferível ativar o SP para utilizar a configuração automática de rede em vez de configurar manualmente a rede SP. Como a configuração automática de rede do SP é de todo o cluster, você não precisa gerenciar manualmente a rede SP para nós individuais.

Esta tarefa aplica-se tanto ao SP como ao BMC.

- A sub-rede que você deseja usar para a configuração automática de rede SP já deve estar definida no cluster e não deve ter conflitos de recursos com a interface de rede SP.

  O `network subnet show` comando exibe informações de sub-rede para o cluster.

  O parâmetro que força a associação de sub-rede (o `-force-update-lif-associations` parâmetro `network subnet` dos comandos) é suportado apenas em LIFs de rede e não na interface de rede SP.

- Se você quiser usar conexões IPv6 para o SP, o IPv6 já deve estar configurado e habilitado para o ONTAP.

  O `network options ipv6 show` comando exibe o estado atual de IPv6 configurações para ONTAP.

Passos

1. Especifique a família de endereços IPv4 ou IPv6 e o nome da sub-rede que você deseja que o SP use usando o `system service-processor network auto-configuration enable` comando.
2. Apresentar a configuração automática da rede SP utilizando o `system service-processor network auto-configuration show` comando.
3. Se, posteriormente, pretender desativar ou reativar a interface de rede SP IPv4 ou IPv6 para todos os nós que estão em quórum, utilize o `system service-processor network modify` comando com os `-address-family` [`true`|`false`` parâmetros [`IPv4`|`IPv6`] e `-enable`].

   Quando a configuração automática de rede do SP está ativada, não é possível modificar o endereço IP do

SP para um nó que está no quórum. Só pode ativar ou desativar a interface de rede SP IPv4 ou IPv6.

Se um nó estiver fora do quórum, você poderá modificar a configuração de rede SP do nó, incluindo o endereço IP do SP, executando `system service-processor network modify` a partir do nó e confirmando que deseja substituir a configuração automática de rede do SP para o nó. No entanto, quando o nó se junta ao quórum, a reconfiguração automática do SP ocorre para o nó com base na sub-rede especificada.

Configure a rede SP/BMC manualmente

Se não tiver a configuração automática de rede configurada para o SP, tem de configurar manualmente a rede SP de um nó para que o SP possa ser acessível utilizando um endereço IP.

O que você vai precisar

Se você quiser usar conexões IPv6 para o SP, o IPv6 já deve estar configurado e habilitado para o ONTAP. Os `network options ipv6` comandos gerenciam IPv6 configurações para o ONTAP.

Esta tarefa aplica-se tanto ao SP como ao BMC.

Você pode configurar o SP para usar IPv4, IPv6 ou ambos. A configuração do SP IPv4 suporta endereçamento estático e DHCP, e a configuração do SP IPv6 suporta somente endereçamento estático.

Se a configuração automática de rede SP tiver sido configurada, não será necessário configurar manualmente a rede SP para nós individuais e o `system service-processor network modify` comando permite ativar ou desativar apenas a interface de rede SP.

Passos

1. Configure a rede SP para um nó usando o `system service-processor network modify` comando.
   - O `-address-family` parâmetro especifica se a configuração IPv4 ou IPv6 do SP deve ser modificada.
   - O `-enable` parâmetro permite a interface de rede da família de endereços IP especificada.
   - O `-dhcp` parâmetro especifica se deve-se usar a configuração de rede do servidor DHCP ou o endereço de rede fornecido.

     Só pode ativar o DHCP (definindo `-dhcp` para `v4`) se estiver a utilizar o IPv4. Não é possível ativar o DHCP para configurações IPv6.
   - O `-ip-address` parâmetro especifica o endereço IP público para o SP.

     É apresentada uma mensagem de aviso quando tenta configurar manualmente a rede SP com endereços atribuídos a uma sub-rede. Ignorar o aviso e prosseguir com a atribuição de endereço manual pode resultar em uma atribuição de endereço duplicado.
   - O `-netmask` parâmetro especifica a máscara de rede para o SP (se estiver usando IPv4.)
   - O `-prefix-length` parâmetro especifica o tamanho do prefixo da rede da máscara de sub-rede para o SP (se estiver usando IPv6.)
   - O `-gateway` parâmetro especifica o endereço IP do gateway para o SP.

2. Configure a rede SP para os nós restantes no cluster repetindo a etapa 1.
3. Exiba a configuração da rede SP e verifique o status da configuração do SP usando o `system service-processor network show` comando com os `-instance` parâmetros ou `-field setup-status`.

   O status de configuração do SP para um nó pode ser um dos seguintes:

   - `not-setup` — não configurado
   - `succeeded` — Configuração bem-sucedida
   - `in-progress` — Configuração em andamento
   - `failed` — a configuração falhou

Exemplo de configuração da rede SP

O exemplo a seguir configura o SP de um nó para usar o IPv4, ativa o SP e exibe a configuração de rede SP para verificar as configurações:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Modifique a configuração do serviço da API do SP

A API SP é uma API de rede segura que permite que o ONTAP se comunique com o SP pela rede. Você pode alterar a porta usada pelo serviço de API do SP, renovar os certificados que o serviço usa para comunicação interna ou desativar o serviço totalmente. Você precisa modificar a configuração somente em situações raras.

Sobre esta tarefa

- O serviço de API do SP usa a porta `50000` por padrão.

  Você pode alterar o valor da porta se, por exemplo, estiver em uma configuração de rede em que a porta `50000` é usada para comunicação por outro aplicativo de rede ou se quiser diferenciar entre o tráfego de outros aplicativos e o tráfego gerado pelo serviço de API do SP.

- Os certificados SSL e SSH usados pelo serviço API SP são internos ao cluster e não são distribuídos externamente.

  No caso improvável de os certificados estarem comprometidos, você pode renová-los.

- O serviço de API do SP está habilitado por padrão.

  Você só precisa desativar o serviço de API SP em situações raras, como em uma LAN privada onde o SP não esteja configurado ou usado e você deseja desativar o serviço.

  Se o serviço de API do SP estiver desativado, a API não aceita conexões de entrada. Além disso, a funcionalidade, como atualizações de firmware SP baseadas em rede e a coleção de logs do "sistema próprio" do SP baseada em rede, torna-se indisponível. O sistema muda para utilizando a interface de série.

Passos

1. Mude para o nível de privilégio avançado utilizando o `set -privilege advanced` comando.
2. Modifique a configuração do serviço API do SP:

Se você quiser…	Use o seguinte comando…
Altere a porta usada pelo serviço de API do SP	`system service-processor api-service modify` com o `-port` {`49152`.`65535`parâmetro

Se você quiser…	Use o seguinte comando…
Renove os certificados SSL e SSH usados pelo serviço API SP para comunicação interna	• Para ONTAP 9.5 ou posterior utilização `system service-processor api-service renew-internal-certificate` • Para ONTAP 9 .4 e uso anterior • `system service-processor api-service renew-certificates` Se nenhum parâmetro for especificado, somente os certificados de host (incluindo os certificados de cliente e servidor) serão renovados. Se o `-renew-all true` parâmetro for especificado, os certificados de host e o certificado de CA raiz serão renovados.
comm	
Desative ou reative o serviço de API do SP	`system service-processor api-service modify` com o `-is-enabled {true`

3. Exiba a configuração do serviço API SP usando o `system service-processor api-service show` comando.

Gerencie nós remotamente usando o SP/BMC

Gerencie um nó remotamente usando a visão geral do SP/BMC

Você pode gerenciar um nó remotamente usando um controlador integrado, chamado de processador de Serviço (SP) ou controlador de gerenciamento de placa base (BMC). Este controlador de gerenciamento remoto está incluído em todos os modelos de plataforma atuais. O controlador permanece operacional independentemente do estado operacional do nó.

As seguintes plataformas suportam BMC em vez de SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320

- AFF A220
- AFF C190

Sobre o SP

O processador de serviço (SP) é um dispositivo de gerenciamento remoto que permite acessar, monitorar e solucionar problemas remotamente de um nó.

Os principais recursos do SP incluem o seguinte:

- O SP permite que você acesse um nó remotamente para diagnosticar, desligar, desligar ou reinicializar o nó, independentemente do estado do controlador do nó.

  O SP é alimentado por uma tensão de espera, que está disponível desde que o nó tenha energia de entrada de pelo menos uma de suas fontes de alimentação.

  Você pode fazer login no SP usando um aplicativo cliente Shell seguro de um host de administração. Em seguida, você pode usar a CLI do SP para monitorar e solucionar problemas do nó remotamente. Além disso, você pode usar o SP para acessar o console serial e executar comandos ONTAP remotamente.

  Você pode acessar o SP a partir do console serial ou acessar o console serial a partir do SP. O SP permite abrir simultaneamente uma sessão de CLI do SP e uma sessão de console separada.

  Por exemplo, quando um sensor de temperatura se torna criticamente alto ou baixo, o ONTAP aciona o SP para desligar a placa-mãe graciosamente. O console serial fica sem resposta, mas você ainda pode pressionar Ctrl-G no console para acessar a CLI do SP. Em seguida, você pode usar o `system power on` comando ou `system power cycle` do SP para ligar ou desligar o nó.

- O SP monitora sensores ambientais e Registra eventos para ajudá-lo a tomar ações de serviço oportunas e eficazes.

  O SP monitora sensores ambientais, como as temperaturas do nó, tensões, correntes e velocidades do ventilador. Quando um sensor ambiental atinge uma condição anormal, o SP Registra as leituras anormais, notifica o ONTAP do problema e envia alertas e notificações de "sistema próprio" conforme necessário por meio de uma mensagem AutoSupport, independentemente de o nó poder enviar mensagens AutoSupport.

  O SP também Registra eventos como progresso da inicialização, alterações na Unidade substituível em Campo (FRU), eventos gerados pelo ONTAP e histórico de comandos do SP. Você pode invocar manualmente uma mensagem do AutoSupport para incluir os arquivos de log do SP coletados de um nó especificado.

  Além de gerar essas mensagens em nome de um nó inativo e anexar informações de diagnóstico adicionais a mensagens AutoSupport, o SP não tem efeito na funcionalidade AutoSupport. As configurações do AutoSupport e o comportamento do conteúdo da mensagem são herdadas do ONTAP.

  > O SP não depende da `-transport` configuração de parâmetro do `system node autosupport modify` comando para enviar notificações. O SP usa apenas o protocolo SMTP (Simple Mail Transport Protocol) e requer a configuração AutoSupport do host para incluir informações do host de e-mail.

  Se o SNMP estiver ativado, o SP gera traps SNMP para hosts de intercetação configurados para todos os eventos de "sistema próprio".

- O SP tem um buffer de memória não volátil que armazena até 4.000 eventos em um log de eventos do sistema (SEL) para ajudá-lo a diagnosticar problemas.

  O SEL armazena cada entrada de log de auditoria como um evento de auditoria. Ele é armazenado na memória flash integrada no SP. A lista de eventos do SEL é enviada automaticamente pelo SP para destinatários especificados por meio de uma mensagem do AutoSupport.

  O SEL contém as seguintes informações:

  - Eventos de hardware detetados pelo SP - por exemplo, status do sensor sobre fontes de alimentação, tensão ou outros componentes
  - Erros detetados pelo SP—por exemplo, um erro de comunicação, uma falha de ventilador ou um erro de memória ou CPU
  - Eventos críticos de software enviados para o SP pelo nó - por exemplo, um pânico, uma falha de comunicação, uma falha de inicialização ou um "sistema próprio" acionado pelo usuário como resultado da emissão do SP `system reset` ou `system power cycle` comando
- O SP monitora o console serial, independentemente de os administradores estarem conetados ou conetados ao console.

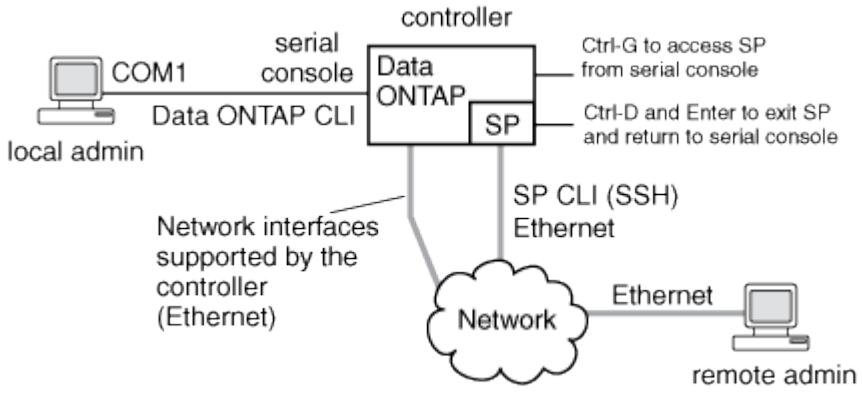
  Quando as mensagens são enviadas para o console, o SP as armazena no log do console. O log do console persiste enquanto o SP tiver energia de qualquer uma das fontes de alimentação do nó. Como o SP funciona com energia em espera, ele permanece disponível mesmo quando o nó é ligado ou desligado.

- A aquisição assistida por hardware está disponível se o SP estiver configurado.
- O serviço API SP permite que o ONTAP se comunique com o SP pela rede.

  O serviço aprimora o gerenciamento do ONTAP do SP, oferecendo suporte a funcionalidades baseadas em rede, como o uso da interface de rede para a atualização de firmware do SP, permitindo que um nó acesse a funcionalidade do SP ou o console do sistema de outro nó e faça o upload do log do SP de outro nó.

  Você pode modificar a configuração do serviço API SP alterando a porta que o serviço usa, renovando os certificados SSL e SSH que são usados pelo serviço para comunicação interna ou desativando o serviço completamente.

O diagrama a seguir ilustra o acesso ao ONTAP e ao SP de um nó. A interface SP é acessada através da porta Ethernet (indicada por um ícone de chave na parte traseira do chassi):



O que o Baseboard Management Controller faz

A partir do ONTAP 9.1, em determinadas plataformas de hardware, o software é personalizado para suportar um novo controlador integrado chamado controlador de gerenciamento de placa base (BMC). O BMC tem comandos de interface de linha de comando (CLI) que você pode usar para gerenciar o dispositivo remotamente.

O BMC funciona de forma semelhante ao processador de Serviço (SP) e usa muitos dos mesmos comandos. O BMC permite que você faça o seguinte:

- Configure as definições de rede BMC.
- Acesse um nó remotamente e execute tarefas de gerenciamento de nós, como diagnosticar, desligar, desligar e reiniciar o nó.

Existem algumas diferenças entre o SP e o BMC:

- O BMC controla completamente a monitorização ambiental dos elementos de alimentação, dos elementos de refrigeração, dos sensores de temperatura, dos sensores de tensão e dos sensores de corrente. O BMC comunica as informações do sensor ao ONTAP através do IPMI.
- Alguns dos comandos de alta disponibilidade (HA) e armazenamento são diferentes.
- O BMC não envia mensagens AutoSupport.

Atualizações automáticas de firmware também estão disponíveis ao executar o ONTAP 9.2 GA ou posterior com os seguintes requisitos:

- A revisão 1,15 ou posterior do firmware do BMC deve ser instalada.

  É necessária uma atualização manual para atualizar o firmware do BMC de 1,12 para 1,15 ou posterior.

- O BMC reinicia automaticamente após a conclusão de uma atualização de firmware.

  As operações do nó não são afetadas durante uma reinicialização do BMC.

Métodos de gerenciamento de atualizações de firmware do SP/BMC

O ONTAP inclui uma imagem de firmware do SP que é chamada de *imagem de linha de base*. Se uma nova versão do firmware do SP ficar disponível posteriormente, você tem a opção de baixá-lo e atualizar o firmware do SP para a versão baixada sem atualizar a versão do ONTAP.

Este tópico aplica-se tanto ao SP como ao BMC.

O ONTAP oferece os seguintes métodos para gerenciar atualizações de firmware do SP:

- A funcionalidade de atualização automática do SP está ativada por predefinição, permitindo que o firmware do SP seja atualizado automaticamente nos seguintes cenários:
  - Quando você atualiza para uma nova versão do ONTAP

O processo de atualização do ONTAP inclui automaticamente a atualização do firmware do SP, desde que a versão do firmware do SP fornecida com o ONTAP seja mais recente do que a versão do SP executada no nó.

> O ONTAP deteta uma atualização automática do SP com falha e aciona uma ação corretiva para tentar novamente a atualização automática do SP até três vezes. Se todas as três tentativas falharem, consulte o link do artigo da base de dados de Conhecimento: https://kb.NetApp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_os/Health_Monitor_SPAutoUpgradeFailedMajorAlert__SP AutoSupport_upgrade_Fails_-_AutoSupport_Message[Health Monitor SPAutoUpgradeFailed SP upgrade_Message].

- Quando você faz o download de uma versão do firmware do SP a partir do site de suporte da NetApp e a versão baixada é mais recente do que a versão que o SP está atualmente em execução
- Quando você faz o downgrade ou reverte para uma versão anterior do ONTAP

  O firmware do SP é atualizado automaticamente para a versão compatível mais recente que é suportada pela versão do ONTAP para a qual você reverteu ou baixou. Não é necessária uma atualização manual do firmware do SP.

Você tem a opção de desativar a funcionalidade de atualização automática do SP usando o `system service-processor image modify` comando. No entanto, é recomendável que você deixe a funcionalidade ativada. Desativar a funcionalidade pode resultar em combinações subótimas ou não qualificadas entre a imagem ONTAP e a imagem de firmware SP.

- O ONTAP permite acionar manualmente uma atualização do SP e especificar como a atualização deve ocorrer usando o `system service-processor image update` comando.

  Você pode especificar as seguintes opções:

  - O pacote de firmware do SP a utilizar (`-package`)

    Você pode atualizar o firmware do SP para um pacote baixado especificando o nome do arquivo do pacote. O comando ADVANCE `system image package show` exibe todos os arquivos de pacote (incluindo os arquivos do pacote de firmware do SP) que estão disponíveis em um nó.

  - Se deve usar o pacote de firmware SP de linha de base para a atualização do SP (`-baseline`)

    Você pode atualizar o firmware do SP para a versão de linha de base fornecida com a versão atual do ONTAP.

  > Se utilizar algumas das opções ou parâmetros de atualização mais avançados, as definições de configuração do BMC poderão ser temporariamente eliminadas. Após a reinicialização, o ONTAP pode levar até 10 minutos para restaurar a configuração do BMC.

- O ONTAP permite exibir o status da atualização de firmware SP mais recente acionada pelo ONTAP usando o `system service-processor image update-progress show` comando.

Qualquer ligação existente ao SP é terminada quando o firmware do SP está a ser atualizado. Este é o caso se a atualização do firmware do SP é acionada automaticamente ou manualmente.

Informações relacionadas

"Downloads do NetApp: Firmware e Diagnóstico do sistema"

Quando o SP/BMC utiliza a interface de rede para atualizações de firmware

Uma atualização de firmware do SP que é acionada a partir do ONTAP com o SP executando a versão 1,5, 2,5, 3,1 ou posterior suporta o uso de um mecanismo de transferência de arquivos baseado em IP através da interface de rede SP.

Este tópico aplica-se tanto ao SP como ao BMC.

Uma atualização de firmware do SP através da interface de rede é mais rápida do que uma atualização através da interface serial. Ele reduz a janela de manutenção durante a qual o firmware do SP está sendo atualizado e também não causa interrupções na operação do ONTAP. As versões do SP que suportam esse recurso estão incluídas no ONTAP. Eles também estão disponíveis no site de suporte da NetApp e podem ser instalados em controladores que executam uma versão compatível do ONTAP.

Quando você estiver executando o SP versão 1,5, 2,5, 3,1 ou posterior, os seguintes comportamentos de atualização de firmware se aplicam:

- Uma atualização de firmware do SP que é *automaticamente* acionada pelo ONTAP usa a interface de rede para a atualização; no entanto, a atualização automática do SP muda para usar a interface serial para a atualização de firmware se ocorrer uma das seguintes condições:
  - A interface de rede SP não está configurada ou não está disponível.
  - A transferência de arquivos baseada em IP falha.
  - O serviço de API do SP está desativado.

Independentemente da versão do SP que você está executando, uma atualização de firmware do SP acionada a partir da CLI do SP sempre usa a interface de rede do SP para a atualização.

Informações relacionadas

"Downloads do NetApp: Firmware e Diagnóstico do sistema"

Contas que podem acessar o SP

Ao tentar acessar o SP, você será solicitado a fornecer credenciais. As contas de usuários de cluster criadas com o `service-processor` tipo de aplicativo têm acesso à CLI do SP em qualquer nó do cluster. As contas de usuário do SP são gerenciadas a partir do ONTAP e autenticadas por senha. A partir do ONTAP 9.9,1, as contas de usuário do SP devem ter a `admin` função.

As contas de usuário para acessar o SP são gerenciadas a partir do ONTAP em vez da CLI do SP. Uma conta de usuário de cluster pode acessar o SP se ele for criado com o `-application` parâmetro do `security login create` comando definido como `service-processor` e o `-authmethod` parâmetro definido como `password`. O SP suporta apenas autenticação por palavra-passe.

Você deve especificar o `-role` parâmetro ao criar uma conta de usuário do SP.

- No ONTAP 9.9,1 e versões posteriores, você deve especificar `admin` para o `-role` parâmetro, e quaisquer modificações em uma conta exigem a `admin` função. Outras funções não são mais permitidas por motivos de segurança.
  - Se você estiver atualizando para o ONTAP 9.9,1 ou versões posteriores, "Alteração nas contas de usuário que podem acessar o processador de serviço"consulte .

    - Se você estiver revertendo para o ONTAP 9.8 ou versões anteriores, "Verifique as contas de usuário que podem acessar o processador de serviço"consulte .
- No ONTAP 9.8 e versões anteriores, qualquer função pode acessar o SP, mas `admin` é recomendado.

Por padrão, a conta de usuário do cluster chamada "admin" inclui o `service-processor` tipo de aplicativo e tem acesso ao SP.

O ONTAP impede que você crie contas de usuário com nomes que são reservados para o sistema (como "root" e "naroot"). Não é possível usar um nome reservado ao sistema para acessar o cluster ou o SP.

Você pode exibir as contas de usuário atuais do SP usando o `-application service-processor` parâmetro `security login show` do comando.

Acesse o SP/BMC de um host de administração

Você pode fazer login no SP de um nó de um host de administração para executar tarefas de gerenciamento de nós remotamente.

O que você vai precisar

Devem ser cumpridas as seguintes condições:

- O host de administração que você usa para acessar o SP deve oferecer suporte a SSHv2.
- Sua conta de usuário já deve estar configurada para acessar o SP.

  Para acessar o SP, sua conta de usuário deve ter sido criada com o `-application` parâmetro do `security login create` comando definido como `service-processor` e o `-authmethod` parâmetro definido como `password`.

Esta tarefa aplica-se tanto ao SP como ao BMC.

Se o SP estiver configurado para usar um endereço IPv4 ou IPv6 e se cinco tentativas de login SSH de um host falharem consecutivamente em 10 minutos, o SP rejeita solicitações de login SSH e suspende a comunicação com o endereço IP do host por 15 minutos. A comunicação é retomada após 15 minutos e você pode tentar fazer login no SP novamente.

O ONTAP impede que você crie ou use nomes reservados ao sistema (como "root" e "naroot") para acessar o cluster ou o SP.

Passos

1. No host de administração, faça login no SP:

   `ssh username@SP_IP_address`

2. Quando lhe for solicitado, introduza a palavra-passe `username` do .

   O prompt SP é exibido, indicando que você tem acesso à CLI do SP.

Exemplos de acesso à SP de um host de administração

O exemplo a seguir mostra como fazer login no SP com uma conta de usuário `joe` , que foi configurada para acessar o SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Os exemplos a seguir mostram como usar o endereço global IPv6 ou o endereço anunciado pelo roteador IPv6 para fazer login no SP em um nó que tenha SSH configurado para IPv6 e o SP configurado para IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Aceda ao SP/BMC a partir da consola do sistema

Você pode acessar o SP a partir do console do sistema (também chamado de *console serial*) para executar tarefas de monitoramento ou solução de problemas.

Sobre esta tarefa

Esta tarefa aplica-se tanto ao SP como ao BMC.

Passos

1. Acesse a CLI do SP a partir do console do sistema pressionando Ctrl-G no prompt.
2. Faça login na CLI do SP quando for solicitado.

   O prompt SP é exibido, indicando que você tem acesso à CLI do SP.

3. Saia da CLI do SP e retorne ao console do sistema pressionando Ctrl-D e pressione Enter.

Exemplo de acesso à CLI do SP a partir do console do sistema

O exemplo a seguir mostra o resultado de pressionar Ctrl-G do console do sistema para acessar a CLI do SP. O `help system power` comando é inserido no prompt do SP, seguido de Ctrl-D e Enter para retornar ao console do sistema.

```
cluster1::>
```

(Pressione Ctrl-G para acessar a CLI do SP.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Pressione Ctrl-D e Enter para retornar ao console do sistema.)

```
cluster1::>
```

Relação entre as sessões de CLI, console SP e console do sistema do SP

Você pode abrir uma sessão de CLI do SP para gerenciar um nó remotamente e abrir uma sessão de console SP separada para acessar o console do nó. A sessão do console SP espelha a saída exibida em uma sessão de console de sistema concorrente. O SP e o console do sistema têm ambientes de shell independentes com autenticação de login independente.

Entender como as sessões de CLI, console SP e console do sistema do SP estão relacionadas ajuda a gerenciar um nó remotamente. O seguinte descreve a relação entre as sessões:

- Somente um administrador pode fazer login na sessão da CLI do SP de cada vez. No entanto, o SP permite que você abra simultaneamente uma sessão da CLI do SP e uma sessão separada do console do SP.

  A CLI do SP é indicada com o prompt SP (`SP>`). A partir de uma sessão CLI do SP, você pode usar o comando SP `system console` para iniciar uma sessão de console do SP. Ao mesmo tempo, você pode iniciar uma sessão de CLI do SP separada por meio de SSH. Se você pressionar Ctrl-D para sair da sessão do console do SP, você retornará automaticamente à sessão da CLI do SP. Se uma sessão da CLI do SP já existir, uma mensagem pergunta se você deseja encerrar a sessão existente da CLI do SP. Se você digitar "'y'", a sessão CLI do SP existente será encerrada, permitindo que você retorne do console do SP para a CLI do SP. Esta ação é gravada no registo de eventos do SP.

  Em uma sessão da CLI do ONTAP conetada por meio de SSH, você pode alternar para o console do sistema de um nó executando o comando ONTAP `system node run-console` de outro nó.

- Por motivos de segurança, a sessão CLI do SP e a sessão do console do sistema têm autenticação de login independente.

  Quando você inicia uma sessão de console do SP a partir da CLI do SP (usando o comando SP `system console`), você será solicitado a fornecer a credencial do console do sistema. Ao acessar a CLI do SP a partir de uma sessão de console do sistema (pressionando Ctrl-G), você será solicitado a fornecer a credencial da CLI do SP.

- A sessão do console SP e a sessão do console do sistema têm ambientes de shell independentes.

  A sessão do console SP espelha a saída que é exibida em uma sessão de console de sistema concorrente. No entanto, a sessão simultânea do console do sistema não espelha a sessão do console do SP.

  A sessão do console SP não espelha a saída de sessões SSH simultâneas.

Gerencie os endereços IP que podem acessar o SP

Por padrão, o SP aceita solicitações de conexão SSH de hosts de administração de qualquer endereço IP. Você pode configurar o SP para aceitar solicitações de conexão SSH apenas dos hosts de administração que têm os endereços IP especificados. As alterações feitas se aplicam ao acesso SSH ao SP de qualquer nó no cluster.

Passos

1. Conceda acesso SP apenas aos endereços IP especificados usando o `system service-processor ssh add-allowed-addresses` comando com o `-allowed-addresses` parâmetro.
   - O valor do `-allowed-addresses` parâmetro deve ser especificado no formato de `address /netmask`, e vários `address/netmask` pares devem ser separados por vírgulas, por exemplo, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Definir o `-allowed-addresses` parâmetro para `0.0.0.0/0, ::/0` permite que todos os endereços IP acessem o SP (o padrão).
   - Quando você altera o padrão limitando o acesso à SP apenas aos endereços IP especificados, o ONTAP solicita que você confirme que deseja que os endereços IP especificados substituam a configuração padrão ""permitir tudo"" (`0.0.0.0/0, ::/0`).
   - O `system service-processor ssh show` comando exibe os endereços IP que podem acessar o SP.
2. Se você quiser impedir que um endereço IP especificado acesse o SP, use o `system service-processor ssh remove-allowed-addresses` comando com o `-allowed-addresses` parâmetro.

   Se você bloquear todos os endereços IP de acessar o SP, o SP se tornará inacessível de qualquer host de administração.

Exemplos de gerenciamento de endereços IP que podem acessar o SP

Os exemplos a seguir mostram a configuração padrão para o acesso SSH ao SP, altere o padrão limitando o acesso SP apenas aos endereços IP especificados, remova os endereços IP especificados da lista de acesso e, em seguida, restaure o acesso SP para todos os endereços IP:

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

Use a ajuda on-line na CLI do SP/BMC

A ajuda on-line exibe os comandos e opções da CLI do SP/BMC.

Sobre esta tarefa

Esta tarefa aplica-se tanto ao SP como ao BMC.

Passos

1. Para exibir informações de ajuda para os comandos SP/BMC, digite o seguinte:

Para acessar a ajuda do SP…	Para acessar a ajuda do BMC…
Digite `help` no prompt SP.	Digite `system` no prompt BMC.

O exemplo a seguir mostra a ajuda online da CLI do SP.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

O exemplo a seguir mostra a ajuda online da CLI do BMC.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Para exibir informações de ajuda para a opção de um comando SP/BMC, digite `help` antes ou depois do comando SP/BMC.

   O exemplo a seguir mostra a ajuda online da CLI do SP para o comando SP `events`.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

O exemplo a seguir mostra a ajuda online da CLI do BMC para o comando BMC `system power`.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

Comandos para gerenciar um nó remotamente

Você pode gerenciar um nó remotamente acessando o SP e executando os comandos da CLI do SP para executar tarefas de gerenciamento de nós. Para várias tarefas de gerenciamento remoto de nós comumente executadas, você também pode usar comandos ONTAP de outro nó no cluster. Alguns comandos do SP são específicos da plataforma e podem não estar disponíveis na sua plataforma.

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
Exiba os comandos SP disponíveis ou subcomandos de um comando SP especificado	`help` [`command`]		
Exibir o nível de privilégio atual para a CLI do SP	`priv show`		
Defina o nível de privilégio para acessar o modo especificado para a CLI do SP	`priv set` {`admin`	`advanced`	`diag`
		Apresentar a data e a hora do sistema	`date`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
	`date`	Exibir eventos registrados pelo SP	`events {all`
`info newest number`	`oldest number`		`search keyword`
		Exibir informações de status do SP e configuração da rede	`sp status[-v -d`
] A `-v` opção exibe estatísticas do SP em forma verbose. A `-d` opção adiciona o log de depuração do SP à tela.	`bmc status[-v -d`	] A `-v` opção exibe estatísticas do SP em forma verbose. A `-d` opção adiciona o log de depuração do SP à tela.	`system service-processor show`
Apresentar o período de tempo em que o SP esteve ativo e o número médio de trabalhos na fila de execução nos últimos 1, 5 e 15 minutos	`sp uptime`	`bmc uptime`	
Exiba os logs do console do sistema	`system log`		
Exiba os arquivos de log do SP ou os arquivos em um arquivo	`sp log history show[ -archive {latest {all` Selecionar		`archive-name] [-dump {all`
`file-name`	`bmc log history show[-archive {latest {all` Selecionar		`archive-name] [-dump {all`
`file-name`		Apresentar o estado de alimentação do controlador de um nó	`system power status`
	`system node power show`	Apresentar informações sobre a bateria	`system battery show`
		Apresentar informações ACP ou o estado dos sensores expansores	`system acp[show sensors show`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
]			Listar todas as FRUs do sistema e suas IDs
`system fru list`			Exibir informações do produto para a FRU especificada
`system fru show fru_id`			Apresentar o registo do histórico de dados da FRU
`system fru log show` (nível de privilégio avançado)			Apresentar o estado dos sensores ambientais, incluindo os respetivos estados e valores atuais
`system sensors` ou `system sensors show`		`system node environment sensors show`	Apresentar o estado e os detalhes do sensor especificado
`system sensors get sensor_name` Pode obter `sensor_name` utilizando o `system sensors` comando ou `system sensors show`.			Exiba as informações da versão do firmware do SP
`version`		`system service-processor image show`	Exiba o histórico de comandos do SP
`sp log audit` (nível de privilégio avançado)	`bmc log audit`		Exiba as informações de depuração do SP
`sp log debug` (nível de privilégio avançado)	`bmc log debug` (nível de privilégio avançado)		Exiba o arquivo de mensagens do SP

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
`sp log messages` (nível de privilégio avançado)	`bmc log messages` (nível de privilégio avançado)		Apresentar as definições de recolha forense do sistema num evento de reposição do watchdog, apresentar as informações forenses do sistema recolhidas durante um evento de reposição do watchdog ou limpar as informações forenses do sistema recolhidas
`system forensics` [`show log dump`		`log clear`]	
	Inicie sessão na consola do sistema	`system console`	
`system node run-console`	Você deve pressionar Ctrl-D para sair da sessão do console do sistema.	Ligue ou desligue o nó ou execute um ciclo de alimentação (desligando e voltando a ligar)	`system power on`
	`system node power on` (nível de privilégio avançado)	`system power off`	
	`system power cycle`		

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
A alimentação em espera permanece ligada para manter o SP em funcionamento sem interrupção. Durante o ciclo de alimentação, ocorre uma breve pausa antes de ligar novamente a alimentação. Usar esses comandos para desligar ou desligar o nó pode causar um desligamento inadequado do nó (também chamado de *desligamento anormal*) e não substitui um desligamento gracioso usando o comando ONTAP `system node halt`.	Crie um despejo de núcleo e redefina o nó	`system core [-f]` A `-f` opção força a criação de um despejo de núcleo e a redefinição do nó.	

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
`system node coredump trigger` (nível de privilégio avançado)	Esses comandos têm o mesmo efeito que pressionar o botão de interrupção não masável (NMI) em um nó, causando um desligamento sujo do nó e forçando um despejo dos arquivos centrais ao interromper o nó. Esses comandos são úteis quando o ONTAP no nó é suspenso ou não responde a comandos como `system node shutdown` . Os arquivos de despejo de núcleo gerados são exibidos na saída do `system node coredump show` comando. O SP permanece operacional desde que a energia de entrada para o nó não seja interrompida.	Reinicie o nó com uma imagem de firmware do BIOS especificada opcionalmente (primária, backup ou atual) para se recuperar de problemas como uma imagem corrompida do dispositivo de inicialização do nó	`system reset {primary`
`backup`	`current`		`system node reset` com o `-firmware {primary` `backup`parâmetro
		`current` (nível de privilégio avançado) `system node reset`	Esta operação causa um desligamento anormal do nó. Se nenhuma imagem de firmware do BIOS for especificada, a imagem atual será usada para a reinicialização. O SP permanece operacional desde que a energia de entrada para o nó não seja interrompida.

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
Apresentar o estado da atualização automática do firmware da bateria ou ativar ou desativar a atualização automática do firmware da bateria na próxima inicialização do SP	`system battery auto_update`[`status enable`		`disable`] (nível de privilégio avançado)
		Compare a imagem atual do firmware da bateria com uma imagem de firmware especificada	`system battery verify` [`image_URL`] (nível de privilégio avançado) Se `image_URL` não for especificado, a imagem padrão do firmware da bateria será usada para comparação.
		Atualize o firmware da bateria a partir da imagem no local especificado	`system battery flash image_URL` (nível de privilégio avançado) Use este comando se o processo de atualização automática do firmware da bateria tiver falhado por algum motivo.
		Atualize o firmware do SP utilizando a imagem no local especificado	`sp update image_URL` `image_URL` não deve exceder 200 carateres.
`bmc update image_URL` `image_URL` não deve exceder 200 carateres.	`system service-processor image update`	Reinicie o SP	`sp reboot`

Se você quiser…	Use este comando SP…	Use este comando BMC…	Ou este comando ONTAP …
	`system service-processor reboot-sp`	Apague o conteúdo flash do NVRAM	`system nvram flash clear` (nível de privilégio avançado) Este comando não pode ser iniciado quando a alimentação do controlador está desligada (`system power off`).
		Saia da CLI do SP	`exit`

Sobre as leituras do sensor SP baseado no limiar e os valores de estado da saída do comando dos sensores do sistema

Os sensores baseados em limites fazem leituras periódicas de uma variedade de componentes do sistema. O SP compara a leitura de um sensor baseado em limites com os limites predefinidos que definem as condições de funcionamento aceitáveis de um componente.

Com base na leitura do sensor, o SP apresenta o estado do sensor para o ajudar a monitorizar a condição do componente.

Exemplos de sensores baseados em limites incluem sensores para as temperaturas do sistema, tensões, correntes e velocidades do ventilador. A lista específica de sensores baseados em limites depende da plataforma.

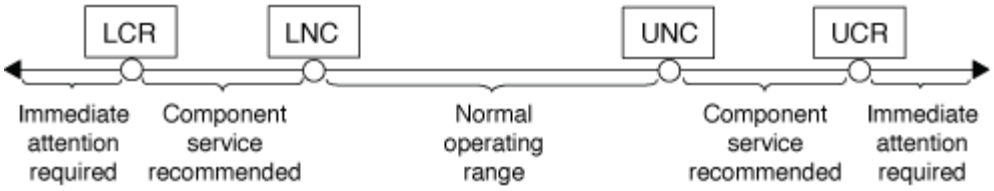
Os sensores baseados em limites têm os seguintes limites, exibidos na saída do comando SP `system sensors`:

- Crítico inferior (LCR)
- Não crítico inferior (LNC)
- Não crítico superior (UNC)
- Crítica superior (UCR)

Uma leitura do sensor entre LNC e LCR ou entre UNC e UCR significa que o componente está mostrando sinais de um problema e uma falha do sistema pode ocorrer como resultado. Portanto, você deve Planejar o serviço de componentes em breve.

Uma leitura do sensor abaixo de LCR ou acima de UCR significa que o componente está avariado e está prestes a ocorrer uma falha do sistema. Portanto, o componente requer atenção imediata.

O diagrama a seguir ilustra os intervalos de gravidade especificados pelos limites:



Você pode encontrar a leitura de um sensor baseado em limiar sob a `Current` coluna na `system sensors` saída do comando. O `system sensors get sensor_name` comando exibe detalhes adicionais para o sensor especificado. À medida que a leitura de um sensor baseado em limites cruza os limites não críticos e críticos, o sensor relata um problema de gravidade crescente. Quando a leitura excede um limite, o status do sensor na `system sensors` saída do comando muda de `ok` para `nc` (não crítico) ou `cr` (crítico) dependendo do limite excedido, e uma mensagem de evento é registrada no log de eventos SEL.

Alguns sensores baseados em limites não têm todos os quatro níveis de limiar. Para esses sensores, os limites em falta mostram `na` como seus limites na `system sensors` saída de comando, indicando que o sensor em particular não tem limite ou problema de gravidade para o determinado limite e o SP não monitora o sensor para esse limite.

Exemplo de saída de comando dos sensores do sistema

O exemplo a seguir mostra algumas das informações exibidas pelo `system sensors` comando na CLI do SP:

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR       | LNC
| UNC       | UCR
-----------------+------------+------------+-------+-----------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000     | 10.000
| 42.000    | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000     | 10.000
| 59.000    | 68.000
CPU1_Error       | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na        | na
| na        | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048
| 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844
| 1.348     | 1.368
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116
| 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465
| 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707
| 1.892     | 1.911
…
```

Exemplo de saída do comando sensor_NAME dos sensores do sistema para um sensor baseado em limiar

O exemplo a seguir mostra o resultado da entrada `system sensors get sensor_name` na CLI do SP para o sensor 5V baseado em limiar:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID              : 5V (0x13)
 Entity ID             : 7.97
 Sensor Type (Analog)  : Voltage
 Sensor Reading        : 5.002 (+/- 0) Volts
 Status                : ok
 Lower Non-Recoverable : na
 Lower Critical        : 4.246
 Lower Non-Critical    : 4.490
 Upper Non-Critical    : 5.490
 Upper Critical        : 5.758
 Upper Non-Recoverable : na
 Assertion Events      :
 Assertions Enabled    : lnc- lcr- ucr+
 Deassertions Enabled  : lnc- lcr- ucr+
```

Acerca dos valores de estado do sensor SP discreto da saída do comando dos sensores do sistema

Os sensores discretos não têm limites. Suas leituras, exibidas sob a `Current` coluna na saída do comando SP CLI `system sensors`, não carregam significados reais e, portanto, são ignoradas pelo SP. A `Status` coluna na `system sensors` saída do comando exibe os valores de status de sensores discretos em formato hexadecimal.

Exemplos de sensores discretos incluem sensores para a ventoinha, falha da unidade de fonte de alimentação (PSU) e falha do sistema. A lista específica de sensores discretos depende da plataforma.

Você pode usar o comando SP CLI `system sensors get sensor_name` para ajudar na interpretação dos valores de status para a maioria dos sensores discretos. Os exemplos a seguir mostram os resultados da entrada `system sensors get sensor_name` para os sensores discretos CPU0_Error e IO_SLOT1_present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                         [Device Present]
```

Embora o `system sensors get sensor_name` comando exiba as informações de status para a maioria dos sensores discretos, ele não fornece informações de status para os sensores discretos System_FW_Status, System_Watchdog, PSU1_Input_Type e PSU2_Input_Type. Pode utilizar as seguintes informações para interpretar os valores de estado destes sensores.

System_FW_Status

A condição do sensor System_FW_Status aparece na forma `0xAABB` de . Pode combinar as informações de `AA` e `BB` para determinar o estado do sensor.

`AA` pode ter um dos seguintes valores:

Valores	Estado do sensor
01	Erro de firmware do sistema
02	Firmware do sistema suspenso
04	Progresso do firmware do sistema

`BB` pode ter um dos seguintes valores:

Valores	Estado do sensor
00	O software do sistema foi desligado corretamente
01	Inicialização da memória em curso
02	Inicialização do NVMEM em curso (quando o NVMEM está presente)
04	Restauração dos valores do hub do controlador de memória (MCH) (quando o NVMEM está presente)
05	O utilizador introduziu a Configuração
13	Inicializando o sistema operacional ou Loader

Valores	Estado do sensor
1F	O BIOS está a ser iniciado
20	O Loader está em execução
21	O Loader está programando o firmware principal do BIOS. Não deve desligar o sistema.
22	O Loader está programando o firmware alternativo do BIOS. Não deve desligar o sistema.
2F	O ONTAP está em execução
60	O SP desligou o sistema
61	O SP ligou o sistema
62	O SP redefiniu o sistema
63	Ciclo de alimentação do SP watchdog
64	Reinicialização a frio do SP watchdog

Por exemplo, o estado 0x042F do sensor System_FW_Status significa "progresso do firmware do sistema (04), ONTAP está em execução (2F)".

System_Watchdog

O sensor System_Watchdog pode ter uma das seguintes condições:

- **0x0080**

  O estado deste sensor não mudou

Valores	Estado do sensor
0x0081	Interrupção do temporizador
0x0180	O temporizador expirou
0x0280	Reinicialização total
0x0480	Desligar
0x0880	Ciclo de alimentação

Por exemplo, o estado 0x0880 do sensor System_Watchdog significa que ocorre um tempo limite de monitorização e provoca um ciclo de alimentação do sistema.

PSU1_Input_Type e PSU2_Input_Type

Para fontes de alimentação de corrente contínua (DC), os sensores PSU1_Input_Type e PSU2_Input_Type não se aplicam. Para fontes de alimentação de corrente alternada (AC), o estado dos sensores pode ter um dos seguintes valores:

Valores	Estado do sensor
0x01 xx	220V tipo de PSU
0x02 xx	110V tipo de PSU

Por exemplo, o estado 0x0280 do sensor PSU1_Input_Type significa que o sensor informa que o tipo de PSU é 110V.

Comandos para gerenciar o SP a partir do ONTAP

O ONTAP fornece comandos para gerenciar o SP, incluindo a configuração de rede SP, a imagem de firmware do SP, o acesso SSH ao SP e a administração geral do SP.

Comandos para gerenciar a configuração de rede SP

Se você quiser…	Execute este comando ONTAP…
Ative a configuração automática de rede SP para o SP usar a família de endereços IPv4 ou IPv6 da sub-rede especificada	`system service-processor network auto-configuration enable`
Desative a configuração automática de rede SP para a família de endereços IPv4 ou IPv6 da sub-rede especificada para o SP	`system service-processor network auto-configuration disable`
Apresentar a configuração automática da rede SP	`system service-processor network auto-configuration show`

Se você quiser…	Execute este comando ONTAP…
Configure manualmente a rede SP para um nó, incluindo o seguinte: • A família de endereços IP (IPv4 ou IPv6) • Se a interface de rede da família de endereços IP especificada deve ser ativada • Se estiver a utilizar IPv4, utilize a configuração de rede a partir do servidor DHCP ou o endereço de rede especificado • O endereço IP público do SP • A máscara de rede para o SP (se utilizar IPv4) • O tamanho do prefixo da rede da máscara de sub-rede para o SP (se estiver usando IPv6) • O endereço IP do gateway para o SP	`system service-processor network modify`
Exiba a configuração de rede SP, incluindo o seguinte: • A família de endereços configurada (IPv4 ou IPv6) e se está ativada • O tipo de dispositivo de gerenciamento remoto • O estado atual do SP e o estado da ligação • Configuração de rede, como endereço IP, endereço MAC, máscara de rede, tamanho do prefixo da máscara de sub-rede, endereço IP atribuído pelo roteador, endereço IP local do link e endereço IP do gateway • A hora em que o SP foi atualizado pela última vez • O nome da sub-rede utilizada para a configuração automática do SP • Se o endereço IP atribuído ao router IPv6 está ativado • Estado da configuração da rede SP • Motivo da falha de configuração da rede SP	`system service-processor network show` A exibição de detalhes completos da rede SP requer o `-instance` parâmetro.
Modifique a configuração do serviço API do SP, incluindo o seguinte: • Alterar a porta usada pelo serviço de API do SP • Ativar ou desativar o serviço de API SP	`system service-processor api-service modify` (nível de privilégio avançado)

Se você quiser…	Execute este comando ONTAP…
Exibir a configuração do serviço da API do SP	`system service-processor api-service show` (nível de privilégio avançado)
Renove os certificados SSL e SSH usados pelo serviço API SP para comunicação interna	• Para o ONTAP 9.5 ou posterior: `system service-processor api-service renew-internal-certificates` • Para o ONTAP 9.4 ou anterior: `system service-processor api-service renew-certificates` (nível de privilégio avançado)

Comandos para gerenciar a imagem de firmware do SP

Se você quiser…	Execute este comando ONTAP…
Exiba os detalhes da imagem de firmware do SP atualmente instalada, incluindo o seguinte: • O tipo de dispositivo de gerenciamento remoto • A imagem (principal ou backup) da qual o SP é inicializado, seu status e versão do firmware • Se a atualização automática do firmware está ativada e o estado da última atualização	`system service-processor image show` O `-is-current` parâmetro indica a imagem (primária ou de cópia de segurança) da qual o SP está atualmente inicializado, não se a versão do firmware instalada for a mais atual.
Ative ou desative a atualização automática de firmware do SP	`system service-processor image modify` Por padrão, o firmware do SP é atualizado automaticamente com a atualização do ONTAP ou quando uma nova versão do firmware do SP é baixada manualmente. Desativar a atualização automática não é recomendado porque isso pode resultar em combinações subótimas ou não qualificadas entre a imagem ONTAP e a imagem de firmware SP.

Se você quiser…	Execute este comando ONTAP…
Transfira manualmente uma imagem de firmware SP num nó	`system node image get` Antes de executar os `system node image` comandos, você deve definir o nível de privilégio como avançado (`set -privilege advanced`), inserindo **y** quando solicitado a continuar. A imagem de firmware do SP é fornecida com o ONTAP. Não é necessário baixar o firmware do SP manualmente, a menos que você queira usar uma versão de firmware do SP diferente da fornecida com o ONTAP.
Exiba o status da última atualização de firmware do SP acionada pelo ONTAP, incluindo as seguintes informações: • A hora de início e fim da atualização de firmware mais recente do SP • Se uma atualização está em andamento e a porcentagem que está concluída	`system service-processor image update-progress show`

Comandos para gerenciar o acesso SSH ao SP

Se você quiser…	Execute este comando ONTAP…
Conceda acesso SP apenas aos endereços IP especificados	`system service-processor ssh add-allowed-addresses`
Bloquear o acesso aos endereços IP especificados ao SP	`system service-processor ssh remove-allowed-addresses`
Exiba os endereços IP que podem acessar o SP	`system service-processor ssh show`

Comandos para administração geral do SP

Se você quiser…	Execute este comando ONTAP…
Exibir informações gerais do SP, incluindo o seguinte: • O tipo de dispositivo de gerenciamento remoto • O estado atual do SP • Se a rede SP está configurada • Informações de rede, como o endereço IP público e o endereço MAC • A versão do firmware do SP e a versão da interface de gestão inteligente da plataforma (IPMI) • Se a atualização automática do firmware do SP está ativada	`system service-processor show` A exibição de informações completas do SP requer o `-instance` parâmetro.
Reinicie o SP em um nó	`system service-processor reboot-sp`
Gere e envie uma mensagem do AutoSupport que inclua os arquivos de log do SP coletados de um nó especificado	`system node autosupport invoke-splog`
Exiba o mapa de alocação dos arquivos de log do SP coletados no cluster, incluindo os números de sequência dos arquivos de log do SP que residem em cada nó de coleta	`system service-processor log show-allocations`

Informações relacionadas

"Referência do comando ONTAP"

Comandos ONTAP para gerenciamento de BMC

Esses comandos ONTAP são suportados no controlador de gerenciamento da placa base (BMC).

O BMC usa alguns dos mesmos comandos que o processador de serviço (SP). Os seguintes comandos SP são suportados no BMC.

Se você quiser…	Use este comando
Apresentar as informações do BMC	**`system service-processor show`**
Apresentar/modificar a configuração da rede BMC	**`system service-processor network show/modify`**
Reinicie o BMC	**`system service-processor reboot-sp`**

Se você quiser…	Use este comando
Apresentar/modificar os detalhes da imagem de firmware do BMC instalada atualmente	**system service-processor image show/modify**
Atualize o firmware do BMC	**system service-processor image update**
Apresentar o estado da atualização de firmware do BMC mais recente	**system service-processor image update-progress show**
Ative a configuração automática de rede para o BMC usar um endereço IPv4 ou IPv6 na sub-rede especificada	**system service-processor network auto-configuration enable**
Desative a configuração automática de rede para um endereço IPv4 ou IPv6 na sub-rede especificada para o BMC	**system service-processor network auto-configuration disable**
Apresentar a configuração automática da rede BMC	**system service-processor network auto-configuration show**

Para comandos que não são suportados pelo firmware do BMC, a seguinte mensagem de erro é retornada.

```
::> Error: Command not supported on this platform.
```

Comandos CLI do BMC

Você pode fazer login no BMC usando SSH. Os seguintes comandos são suportados a partir da linha de comando BMC.

Comando	Função
sistema	Exibir uma lista de todos os comandos.
consola do sistema	Ligue à consola do sistema. `Ctrl+D`Utilize para sair da sessão.
núcleo do sistema	Descarregue o núcleo do sistema e reinicie.
ciclo de alimentação do sistema	Desligue o sistema e, em seguida, ligue-o.
desligar o sistema	Desligue o sistema.
ligar o sistema	Ligue o sistema.

Comando	Função
estado de alimentação do sistema	Estado de alimentação do sistema de impressão.
reposição do sistema	Reinicie o sistema.
registo do sistema	Imprimir registos da consola do sistema
apresentação da fru do sistema [id]	Despejar todas/informações da unidade substituível em campo (FRU) selecionada.

Gerenciar o tempo do cluster (somente administradores de cluster)

Podem ocorrer problemas quando o tempo do cluster é impreciso. Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

O NTP está sempre ativado. No entanto, a configuração ainda é necessária para que o cluster sincronize com uma fonte de tempo externa. O ONTAP permite gerenciar a configuração NTP do cluster das seguintes maneiras:

- Pode associar um máximo de 10 servidores NTP externos ao cluster (`cluster time-service ntp server create`).
  - Para redundância e qualidade do serviço de tempo, você deve associar pelo menos três servidores NTP externos ao cluster.
  - Você pode especificar um servidor NTP usando seu endereço IPv4 ou IPv6 ou nome de host totalmente qualificado.
  - Pode especificar manualmente a versão NTP (v3 ou v4) a utilizar.

    Por padrão, o ONTAP seleciona automaticamente a versão NTP que é suportada para um determinado servidor NTP externo.

  Se a versão NTP especificada não for suportada para o servidor NTP, a troca de tempo não poderá ocorrer.

  - No nível de privilégio avançado, você pode especificar um servidor NTP externo que está associado ao cluster para ser a principal fonte de tempo para corrigir e ajustar a hora do cluster.
- Pode visualizar os servidores NTP associados ao cluster (`cluster time-service ntp server show`).
- Pode modificar a configuração NTP do cluster (`cluster time-service ntp server modify`).
- Você pode desassociar o cluster de um servidor NTP externo (`cluster time-service ntp server delete`).

- No nível de privilégio avançado, pode repor a configuração limpando a associação de todos os servidores NTP externos com o cluster (`cluster time-service ntp server reset`).

Um nó que se junta a um cluster adota automaticamente a configuração NTP do cluster.

Além de usar o NTP, o ONTAP também permite gerenciar manualmente o tempo do cluster. Esse recurso é útil quando você precisa corrigir o tempo errado (por exemplo, o tempo de um nó ficou significativamente incorreto após uma reinicialização). Nesse caso, você pode especificar um tempo aproximado para o cluster até que o NTP possa sincronizar com um servidor de hora externo. O tempo definido manualmente entra em vigor em todos os nós do cluster.

Você pode gerenciar manualmente o tempo do cluster das seguintes maneiras:

- Pode definir ou modificar o fuso horário, a data e a hora no cluster (`cluster date modify`).
- Pode apresentar as definições atuais de fuso horário, data e hora do cluster (`cluster date show`).

> As programações de trabalhos não se ajustam às alterações manuais de data e hora do cluster. Esses trabalhos são programados para serem executados com base na hora atual do cluster quando o trabalho foi criado ou quando o trabalho foi executado mais recentemente. Portanto, se você alterar manualmente a data ou a hora do cluster, use os `job show` comandos e `job history show` para verificar se todos os trabalhos agendados estão na fila e concluídos de acordo com seus requisitos.

Comandos para gerenciar o tempo do cluster

Você usa os `cluster time-service ntp server` comandos para gerenciar os servidores NTP para o cluster. Você usa os `cluster date` comandos para gerenciar o tempo do cluster manualmente.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Os comandos a seguir permitem gerenciar os servidores NTP para o cluster:

Se você quiser…	Use este comando…
Associe o cluster a um servidor NTP externo sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Associe o cluster a um servidor NTP externo com autenticação simétrica Artigo disponível no ONTAP 9.5 ou posterior	`cluster time-service ntp server create -server server_ip_address -key-id key_id` O `key_id` deve se referir a uma chave compartilhada existente configurada com "chave ntp de serviço de tempo do cluster'.

Se você quiser…	Use este comando…
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária. Disponível no ONTAP 9.5 ou posterior	`cluster time-service ntp server modify -server server_name -key-id key_id`
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Exibir informações sobre os servidores NTP associados ao cluster	`cluster time-service ntp server show`
Modifique a configuração de um servidor NTP externo associado ao cluster	`cluster time-service ntp server modify`
Dissociar um servidor NTP do cluster	`cluster time-service ntp server delete`
Redefina a configuração limpando a associação de todos os servidores NTP externos com o cluster	`cluster time-service ntp server reset` Este comando requer o nível de privilégio avançado.

Os comandos a seguir permitem gerenciar o tempo do cluster manualmente:

Se você quiser…	Use este comando…
Defina ou modifique o fuso horário, a data e a hora	`cluster date modify`
Exiba as configurações de fuso horário, data e hora do cluster	`cluster date show`

Informações relacionadas

"Referência do comando ONTAP"

Gerencie o banner e o MOTD

Gerencie o banner e a visão geral do MOTD

O ONTAP permite configurar um banner de login ou uma mensagem do dia (MOTD) para comunicar informações administrativas aos usuários da CLI do cluster ou máquina virtual de armazenamento (SVM).

Um banner é exibido em uma sessão de console (apenas para acesso ao cluster) ou uma sessão SSH (para acesso ao cluster ou SVM) antes que um usuário seja solicitado a autenticação, como uma senha. Por exemplo, você pode usar o banner para exibir uma mensagem de aviso como a seguinte para alguém que tenta fazer login no sistema:

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

Um MOTD é exibido em uma sessão de console (apenas para acesso de cluster) ou uma sessão SSH (para acesso de cluster ou SVM) depois que um usuário é autenticado, mas antes que o prompt de clustershell seja exibido. Por exemplo, você pode usar o MOTD para exibir uma mensagem de boas-vindas ou informativa, como a seguinte, que somente usuários autenticados verão:

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

Você pode criar ou modificar o conteúdo do banner ou MOTD usando o `security login banner modify` comando ou `security login motd modify`, respetivamente, das seguintes maneiras:

- Você pode usar a CLI interativamente ou não interativamente para especificar o texto a ser usado para o banner ou MOTD.

  O modo interativo, iniciado quando o comando é usado sem o `-message` parâmetro ou `-uri`, permite que você use novas linhas (também conhecidas como final de linhas) na mensagem.

  O modo não interativo, que usa o `-message` parâmetro para especificar a cadeia de carateres da mensagem, não suporta novas linhas.

- Você pode fazer upload de conteúdo de um local FTP ou HTTP para usar para o banner ou MOTD.
- Pode configurar o MOTD para apresentar conteúdo dinâmico.

Exemplos do que você pode configurar o MOTD para exibir dinamicamente incluem o seguinte:

- Nome do cluster, nome do nó ou nome do SVM
- Data e hora do cluster
- Nome do utilizador que inicia sessão
- Último login para o usuário em qualquer nó no cluster
- Nome do dispositivo de início de sessão ou endereço IP
- Nome do sistema operacional
- Versão de versão do software
- String de versão de cluster eficaz a `security login motd modify` página man descreve as sequências de escape que você pode usar para ativar o MOTD para exibir conteúdo gerado dinamicamente.

O banner não suporta conteúdo dinâmico.

Você pode gerenciar o banner e o MOTD no nível do cluster ou SVM:

- Os seguintes fatos se aplicam ao banner:
  - O banner configurado para o cluster também é usado para todos os SVMs que não têm uma mensagem de banner definida.
  - É possível configurar um banner no nível da SVM para cada SVM.

    Se um banner no nível do cluster tiver sido configurado, ele será substituído pelo banner no nível da SVM para determinado SVM.
- Os seguintes factos aplicam-se ao MOTD:
  - Por padrão, o MOTD configurado para o cluster também é ativado para todos os SVMs.
  - Além disso, é possível configurar um MOTD no nível da SVM para cada SVM.

    Nesse caso, os usuários que fizerem login no SVM verão dois MOTDs, um definido no nível do cluster e o outro no nível SVM.
  - O MOTD no nível do cluster pode ser ativado ou desativado por SVM pelo administrador do cluster.

    Se o administrador do cluster desativar o MOTD em nível de cluster para um SVM, um usuário que faz login no SVM não verá o MOTD em nível de cluster.

Crie um banner

Você pode criar um banner para exibir uma mensagem para alguém que tente acessar o cluster ou SVM. O banner é exibido em uma sessão de console (apenas para acesso ao cluster) ou em uma sessão SSH (para acesso ao cluster ou SVM) antes que um usuário seja solicitado a autenticação.

Passos

1. Use o `security login banner modify` comando para criar um banner para o cluster ou SVM:

Se você quiser…	Então…
Especifique uma mensagem que seja uma única linha	Utilize o `-messagetext` parâmetro " " para especificar o texto.
Inclua novas linhas (também conhecidas como fim de linhas) na mensagem	Use o comando sem o `-message` parâmetro ou `-uri` para iniciar o modo interativo para editar o banner.
Faça upload de conteúdo de um local para usar para o banner	Use o `-uri` parâmetro para especificar a localização FTP ou HTTP do conteúdo.

O tamanho máximo para um banner é de 2.048 bytes, incluindo novas linhas.

Um banner criado usando o `-uri` parâmetro é estático. Não é atualizado automaticamente para refletir as alterações subsequentes do conteúdo fonte.

O banner criado para o cluster também é exibido para todos os SVMs que não têm um banner existente. Qualquer banner criado posteriormente para um SVM substitui o banner no nível do cluster desse SVM. Especificar o `-message` parâmetro com um hífen entre aspas duplas (`"-"`) para o SVM redefine o SVM para usar o banner no nível do cluster.

2. Verifique se o banner foi criado exibindo-o com o `security login banner show` comando.

   Especificar o `-message` parâmetro com uma string vazia (`""`) exibe banners que não têm conteúdo.

   Especificar o `-message` parâmetro com `"-"` exibe todos os SVMs (admin ou dados) que não têm um banner configurado.

Exemplos de criação de banners

O exemplo a seguir usa o modo não interativo para criar um banner para o cluster "'cluster1"":

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

O exemplo a seguir usa o modo interativo para criar um banner para o "VM1" SVM:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

O exemplo a seguir exibe os banners que foram criados:

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

Informações relacionadas

Gerenciar o banner

Gerenciar o banner

É possível gerenciar o banner no nível do cluster ou SVM. O banner configurado para o cluster também é usado para todos os SVMs que não têm uma mensagem de banner definida. Um banner criado posteriormente para um SVM substitui o banner do cluster para esse SVM.

Opções

- Gerencie o banner no nível do cluster:

Se você quiser…	Então…
Crie um banner para exibir todas as sessões de login da CLI	Definir um banner no nível do cluster: `*security login banner modify -vserver *cluster_name* { [-message "text"]
[*-uri ftp_or_http_addr*] }*`	Remova o banner para todos os logins (cluster e SVM)
Defina o banner para uma string vazia (`""`): **`security login banner modify -vserver * -message ""`**	Substituir um banner criado por um administrador SVM
Modifique a mensagem de banner SVM: `*security login banner modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*`

- Gerencie o banner no nível da SVM:

  Não é necessário especificar `-vserver *svm_name*` no contexto SVM.

Se você quiser…	Então…
Substitua o banner fornecido pelo administrador do cluster por um banner diferente para o SVM	Crie um banner para o SVM: `*security login banner modify -vserver *svm_name* { [-message "text"]
[-uri ftp_or_http_addr] }*`	Suprimir o banner fornecido pelo administrador do cluster para que nenhum banner seja exibido para o SVM
Defina o banner SVM para uma cadeia vazia para o SVM: **`security login banner modify -vserver *svm_name* -message ""`**	Use o banner no nível do cluster quando o SVM usar um banner no nível da SVM

Crie um MOTD

Você pode criar uma mensagem do dia (MOTD) para comunicar informações a usuários CLI autenticados. O MOTD é exibido em uma sessão de console (somente para acesso ao cluster) ou em uma sessão SSH (para acesso ao cluster ou SVM) depois que um usuário é autenticado, mas antes que o prompt do clustershell seja exibido.

Passos

1. Use o `security login motd modify` comando para criar um MOTD para o cluster ou SVM:

Se você quiser…	Então…
Especifique uma mensagem que seja uma única linha	Utilize o `-messagetext` parâmetro " " para especificar o texto.
Incluir novas linhas (também conhecido como fim de linhas)	Use o comando sem o `-message` parâmetro ou `-uri` para iniciar o modo interativo para editar o MOTD.
Faça upload de conteúdo de um local para usar para o MOTD	Use o `-uri` parâmetro para especificar a localização FTP ou HTTP do conteúdo.

   O tamanho máximo para um MOTD é de 2.048 bytes, incluindo novas linhas.

   A `security login motd modify` página man descreve as sequências de escape que você pode usar para ativar o MOTD para exibir conteúdo gerado dinamicamente.

   Um MOTD criado usando o `-uri` parâmetro é estático. Não é atualizado automaticamente para refletir as alterações subsequentes do conteúdo fonte.

   Um MOTD criado para o cluster também é exibido para todos os logins SVM por padrão, juntamente com um MOTD no nível SVM que você pode criar separadamente para um determinado SVM. Definir o `-is-cluster-message-enabled` parâmetro como `false` para um SVM impede que o MOTD no nível do cluster seja exibido para esse SVM.

2. Verifique se o MOTD foi criado exibindo-o com o `security login motd show` comando.

   Especificando o `-message` parâmetro com uma string vazia (`""`) exibe MOTDs que não estão configurados ou não têm conteúdo.

   Consulte a "segurança login motd modificar" página man do comando para obter uma lista de parâmetros a serem usados para permitir que o MOTD exiba conteúdo gerado dinamicamente. Certifique-se de verificar a página de manual específica para a sua versão do ONTAP.

Exemplos de criação de MOTDs

O exemplo a seguir usa o modo não interativo para criar um MOTD para o cluster ""cluster1"":

```
cluster1::> security login motd modify -message "Greetings!"
```

O exemplo a seguir usa o modo interativo para criar um MOTD para o SVM "VM1" que usa sequências de escape para exibir conteúdo gerado dinamicamente:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

O exemplo a seguir exibe os MOTDs que foram criados:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

Gerencie o MOTD no ONTAP

É possível gerenciar a mensagem do dia (MOTD) no nível do cluster ou SVM. Por padrão, o MOTD configurado para o cluster também é ativado para todos os SVMs. Além disso, é possível configurar um MOTD no nível da SVM para cada SVM. O MOTD no nível do cluster pode ser ativado ou desativado para cada SVM pelo administrador do cluster.

Saiba mais sobre o "sequências de fuga" que pode ser usado para gerar conteúdo dinamicamente para o MOTD na referência de comando ONTAP.

Opções

- Gerencie o MOTD no nível do cluster:

Se você quiser…	Então…
Crie um MOTD para todos os logins quando não houver MOTD existente	Definir um MOTD de nível de cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Altere o MOTD para todos os logins quando nenhum MOTDs no nível SVM estiver configurado
Modifique o MOTD no nível do cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"] }	[-uri ftp_or_http_addr] }*`
Remova o MOTD para todos os logins quando nenhum MOTDs de nível SVM estiver configurado	Defina o MOTD de nível de cluster para uma cadeia vazia (`""`): **`security login motd modify -vserver *cluster_name* -message ""`**
Peça a cada SVM que exiba o MOTD no nível do cluster em vez de usar o MOTD no nível da SVM	Defina um MOTD de nível de cluster e, em seguida, defina todos os MOTDs de nível SVM para uma cadeia vazia com o MOTD de nível de cluster ativado: a. `*security login motd modify -vserver *cluster_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*` .. **`security login motd modify { -vserver !"*cluster_name*" } -message "" -is -cluster-message-enabled true`**	Tenha um MOTD exibido apenas para SVMs selecionadas e não use nenhum MOTD no nível do cluster
Defina o MOTD de nível de cluster para uma cadeia vazia e, em seguida, defina MOTDs de nível SVM para SVMs selecionadas: a. **`security login motd modify -vserver *cluster_name* -message ""`** b. `*security login motd modify -vserver *svm_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] }*` + Você pode repetir esta etapa para cada SVM conforme necessário.
Use o mesmo MOTD no nível da SVM para todos os SVMs (dados e administradores)	Defina o cluster e todos os SVMs para usar o mesmo MOTD: `*security login motd modify *-vserver* * { [-message "*text*"]

Se você quiser…	Então…
[-uri *ftp_or_http_addr*] }*` [NOTE] ==== Se você usar o modo interativo, a CLI solicitará que você insira o MOTD individualmente para o cluster e cada SVM. Você pode colar o mesmo MOTD em cada instância quando for solicitado. ====	Tenha um MOTD de nível de cluster disponível opcionalmente para todos os SVMs, mas não queira que o MOTD seja exibido para logins de cluster
Defina um MOTD no nível do cluster, mas desative sua exibição para o cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false*`
Remova todos os MOTDs nos níveis de cluster e SVM quando apenas alguns SVMs tiverem MOTDs no nível do cluster e SVM	Defina o cluster e todos os SVMs para usar uma cadeia vazia para o MOTD: **`security login motd modify -vserver * -message ""`**
Modifique o MOTD apenas para os SVMs que têm uma cadeia de carateres não vazia, quando outros SVMs usam uma cadeia vazia e quando um MOTD diferente é usado no nível do cluster	Use consultas estendidas para modificar o MOTD seletivamente: `*security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Exibir todos os MOTDs que contêm texto específico (por exemplo, "'janeiro"" seguido de "'2015"") em qualquer lugar em uma mensagem única ou multilinha, mesmo que o texto seja dividido em linhas diferentes
Use uma consulta para exibir MOTDs: **`security login motd show -message *"January"*"2015"*`**	Crie interativamente um MOTD que inclua novas linhas múltiplas e consecutivas (também conhecidas como fim de linhas, ou EOLS)

- Gerencie o MOTD no nível SVM:

  Não é necessário especificar `-vserver *svm_name*` no contexto SVM.

Se você quiser…	Então…
Use um MOTD no nível da SVM diferente, quando o SVM já tiver um MOTD no nível da SVM	Modifique o MOTD no nível da SVM: `*security login motd modify -vserver *svm_name* { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Use apenas o MOTD no nível do cluster para SVM, quando o SVM já tiver um MOTD no nível do SVM
Defina o SVM-level MOTD para uma cadeia vazia e, em seguida, faça com que o administrador de cluster ative o cluster-level MOTD para o SVM: a. **`security login motd modify -vserver *svm_name* -message ""`** b. (Para o administrador do cluster) **`security login motd modify -vserver *svm_name* -is-cluster-message-enabled true`**	Não é possível que o SVM exiba nenhum MOTD quando os MOTDs de nível de cluster e SVM forem exibidos atualmente para o SVM

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Gerenciar trabalhos e agendar

Os trabalhos são colocados em uma fila de trabalhos e executados em segundo plano quando os recursos estão disponíveis. Se uma tarefa estiver consumindo muitos recursos de cluster, você pode pará-la ou pausar até que haja menos demanda no cluster. Também pode monitorizar e reiniciar trabalhos.

Categorias de trabalho

Existem três categorias de trabalhos que você pode gerenciar: Afiliados ao servidor, afiliados a cluster e privados.

Um trabalho pode estar em qualquer uma das seguintes categorias:

- **Empregos afiliados ao servidor**

  Esses trabalhos são enfileirados pela estrutura de gerenciamento para um nó específico a ser executado.

- **Empregos afiliados a cluster**

  Esses trabalhos são enfileirados pela estrutura de gerenciamento para qualquer nó no cluster a ser executado.

- **Empregos privados**

  Essas tarefas são específicas para um nó e não usam o banco de dados replicado (RDB) ou qualquer outro mecanismo de cluster. Os comandos que gerem trabalhos privados requerem o nível de privilégio avançado ou superior.

Comandos para gerir trabalhos

Quando você insere um comando que invoca uma tarefa, normalmente, o comando informa que a tarefa foi enfileirada e retorna ao prompt de comando CLI. No entanto, alguns comandos reportam o progresso da tarefa e não retornam ao prompt de comando da CLI até que a tarefa seja concluída. Nesses casos, você pode pressionar Ctrl-C para mover o trabalho para o fundo.

Se você quiser…	Use este comando…
Exibir informações sobre todos os trabalhos	`job show`
Exibir informações sobre trabalhos por nó	`job show bynode`
Exibir informações sobre trabalhos afiliados ao cluster	`job show-cluster`
Exibir informações sobre os trabalhos concluídos	`job show-completed`
Apresentar informações sobre o histórico de trabalhos	`job history show` São armazenados até 25.000 registos de trabalho para cada nó no cluster. Consequentemente, tentar exibir o histórico completo do trabalho pode levar muito tempo. Para evitar tempos de espera potencialmente longos, você deve exibir tarefas por nó, máquina virtual de armazenamento (SVM) ou ID de Registro.
Apresentar a lista de trabalhos privados	`job private show` (nível de privilégio avançado)
Exibir informações sobre trabalhos privados concluídos	`job private show-completed` (nível de privilégio avançado)
Exibir informações sobre o estado de inicialização para gerentes de tarefas	`job initstate show` (nível de privilégio avançado)
Monitorize o progresso de um trabalho	`job watch-progress`
Monitore o progresso de um trabalho privado	`job private watch-progress` (nível de privilégio avançado)
Pausar um trabalho	`job pause`
Pausar um trabalho privado	`job private pause` (nível de privilégio avançado)
Retomar um trabalho em pausa	`job resume`

Se você quiser…	Use este comando…
Retomar um trabalho privado em pausa	`job private resume` (nível de privilégio avançado)
Parar um trabalho	`job stop`
Parar um trabalho privado	`job private stop` (nível de privilégio avançado)
Eliminar um trabalho	`job delete`
Eliminar um trabalho privado	`job private delete` (nível de privilégio avançado)
Desassocie uma tarefa afiliada ao cluster a um nó não disponível que o possua, para que outro nó possa assumir a propriedade dessa tarefa	`job unclaim` (nível de privilégio avançado)

Você pode usar o `event log show` comando para determinar o resultado de uma tarefa concluída.

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerir agendas de trabalhos

Muitas tarefas - por exemplo, cópias Snapshot de volume - podem ser configuradas para serem executadas em programações especificadas.os horários que são executados em momentos específicos são chamados de programações *cron* (semelhantes às programações UNIX `cron`). As programações que são executadas em intervalos são chamadas *interval* programações. Utilize os `job schedule` comandos para gerir agendas de trabalhos.

As programações de trabalhos não se ajustam às alterações manuais da data e hora do cluster. Esses trabalhos são programados para serem executados com base na hora atual do cluster quando o trabalho foi criado ou quando o trabalho foi executado mais recentemente. Portanto, se você alterar manualmente a data ou a hora do cluster, use os `job show` comandos e `job history show` para verificar se todos os trabalhos agendados estão na fila e concluídos de acordo com seus requisitos.

Se o cluster fizer parte de uma configuração do MetroCluster, as programações de tarefas em ambos os clusters devem ser idênticas. Portanto, se você criar, modificar ou excluir um agendamento de trabalhos, deverá executar a mesma operação no cluster remoto.

Se você quiser…	Use este comando…
Exibir informações sobre todas as programações	`job schedule show`
Exibir a lista de trabalhos por agendamento	`job schedule show-jobs`

Se você quiser…	Use este comando…
Exibir informações sobre cronogramas do cron	`job schedule cron show`
Exibir informações sobre programações de intervalos	`job schedule interval show`
Crie um cronograma cron	`job schedule cron create` A partir do ONTAP 9.10,1, você pode incluir o SVM para sua agenda de trabalho.
Crie um agendamento de intervalos	`job schedule interval create` É necessário especificar pelo menos um dos seguintes parâmetros: `-days`, `-hours`, `-minutes`, `-seconds` Ou .
Modifique um cronograma do cron	`job schedule cron modify`
Modificar um agendamento de intervalos	`job schedule interval modify`
Eliminar uma agenda	`job schedule delete`
Exclua um cronograma do cron	`job schedule cron delete`
Eliminar um agendamento de intervalos	`job schedule interval delete`

Informações relacionadas

"Referência do comando ONTAP"

Fazer backup e restaurar configurações de cluster (somente administradores de cluster)

Quais são os arquivos de backup de configuração

Os arquivos de backup de configuração são arquivos de arquivo (.7z) que contêm informações para todas as opções configuráveis que são necessárias para o cluster e os nós dentro dele, para operar corretamente.

Esses arquivos armazenam a configuração local de cada nó, além da configuração replicada em todo o cluster. Você usa arquivos de backup de configuração para fazer backup e restaurar a configuração do cluster.

Existem dois tipos de arquivos de backup de configuração:

- * Ficheiro de cópia de segurança da configuração do nó*

  Cada nó íntegro no cluster inclui um arquivo de backup de configuração de nós, que contém todas as

informações de configuração e metadados necessários para que o nó opere de forma saudável no cluster.

- **Ficheiro de cópia de segurança de configuração de cluster**

  Esses arquivos incluem um arquivo de todos os arquivos de backup de configuração de nó no cluster, além das informações replicadas de configuração de cluster (o banco de dados replicado ou arquivo RDB). Os arquivos de backup de configuração de cluster permitem restaurar a configuração de todo o cluster ou de qualquer nó no cluster. As programações de backup de configuração de cluster criam esses arquivos automaticamente e os armazenam em vários nós no cluster.

> Os ficheiros de cópia de segurança de configuração contêm apenas informações de configuração. Eles não incluem nenhum dado de usuário. Para obter informações sobre como restaurar dados do usuário, "Proteção de dados"consulte .

Como o backup automático das configurações de nó e cluster é feito automaticamente

Três programações separadas criam automaticamente arquivos de backup de configuração de cluster e nó e replicam-os entre os nós do cluster.

Os arquivos de backup de configuração são criados automaticamente de acordo com as seguintes programações:

- A cada 8 horas
- Diariamente
- Semanalmente

Em cada um desses momentos, um arquivo de backup de configuração de nós é criado em cada nó íntegro no cluster. Todos esses arquivos de backup de configuração de nó são coletados em um único arquivo de backup de configuração de cluster, juntamente com a configuração de cluster replicada e salvos em um ou mais nós no cluster.

Comandos para gerenciar programações de backup de configuração

Você pode usar os `system configuration backup settings` comandos para gerenciar programações de backup de configuração.

Esses comandos estão disponíveis no nível avançado de privilégio.

Se você quiser…	Use este comando…
Altere as configurações de um agendamento de backup de configuração: • Especifique um URL remoto (HTTP, HTTPS, FTP, FTPS ou TFTP) onde os arquivos de backup de configuração serão carregados além dos locais padrão no cluster • Especifique um nome de usuário a ser usado para fazer login no URL remoto • Defina o número de backups a serem mantidos para cada agendamento de backup de configuração	`system configuration backup settings modify` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição. O servidor da Web para o qual você está fazendo o upload do arquivo de backup de configuração deve ter as operações de COLOCAÇÃO ativadas para HTTP e POST ativadas para HTTPS. Para obter mais informações, consulte a documentação do servidor Web.
Defina a senha a ser usada para fazer login no URL remoto	`system configuration backup settings set-password`
Ver as definições do agendamento da cópia de segurança da configuração	`system configuration backup settings show` Você define o `-instance` parâmetro para exibir o nome de usuário e o número de backups a serem mantidos para cada agendamento.

Comandos para gerenciar arquivos de backup de configuração

Você usa os `system configuration backup` comandos para gerenciar arquivos de backup de configuração de cluster e nó.

Esses comandos estão disponíveis no nível avançado de privilégio.

Se você quiser…	Use este comando…
Crie um novo arquivo de backup de configuração de nó ou cluster	`system configuration backup create`
Copie um arquivo de backup de configuração de um nó para outro nó no cluster	`system configuration backup copy`

Se você quiser…	Use este comando…
Carregar um arquivo de backup de configuração de um nó no cluster para um URL remoto (FTP, HTTP, HTTPS, TFTP ou FTPS)	`system configuration backup upload` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição. O servidor da Web para o qual você está fazendo o upload do arquivo de backup de configuração deve ter as operações de COLOCAÇÃO ativadas para HTTP e POST ativadas para HTTPS. Alguns servidores da Web podem exigir a instalação de um módulo adicional. Para obter mais informações, consulte a documentação do servidor Web. Os formatos de URL suportados variam de acordo com a versão do ONTAP. Saiba mais sobre os comandos de configuração do sistema no ""Referência do comando ONTAP".
Faça o download de um arquivo de backup de configuração de um URL remoto para um nó no cluster e, se especificado, valide o certificado digital	`system configuration backup download` Quando utilizar HTTPS na URL remota, utilize a `-validate-certification` opção para ativar ou desativar a validação de certificados digitais. A validação do certificado está desativada por predefinição.
Renomeie um arquivo de backup de configuração em um nó no cluster	`system configuration backup rename`
Visualize os arquivos de backup de configuração de nó e cluster para um ou mais nós no cluster	`system configuration backup show`
Exclua um arquivo de backup de configuração em um nó	`system configuration backup delete` Este comando exclui o arquivo de backup de configuração somente no nó especificado. Se o arquivo de backup de configuração também existir em outros nós no cluster, ele permanecerá nesses nós.

Encontre um arquivo de backup de configuração para usar para recuperar um nó

Você usa um arquivo de backup de configuração localizado em um URL remoto ou em um nó no cluster para recuperar uma configuração de nó.

Sobre esta tarefa

Você pode usar um arquivo de backup de configuração de cluster ou nó para restaurar uma configuração de nó.

Passo

1. Disponibilize o arquivo de backup de configuração para o nó para o qual você precisa restaurar a configuração.

Se o arquivo de backup de configuração estiver localizado…	Então…
Em um URL remoto	Use o `system configuration backup download` comando no nível de privilégio avançado para baixá-lo para o nó de recuperação.
Em um nó no cluster	a. Use o `system configuration backup show` comando no nível de privilégio avançado para exibir a lista de arquivos de backup de configuração disponíveis no cluster que contém a configuração do nó de recuperação. b. Se o arquivo de backup de configuração que você identificar não existir no nó de recuperação, use o `system configuration backup copy` comando para copiá-lo para o nó de recuperação.

Se você recriou o cluster anteriormente, você deve escolher um arquivo de backup de configuração que foi criado após a recriação do cluster. Se você precisar usar um arquivo de backup de configuração que foi criado antes da recriação do cluster, depois de recuperar o nó, você deve recriar o cluster novamente.

Restaure a configuração do nó usando um arquivo de backup de configuração

Você restaura a configuração do nó usando o arquivo de backup de configuração identificado e disponibilizado para o nó de recuperação.

Sobre esta tarefa

Você só deve executar esta tarefa para se recuperar de um desastre que resultou na perda dos arquivos de configuração local do nó.

Passos

1. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

2. Se o nó estiver saudável, no nível de privilégio avançado de um nó diferente, use o `cluster modify`

comando com os `-node` parâmetros e `-eligibility` para marcá-lo inelegível e isolá-lo do cluster.

Se o nó não estiver saudável, então você deve pular esta etapa.

Este exemplo modifica o node2 para ser inelegível para participar do cluster para que sua configuração possa ser restaurada:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Use o `system configuration recovery node restore` comando no nível de privilégio avançado para restaurar a configuração do nó a partir de um arquivo de backup de configuração.

   Se o nó perdeu sua identidade, incluindo seu nome, então você deve usar o `-nodename-in-backup` parâmetro para especificar o nome do nó no arquivo de backup de configuração.

   Este exemplo restaura a configuração do nó usando um dos arquivos de backup de configuração armazenados no nó:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

   A configuração é restaurada e o nó é reiniciado.

4. Se você marcou o nó inelegível, use o `system configuration recovery cluster sync` comando para marcar o nó como qualificado e sincronizá-lo com o cluster.
5. Se você estiver operando em um ambiente SAN, use o `system node reboot` comando para reinicializar o nó e restabelecer o quorum SAN.

Depois de terminar

Se você recriou anteriormente o cluster e se estiver restaurando a configuração do nó usando um arquivo de backup de configuração que foi criado antes da recriação do cluster, você deverá recriar o cluster novamente.

Encontre uma configuração a ser usada para recuperar um cluster

Você usa a configuração de um nó no cluster ou de um arquivo de backup de configuração de cluster para recuperar um cluster.

Passos

1. Escolha um tipo de configuração para recuperar o cluster.

   - Um nó no cluster

Se o cluster consistir em mais de um nó e um dos nós tiver uma configuração de cluster a partir de quando o cluster estava na configuração desejada, então você pode recuperar o cluster usando a configuração armazenada nesse nó.

Na maioria dos casos, o nó que contém o anel de replicação com o ID de transação mais recente é o melhor nó a ser usado para restaurar a configuração do cluster. O `cluster ring show` comando no nível de privilégio avançado permite exibir uma lista dos anéis replicados disponíveis em cada nó no cluster.

- Um arquivo de backup de configuração de cluster

  Se você não conseguir identificar um nó com a configuração correta do cluster ou se o cluster consistir em um único nó, você poderá usar um arquivo de backup de configuração de cluster para recuperar o cluster.

Se você estiver recuperando o cluster de um arquivo de backup de configuração, todas as alterações de configuração feitas desde que o backup foi feito serão perdidas. Você deve resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração atual após a recuperação. Consulte o artigo da base de dados de Conhecimento "Guia de resolução da cópia de segurança da configuração do ONTAP"para obter orientações sobre resolução de problemas.

2. Se você optar por usar um arquivo de backup de configuração de cluster, disponibilize o arquivo para o nó que você planeja usar para recuperar o cluster.

Se o arquivo de backup de configuração estiver localizado…	**Então…**
Em um URL remoto	Use o `system configuration backup download` comando no nível de privilégio avançado para baixá-lo para o nó de recuperação.
Em um nó no cluster	a. Use o `system configuration backup show` comando no nível de privilégio avançado para encontrar um arquivo de backup de configuração de cluster que foi criado quando o cluster estava na configuração desejada. b. Se o arquivo de backup de configuração de cluster não estiver localizado no nó que você pretende usar para recuperar o cluster, use o `system configuration backup copy` comando para copiá-lo para o nó de recuperação.

Restaurar uma configuração de cluster a partir de uma configuração existente

Para restaurar uma configuração de cluster a partir de uma configuração existente após uma falha de cluster, crie novamente o cluster usando a configuração de cluster que você escolheu e disponibilizou para o nó de recuperação e, em seguida, rejunte cada nó adicional ao novo cluster.

Sobre esta tarefa

Você só deve executar essa tarefa para se recuperar de um desastre que resultou na perda da configuração do cluster.

> Se você estiver recriando o cluster a partir de um arquivo de backup de configuração, entre em Contato com o suporte técnico para resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração presente no cluster.
>
> Se você estiver recuperando o cluster de um arquivo de backup de configuração, todas as alterações de configuração feitas desde que o backup foi feito serão perdidas. Você deve resolver quaisquer discrepâncias entre o arquivo de backup de configuração e a configuração atual após a recuperação. Consulte o artigo da base de dados de Conhecimento "Guia de resolução de backup de configuração do ONTAP para orientação de solução de problemas" .

Passos

1. Desativar o failover de storage para cada par de HA:

   `storage failover modify -node node_name -enabled false`

   Você só precisa desativar o failover de storage uma vez para cada par de HA. Quando você desativa o failover de armazenamento para um nó, o failover de armazenamento também é desativado no parceiro do nó.

2. Interrompa cada nó, exceto o nó em recuperação:

   `system node halt -node node_name -reason "text"`

   ```
   cluster1::*> system node halt -node node0 -reason "recovering cluster"

   Warning: Are you sure you want to halt the node? {y|n}: y
   ```

3. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

4. No nó de recuperação, use o **`system configuration recovery cluster recreate`** comando para recriar o cluster.

   Este exemplo recria o cluster usando as informações de configuração armazenadas no nó de recuperação:

   ```
   cluster1::*> configuration recovery cluster recreate -from node

   Warning: This command will destroy your existing cluster. It will
            rebuild a new single-node cluster consisting of this node
            and its current configuration. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress.
   Do you want to continue? {y|n}: y
   ```

Um novo cluster é criado no nó de recuperação.

5. Se você estiver recriando o cluster a partir de um arquivo de backup de configuração, verifique se a recuperação do cluster ainda está em andamento:

   system configuration recovery cluster show

   Não é necessário verificar o estado de recuperação do cluster se estiver recriando o cluster a partir de um nó íntegro.

   ```
   cluster1::*> system configuration recovery cluster show
    Recovery Status: in-progress
    Is Recovery Status Persisted: false
   ```

6. Inicialize cada nó que precisa ser reUnido ao cluster recriado.

   É necessário reinicializar os nós um de cada vez.

7. Para cada nó que precisa ser Unido ao cluster recriado, faça o seguinte:

   a. A partir de um nó íntegro no cluster recriado, junte-se novamente ao nó de destino:

      system configuration recovery cluster rejoin -node *node_name*

      Este exemplo rejura o nó de destino "'node2"" para o cluster recriado:

      ```
      cluster1::*> system configuration recovery cluster rejoin -node node2

      Warning: This command will rejoin node "node2" into the local
               cluster, potentially overwriting critical cluster
               configuration files. This command should only be used
               to recover from a disaster. Do not perform any other
               recovery operations while this operation is in progress.
               This command will cause node "node2" to reboot.
      Do you want to continue? {y|n}: y
      ```

      O nó de destino é reinicializado e, em seguida, se junta ao cluster.

   b. Verifique se o nó de destino está íntegro e formou quórum com o restante dos nós no cluster:

      cluster show -eligibility true

      O nó de destino deve voltar a juntar-se ao cluster recriado antes de poder voltar a aderir a outro nó.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. Se você criou novamente o cluster a partir de um arquivo de backup de configuração, defina o status de recuperação para ser concluído:

   `system configuration recovery cluster modify -recovery-status complete`

9. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

10. Se o cluster consistir em apenas dois nós, use o **`cluster ha modify`** comando para reativar a HA do cluster.
11. Use o **`storage failover modify`** comando para reativar o failover de storage para cada par de HA.

Depois de terminar

Se o cluster tiver relacionamentos de pares SnapMirror, você também precisará recriar esses relacionamentos. Para obter mais informações, "Proteção de dados"consulte .

Sincronize um nó com o cluster

Se houver quorum em todo o cluster, mas um ou mais nós estiverem fora de sincronia com o cluster, será necessário sincronizar o nó para restaurar o banco de dados replicado (RDB) no nó e colocá-lo no quorum.

Passo

1. A partir de um nó saudável, use o `system configuration recovery cluster sync` comando no nível de privilégio avançado para sincronizar o nó que está fora de sincronia com a configuração do cluster.

   Este exemplo sincroniza um nó (*node2*) com o resto do cluster:

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Resultado

O RDB é replicado para o nó e o nó se torna elegível para participar do cluster.

Gerenciar despejos principais (somente administradores de cluster) no ONTAP

Quando um nó entra em pânico, um despejo de núcleo ocorre e o sistema cria um arquivo de despejo de núcleo que o suporte técnico pode usar para solucionar o problema. Você pode configurar ou exibir atributos de despejo de memória. Você também pode salvar, exibir, segmentar, carregar ou excluir um arquivo de despejo de memória.

Você pode gerenciar despejos principais das seguintes maneiras:

- Configurar os despejos principais e exibir as configurações
- Exibindo informações básicas, o status e os atributos dos despejos principais

  Os arquivos e relatórios de despejo de memória são armazenados `/mroot/etc/crash/` no diretório de um nó. Você pode exibir o conteúdo do diretório usando os `system node coredump` comandos ou um navegador da Web.

- Salvando o conteúdo do despejo do núcleo e carregando o arquivo salvo em um local especificado ou no suporte técnico

  O ONTAP impede que você inicie o salvamento de um arquivo de despejo de memória durante uma aquisição, uma realocação agregada ou um giveback.

- Excluindo arquivos de despejo de memória que não são mais necessários

Comandos para gerenciar despejos principais

Você usa os `system node coredump config` comandos para gerenciar a configuração de despejos de núcleo, os `system node coredump` comandos para gerenciar os arquivos de despejo de núcleo e os

`system node coredump reports` comandos para gerenciar relatórios de núcleo de aplicativos.

Saiba mais sobre os comandos descritos neste tópico no "Referência do comando ONTAP".

Se você quiser…	Use este comando…
Configurar despejos de núcleo	`system node coredump config modify`
Apresentar as definições de configuração para despejos de núcleo	`system node coredump config show`
Exibir informações básicas sobre despejos de núcleo	`system node coredump show`
Acione manualmente um despejo de memória quando você reiniciar um nó	`system node reboot` com ambos `-dump` os parâmetros e `-skip-lif-migration-before -reboot` O parâmetro link:https://docs.NetApp.com/US-en/ONTAP-cli//system-node-reboot.html[`skip-lif-migration-before-reboot` especifica que a migração de LIF antes de uma reinicialização será ignorada.
Acione manualmente um despejo de núcleo quando você desligar um nó	`system node halt` com ambos `-dump` os parâmetros e `-skip-lif-migration-before -shutdown` O parâmetro link:https://docs.NetApp.com/US-en/ONTAP-cli/system-node-halt.html[`skip-lif-migration-before-shutdown` especifica que a migração de LIF antes de um desligamento será ignorada.
Salve um despejo de memória especificado	`system node coredump save`
Salve todos os despejos de núcleo não salvos que estão em um nó especificado	`system node coredump save-all`
Gere e envie uma mensagem AutoSupport com um arquivo de despejo de memória que você especificar	`system node autosupport invoke-core-upload` O `-uri` parâmetro opcional especifica um destino alternativo para a mensagem AutoSupport.

Se você quiser…	Use este comando…
Exibir informações de status sobre os despejos do núcleo	`system node coredump status`
Exclua um despejo de memória especificado	`system node coredump delete`
Exclua todos os despejos de núcleo não salvos ou todos os arquivos de núcleo salvos em um nó	`system node coredump delete-all`
Exibir relatórios de despejo do núcleo do aplicativo	`system node coredump reports show`
Excluir um relatório de despejo do núcleo do aplicativo	`system node coredump reports delete`

Informações relacionadas

"Referência do comando ONTAP"

Informações sobre direitos autorais

Informações sobre marcas comerciais