Gerenciamento de serviços iSCSI

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciamento de serviços iSCSI . . . 1
- Gerenciamento de serviços iSCSI . . . 1
- Como a autenticação iSCSI funciona . . . 1
- Gerenciamento de segurança do iniciador iSCSI . . . 2
- Isolamento do ponto de extremidade iSCSI . . . 2
- O que é a autenticação CHAP . . . 2
- Como usar listas de acesso à interface iSCSI para limitar as interfaces do iniciador pode aumentar o desempenho e a segurança . . . 3
- Serviço de nomes de armazenamento de Internet (iSNS) . . . 4

Gerenciamento de serviços iSCSI

Gerenciamento de serviços iSCSI

Você pode gerenciar a disponibilidade do serviço iSCSI nas interfaces lógicas iSCSI da máquina virtual de storage (SVM) usando os `vserver iscsi interface enable` comandos ou `vserver iscsi interface disable`.

Por predefinição, o serviço iSCSI está ativado em todas as interfaces lógicas iSCSI.

Como o iSCSI é implementado no host

O iSCSI pode ser implementado no host usando hardware ou software.

Você pode implementar iSCSI de uma das seguintes maneiras:

- Usando o software Initiator que usa as interfaces Ethernet padrão do host.
- Através de um adaptador de barramento de host iSCSI (HBA): Um HBA iSCSI aparece para o sistema operacional do host como um adaptador de disco SCSI com discos locais.
- Usando um adaptador TOE (TCP Offload Engine) que descarrega o processamento TCP/IP.

  O processamento do protocolo iSCSI ainda é realizado pelo software anfitrião.

Como a autenticação iSCSI funciona

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar uma sessão iSCSI. O sistema de armazenamento permite ou nega a solicitação de login ou determina que não é necessário fazer login.

Os métodos de autenticação iSCSI são:

- Challenge Handshake Authentication Protocol (CHAP) - o iniciador faz login usando um nome de usuário e senha CHAP.

  Você pode especificar uma senha CHAP ou gerar uma senha secreta hexadecimal. Existem dois tipos de nomes de usuário CHAP e senhas:

  - Entrada - o sistema de armazenamento autentica o iniciador.

    As configurações de entrada são necessárias se você estiver usando a autenticação CHAP.

  - Outbound — esta é uma configuração opcional para permitir que o iniciador autentique o sistema de armazenamento.

    Só pode utilizar as definições de saída se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento.

- Negar - o iniciador tem acesso negado ao sistema de armazenamento.

- Nenhum - o sistema de storage não requer autenticação para o iniciador.

Pode definir a lista de iniciadores e os respetivos métodos de autenticação. Você também pode definir um método de autenticação padrão que se aplica a iniciadores que não estão nesta lista.

Informações relacionadas

"Opções de multipathing do Windows com Data ONTAP: Fibre Channel e iSCSI"

Gerenciamento de segurança do iniciador iSCSI

O ONTAP fornece uma série de recursos para gerenciar a segurança para iniciadores iSCSI. Pode definir uma lista de iniciadores iSCSI e o método de autenticação para cada um, apresentar os iniciadores e os respetivos métodos de autenticação associados na lista de autenticação, adicionar e remover iniciadores da lista de autenticação e definir o método de autenticação do iniciador iSCSI predefinido para iniciadores que não estão na lista.

Isolamento do ponto de extremidade iSCSI

A partir do ONTAP 9.1, os comandos de segurança iSCSI existentes foram melhorados para aceitar um intervalo de endereços IP ou vários endereços IP.

Todos os iniciadores iSCSI devem fornecer endereços IP de origem ao estabelecer uma sessão ou conexão com um destino. Essa nova funcionalidade impede que um iniciador faça login no cluster se o endereço IP de origem não for suportado ou desconhecido, fornecendo um esquema de identificação exclusivo. Qualquer iniciador originado de um endereço IP não suportado ou desconhecido terá seu login rejeitado na camada de sessão iSCSI, impedindo que o iniciador acesse qualquer LUN ou volume dentro do cluster.

Implemente essa nova funcionalidade com dois novos comandos para ajudar a gerenciar entradas pré-existentes.

Adicionar intervalo de endereços do iniciador

Melhore o gerenciamento de segurança do iniciador iSCSI adicionando um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Remova o intervalo de endereços do iniciador

Remova um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

O que é a autenticação CHAP

O CHAP (Challenge Handshake Authentication Protocol) permite a comunicação autenticada entre iniciadores e destinos iSCSI. Quando você usa autenticação CHAP,

você define nomes de usuário CHAP e senhas tanto no iniciador quanto no sistema de armazenamento.

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar a sessão. A solicitação de login inclui o nome de usuário CHAP do iniciador e o algoritmo CHAP. O sistema de armazenamento responde com um desafio CHAP. O iniciador fornece uma resposta CHAP. O sistema de armazenamento verifica a resposta e autentica o iniciador. A senha CHAP é usada para calcular a resposta.

Diretrizes para o uso da autenticação CHAP

Você deve seguir certas diretrizes ao usar a autenticação CHAP.

- Se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de saída no iniciador. Se também definir um nome de utilizador e uma palavra-passe de saída no sistema de armazenamento para ativar a autenticação bidirecional, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de entrada no iniciador.
- Você não pode usar o mesmo nome de usuário e senha para configurações de entrada e saída no sistema de armazenamento.
- Os nomes de usuário CHAP podem ser de 1 a 128 bytes.

  Um nome de usuário nulo não é permitido.

- As senhas CHAP (segredos) podem ter 1 a 512 bytes.

  As senhas podem ser valores hexadecimais ou strings. Para valores hexadecimais, você deve inserir o valor com um prefixo "'0x'" ou "'0x'". Não é permitida uma palavra-passe nula.

> O ONTAP permite o uso de carateres especiais, letras não inglesas, números e espaços para senhas CHAP (segredos). No entanto, isso está sujeito a restrições de host. Se algum destes não for permitido pelo seu anfitrião específico, não poderão ser utilizados.
>
> Por exemplo, o iniciador de software iSCSI da Microsoft requer que as senhas CHAP do iniciador e do destino tenham pelo menos 12 bytes se a criptografia IPsec não estiver sendo usada. O comprimento máximo da senha é de 16 bytes, independentemente de o IPsec ser usado.
>
> Para restrições adicionais, você deve ver a documentação do iniciador.

Como usar listas de acesso à interface iSCSI para limitar as interfaces do iniciador pode aumentar o desempenho e a segurança

As listas de acesso à interface ISCSI podem ser usadas para limitar o número de LIFs em uma SVM que um iniciador pode acessar, aumentando assim a performance e a segurança.

Quando um iniciador inicia uma sessão de descoberta usando um comando iSCSI `SendTargets`, ele recebe os endereços IP associados ao LIF (interface de rede) que está na lista de acesso. Por padrão, todos os

iniciadores têm acesso a todas as LIFs iSCSI na SVM. Você pode usar a lista de acesso para restringir o número de LIFs em uma SVM a que um iniciador tem acesso.

Serviço de nomes de armazenamento de Internet (iSNS)

O iSNS (Internet Storage Name Service) é um protocolo que permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento TCP/IP. Um servidor iSNS mantém informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI IQN e grupos de portais.

Você pode obter um servidor iSNS de um fornecedor terceirizado. Se você tiver um servidor iSNS na rede configurado e habilitado para uso pelo iniciador e destino, poderá usar o LIF de gerenciamento de uma máquina virtual de armazenamento (SVM) para Registrar todos os LIFs iSCSI para esse SVM no servidor iSNS. Depois que o Registro estiver concluído, o iniciador iSCSI pode consultar o servidor iSNS para descobrir todos os LIFs para esse SVM específico.

Se você decidir usar um serviço iSNS, deve garantir que suas máquinas virtuais de armazenamento (SVMs) estejam registradas corretamente em um servidor iSNS (Internet Storage Name Service).

Se você não tiver um servidor iSNS na rede, você deverá configurar manualmente cada destino para ser visível para o host.

O que um servidor iSNS faz

Um servidor iSNS usa o protocolo iSNS (Internet Storage Name Service) para manter informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI (IQNs) e grupos de portais.

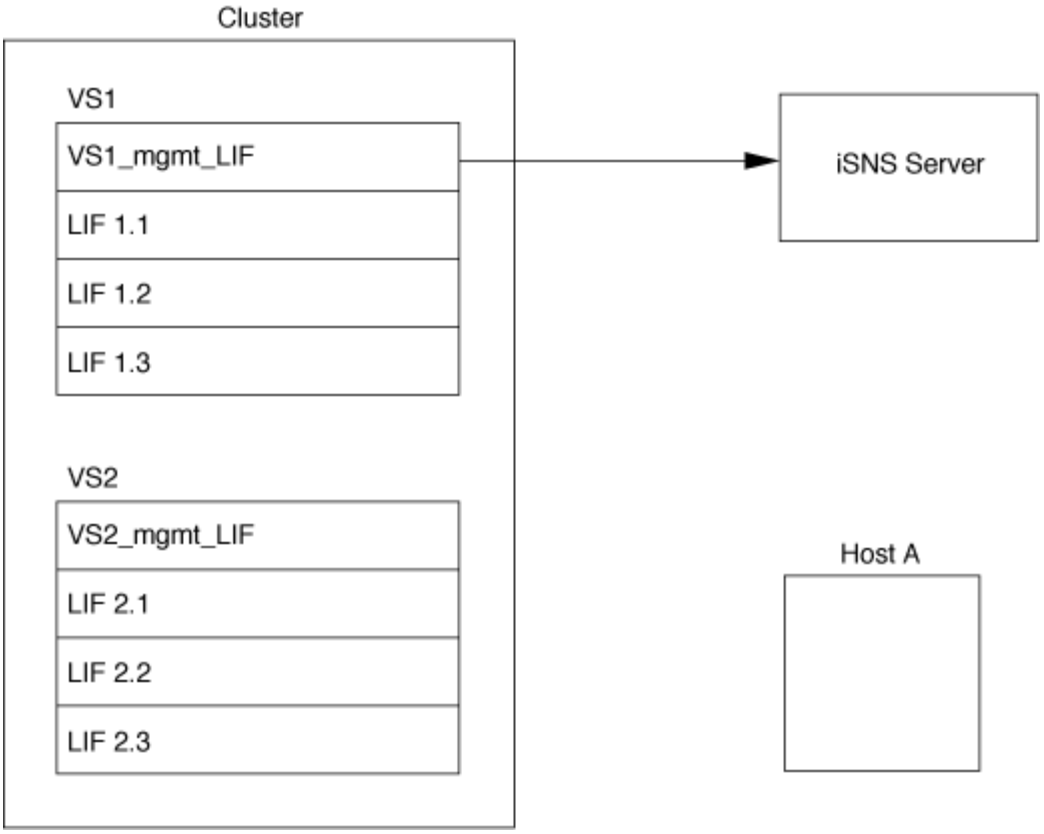
O protocolo iSNS permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento IP. Um iniciador iSCSI pode consultar o servidor iSNS para descobrir dispositivos de destino iSCSI.

A NetApp não fornece ou revender servidores iSNS. Você pode obter esses servidores de um fornecedor suportado pelo NetApp.

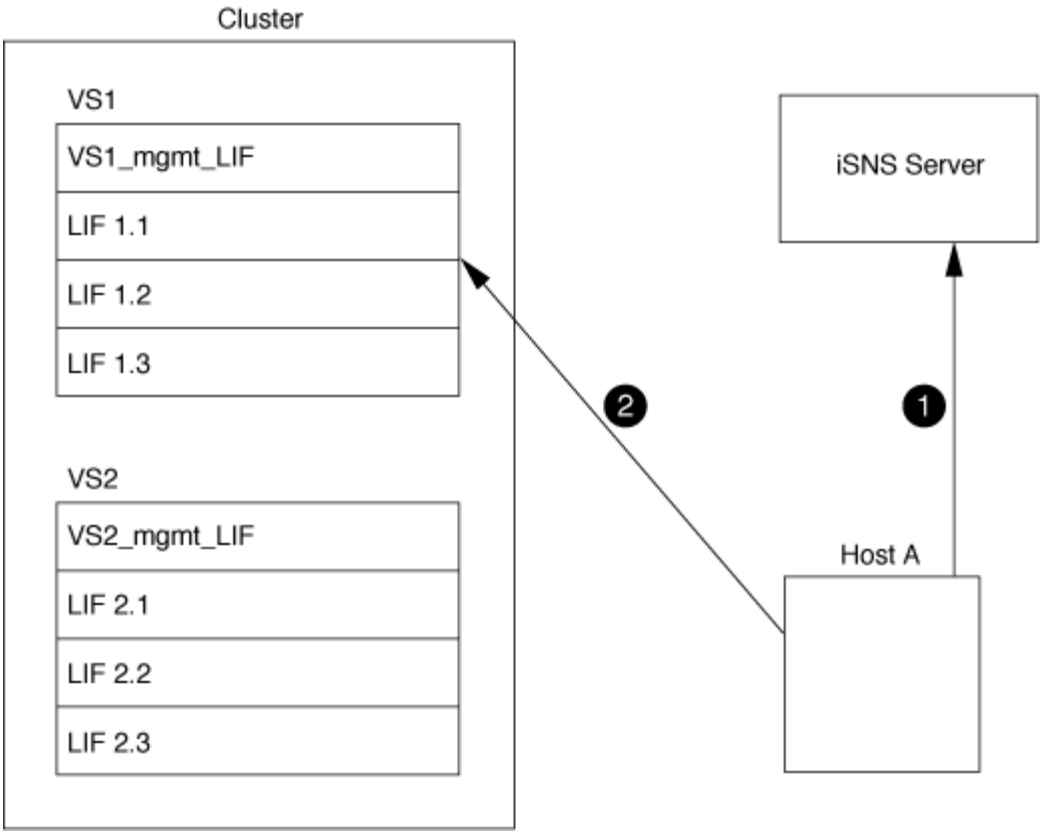
Como os SVMs interagem com um servidor iSNS

O servidor iSNS se comunica com cada máquina virtual de storage (SVM) por meio do LIF de gerenciamento do SVM. O LIF de gerenciamento Registra todos os nomes, alias e informações do portal do nó de destino iSCSI com o serviço iSNS para um SVM específico.

No exemplo a seguir, o SVM "'VS1'" usa o gerenciamento de SVM LIF "'VS1_mgmt_lif" para se Registrar no servidor iSNS. Durante o Registro do iSNS, um SVM envia todas as LIFs iSCSI por meio do LIF de gerenciamento do SVM para o iSNS Server. Depois que o Registro do iSNS for concluído, o servidor iSNS tem uma lista de todos os LIFs que servem iSCSI em "'VS1"". Se um cluster contiver vários SVMs, cada SVM precisará se Registrar individualmente no servidor iSNS para usar o serviço iSNS.



No próximo exemplo, depois que o servidor iSNS concluir o Registro com o destino, o Host A pode descobrir todos os LIFs para "'VS1" através do servidor iSNS, conforme indicado na Etapa 1. Depois que o Host A concluir a descoberta dos LIFs para "'VS1"", o Host A pode estabelecer uma conexão com qualquer um dos LIFs em "'VS1"", como mostrado na Etapa 2. O host A não está ciente de nenhum dos LIFs em "'VS2" até que o LIF de gerenciamento "'VS2_mgmt_LIF" para Registros "'VS2" com o servidor iSNS.



No entanto, se você definir as listas de acesso à interface, o host só poderá usar as LIFs definidas na lista de acesso à interface para acessar o destino.

Depois que o iSNS for configurado inicialmente, o ONTAP atualizará automaticamente o servidor iSNS quando as configurações do SVM mudarem.

Pode ocorrer um atraso de alguns minutos entre o momento em que você faz as alterações de configuração e quando o ONTAP envia a atualização para o servidor iSNS. Forçar uma atualização imediata das informações do iSNS no servidor iSNS: `vserver iscsi isns update`

Comandos para gerenciar iSNS

O ONTAP fornece comandos para gerenciar seu serviço iSNS.

Se você quiser…	Use este comando…
Configurar um serviço iSNS	`vserver iscsi isns create`
Inicie um serviço iSNS	`vserver iscsi isns start`
Modifique um serviço iSNS	`vserver iscsi isns modify`
Exibir a configuração do serviço iSNS	`vserver iscsi isns show`
Forçar uma atualização das informações do iSNS registradas	`vserver iscsi isns update`

Pare um serviço iSNS	`vserver iscsi isns stop`
Remova um serviço iSNS	`vserver iscsi isns delete`
Veja a página de manual para um comando	`man` *`command name`*

Consulte a página de manual de cada comando para obter mais informações.

Informações sobre direitos autorais

Informações sobre marcas comerciais