iSCSI-Service-Management

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/san-admin/iscsi-service-management-system-interfaces-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

iSCSI-Service-Management . . . 1
- Informationen zur Verwaltung des iSCSI-Service in ONTAP . . . 1
  - Wie iSCSI auf dem Host implementiert ist . . . 1
- Wie die iSCSI-Authentifizierung in ONTAP funktioniert . . . 1
- Informationen zum Sicherheitsmanagement von iSCSI-Initiatoren in ONTAP . . . 2
- Informationen zur iSCSI-Endpunktisolierung in ONTAP . . . 2
  - Initiator-Adressbereich hinzufügen . . . 2
  - Initiator-Adressbereich entfernen . . . 2
- Informationen zur CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP . . . 3
  - Richtlinien für die Verwendung der CHAP-Authentifizierung . . . 4
- Wie ONTAP iSCSI Schnittstellenzugriffslisten die Performance und Sicherheit verbessern . . . 4
- iSNS in ONTAP . . . 5
  - Was ein iSNS-Server tut . . . 5
  - Wie SVMs mit einem iSNS-Server interagieren . . . 5
  - Befehle zur Verwaltung von iSNS . . . 7

iSCSI-Service-Management

Informationen zur Verwaltung des iSCSI-Service in ONTAP

Die Verfügbarkeit des iSCSI-Service auf den iSCSI-Logischen Schnittstellen der Storage Virtual Machine (SVM) kann mit den `vserver iscsi interface enable`- oder `vserver iscsi interface disable`-Befehlen verwaltet werden.

Standardmäßig ist der iSCSI-Service auf allen iSCSI-Logischen Schnittstellen aktiviert.

Wie iSCSI auf dem Host implementiert ist

iSCSI kann auf dem Host mit Hardware oder Software implementiert werden.

iSCSI kann auf eine der folgenden Arten implementiert werden:

- Verwendung von Initiator-Software, die die Standard-Ethernet-Schnittstellen des Hosts verwendet.
- Über einen iSCSI Hostbusadapter (HBA): Ein iSCSI HBA erscheint dem Host-Betriebssystem als SCSI-Festplattenadapter mit lokalen Festplatten.
- Verwendung eines TCP Offload Engine (TOE) Adapters, der die TCP/IP-Verarbeitung auslagert.

  Die Verarbeitung des iSCSI-Protokolls erfolgt weiterhin durch die Host-Software.

Wie die iSCSI-Authentifizierung in ONTAP funktioniert

In der Anfangsphase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanfrage an das Speichersystem, um eine iSCSI-Sitzung zu beginnen. Das Speichersystem genehmigt oder verweigert anschließend die Anmeldeanfrage oder stellt fest, dass keine Anmeldung erforderlich ist.

iSCSI-Authentifizierungsverfahren sind:

- Challenge Handshake Authentication Protocol (CHAP): Der Initiator meldet sich mit einem CHAP-Benutzernamen und Passwort an.

  Sie können ein CHAP-Passwort festlegen oder ein hexadezimales geheimes Passwort generieren. Es gibt zwei Arten von CHAP-Benutzernamen und Passwörtern:

  - Eingehend, das Speichersystem authentifiziert den Initiator.

    Eingangseinstellungen sind erforderlich, wenn Sie die CHAP-Authentifizierung verwenden.

  - Ausgehend, dies ist eine optionale Einstellung, um dem Initiator die Authentifizierung des Speichersystems zu ermöglichen.

    Ausgehende Einstellungen können nur verwendet werden, wenn im Speichersystem ein eingehender Benutzername und ein Passwort definiert sind.

- deny—Dem Initiator wird der Zugriff auf das Speichersystem verweigert.

- keine, das Speichersystem erfordert keine Authentifizierung für den Initiator.

Sie können die Liste der Initiatoren und deren Authentifizierungsverfahren definieren. Es kann auch ein Standard-Authentifizierungsverfahren definiert werden, das für Initiatoren gilt, die nicht in dieser Liste enthalten sind.

Verwandte Informationen

"Windows Multipathing Optionen mit Data ONTAP: Fibre Channel und iSCSI"

Informationen zum Sicherheitsmanagement von iSCSI-Initiatoren in ONTAP

ONTAP bietet zahlreiche Funktionen zur Verwaltung der Sicherheit für iSCSI-Initiatoren. Es ist möglich, eine Liste von iSCSI-Initiatoren und das jeweilige Authentifizierungsverfahren für jeden Initiator zu definieren, die Initiatoren und ihre zugehörigen Authentifizierungsverfahren in der Authentifizierungsliste anzuzeigen, Initiatoren zur Authentifizierungsliste hinzuzufügen oder daraus zu entfernen sowie das Standard-Authentifizierungsverfahren für iSCSI-Initiatoren festzulegen, die nicht in der Liste enthalten sind.

Informationen zur iSCSI-Endpunktisolierung in ONTAP

Die bestehenden iSCSI-Sicherheitsbefehle können einen IP-Adressbereich oder mehrere IP-Adressen akzeptieren.

Alle iSCSI-Initiatoren müssen beim Aufbau einer Sitzung oder Verbindung mit einem Ziel ihre Ursprungs-IP-Adresse angeben. Diese neue Funktion verhindert, dass sich ein Initiator im Cluster anmeldet, wenn die Ursprungs-IP-Adresse nicht unterstützt wird oder unbekannt ist, und stellt ein eindeutiges Identifizierungsschema bereit. Jeder Initiator, der von einer nicht unterstützten oder unbekannten IP-Adresse stammt, wird auf der iSCSI-Sitzungsschicht bei der Anmeldung abgewiesen, sodass der Initiator keinen Zugriff auf LUNs oder Volumes innerhalb des Clusters erhält.

Diese neue Funktionalität wird mit zwei neuen Befehlen implementiert, die bei der Verwaltung bereits vorhandener Einträge unterstützen.

Initiator-Adressbereich hinzufügen

Die Sicherheitsverwaltung des iSCSI-Initiators lässt sich verbessern, indem ein IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security add-initiator-address-range` Befehl hinzugefügt werden.

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

Initiator-Adressbereich entfernen

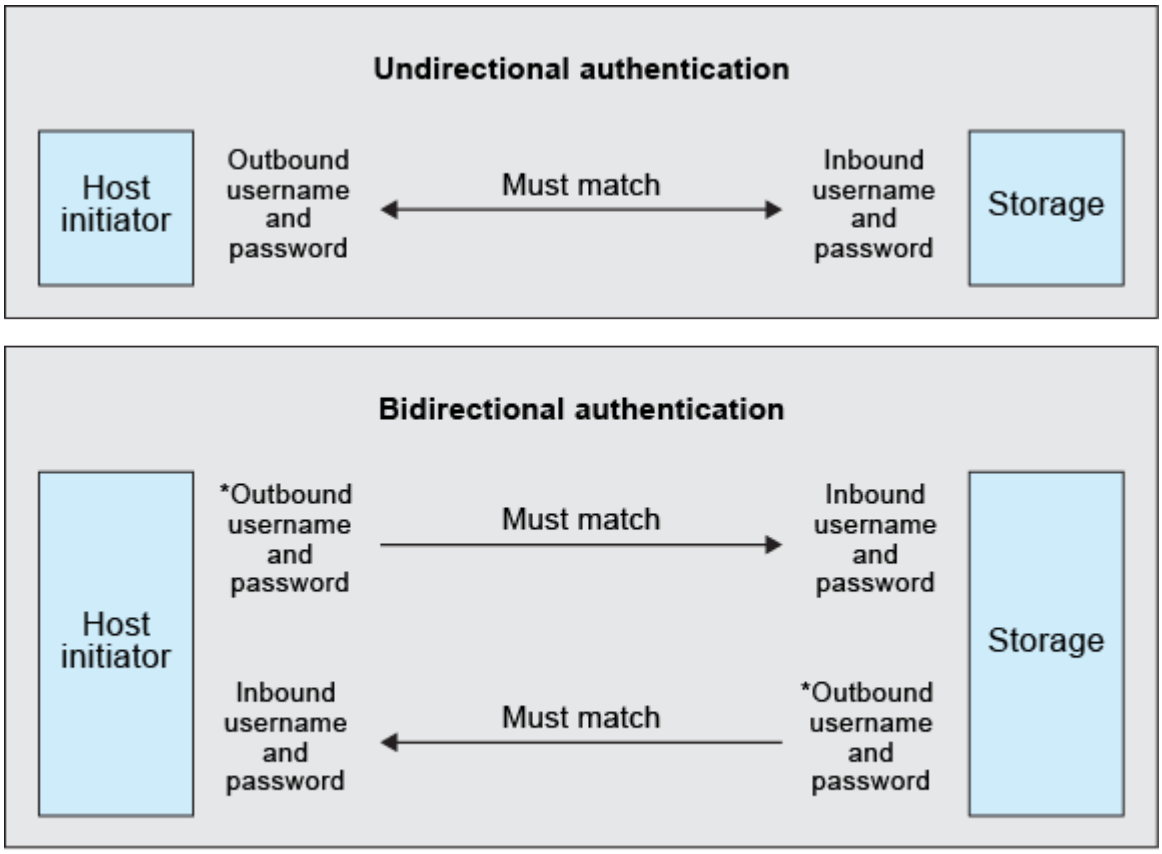
Einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security remove-initiator-address-range` Befehl entfernen.

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

Informationen zur CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP

Das Challenge Handshake Authentication Protocol (CHAP) ermöglicht die authentifizierte Kommunikation zwischen iSCSI-Initiatoren und Zielen. Bei Verwendung der CHAP-Authentifizierung werden CHAP-Benutzernamen und -Passwörter sowohl auf dem Initiator als auch auf dem Speichersystem definiert.

In der Initialisierungsphase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanfrage an das Speichersystem, um die Sitzung zu beginnen. Die Anmeldeanfrage enthält den CHAP-Benutzernamen des Initiators und den CHAP-Algorithmus. Das Speichersystem antwortet mit einer CHAP-Herausforderung. Der Initiator gibt eine CHAP-Antwort an. Das Speichersystem überprüft die Antwort und authentifiziert den Initiator. Das CHAP-Passwort wird zur Berechnung der Antwort verwendet.



Authentifizierung	Ausgehend	Eingehend	Übereinstimmung?
Unidirektional	Benutzername und Passwort des Host-Initiators	Benutzername und Passwort für Storage	Muss übereinstimmen
Bidirektional	Benutzername und Passwort des Host-Initiators	Benutzername und Passwort für Storage	Muss übereinstimmen
Bidirektional	Benutzername und Passwort für Storage	Benutzername und Passwort des Host-Initiators	Muss übereinstimmen

Der Benutzername und das Passwort für den ausgehenden Host-Initiator müssen sich von dem Benutzernamen und dem Passwort für das Speichersystem unterscheiden.

Richtlinien für die Verwendung der CHAP-Authentifizierung

Diese Richtlinien sind bei der Verwendung der CHAP-Authentifizierung zu beachten.

- Wenn auf dem Speichersystem ein Benutzername und ein Passwort für eingehende Verbindungen definiert werden, müssen derselbe Benutzername und dasselbe Passwort für die ausgehenden CHAP-Einstellungen auf dem Initiator verwendet werden. Wenn auf dem Speichersystem zusätzlich ein Benutzername und ein Passwort für ausgehende Verbindungen definiert werden, um die bidirektionale Authentifizierung zu ermöglichen, müssen derselbe Benutzername und dasselbe Passwort für die eingehenden CHAP-Einstellungen auf dem Initiator verwendet werden.
- Sie können nicht denselben Benutzernamen und dasselbe Passwort für die Einstellungen für eingehende und ausgehende Verbindungen im Speichersystem verwenden.
- CHAP-Benutzernamen können zwischen 1 und 128 Byte lang sein.

  Das System lässt keine leeren Benutzernamen zu.

- CHAP-Passwörter (Geheimnisse) können 1 bis 512 Byte lang sein.

  Passwörter können Hexadezimalwerte oder Zeichenketten sein. Bei Hexadezimalwerten sollte der Wert mit dem Präfix “0x” oder “0X” eingegeben werden.

  Das System lässt kein leeres Passwort zu.

> ONTAP erlaubt die Verwendung von Sonderzeichen, nicht-englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Geheimnisse). Dies unterliegt jedoch den Einschränkungen des Hosts. Wenn einer dieser Werte von Ihrem spezifischen Host nicht erlaubt ist, können sie nicht verwendet werden.
>
> Beispielsweise erfordert der Microsoft iSCSI Softwareinitiator, dass sowohl das Initiator- als auch das Ziel-CHAP-Passwort mindestens 12 Byte lang sind, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Passwortlänge beträgt unabhängig davon, ob IPsec verwendet wird, 16 Byte.
>
> Zusätzliche Einschränkungen sind in der Dokumentation des Initiators aufgeführt.

Wie ONTAP iSCSI Schnittstellenzugriffslisten die Performance und Sicherheit verbessern

ISCSI-Schnittstellenzugriffslisten können verwendet werden, um die Anzahl der LIFs in einer SVM zu begrenzen, auf die ein Initiator zugreifen kann, wodurch Leistung und Sicherheit erhöht werden.

Wenn ein Initiator eine Erkennungssitzung mit einem iSCSI `SendTargets` Befehl startet, erhält er die IP-Adressen, die der LIF (Netzwerkschnittstelle) zugeordnet sind und sich in der Zugriffsliste befindet. Standardmäßig haben alle Initiatoren Zugriff auf alle iSCSI LIFs in der SVM. Mit der Zugriffsliste kann die Anzahl der LIFs in der SVM, auf die ein Initiator Zugriff hat, eingeschränkt werden.

iSNS in ONTAP

Der Internet Storage Name Service (iSNS) ist ein Protokoll, das die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem TCP/IP-Speichernetzwerk ermöglicht. Ein iSNS-Server verwaltet Informationen über aktive iSCSI-Geräte im Netzwerk, einschließlich ihrer IP-Adressen, iSCSI-Node-Namen (IQNs) und Portalgruppen.

Sie können einen iSNS-Server von einem Drittanbieter beziehen. Wenn Sie in Ihrem Netzwerk einen iSNS-Server konfiguriert und für die Verwendung durch Initiator und Ziel aktiviert haben, kann die Management-LIF einer Storage Virtual Machine (SVM) verwendet werden, um alle iSCSI-LIFs dieser SVM auf dem iSNS-Server zu registrieren. Nach Abschluss der Registrierung kann der iSCSI-Initiator den iSNS-Server abfragen, um alle LIFs für diese SVM zu ermitteln.

Wenn Sie sich für die Nutzung eines iSNS-Service entscheiden, muss sichergestellt sein, dass Ihre Storage Virtual Machines (SVMs) ordnungsgemäß bei einem Internet Storage Name Service (iSNS) Server registriert sind.

Falls kein iSNS-Server im Netzwerk vorhanden ist, muss jedes Ziel manuell so konfiguriert werden, dass es für den Host sichtbar ist.

Was ein iSNS-Server tut

Ein iSNS Server verwendet das Internet Storage Name Service (iSNS) Protokoll, um Informationen über aktive iSCSI-Geräte im Netzwerk zu verwalten, einschließlich ihrer IP-Adressen, iSCSI-Node-Namen (IQNs) und Portalgruppen.

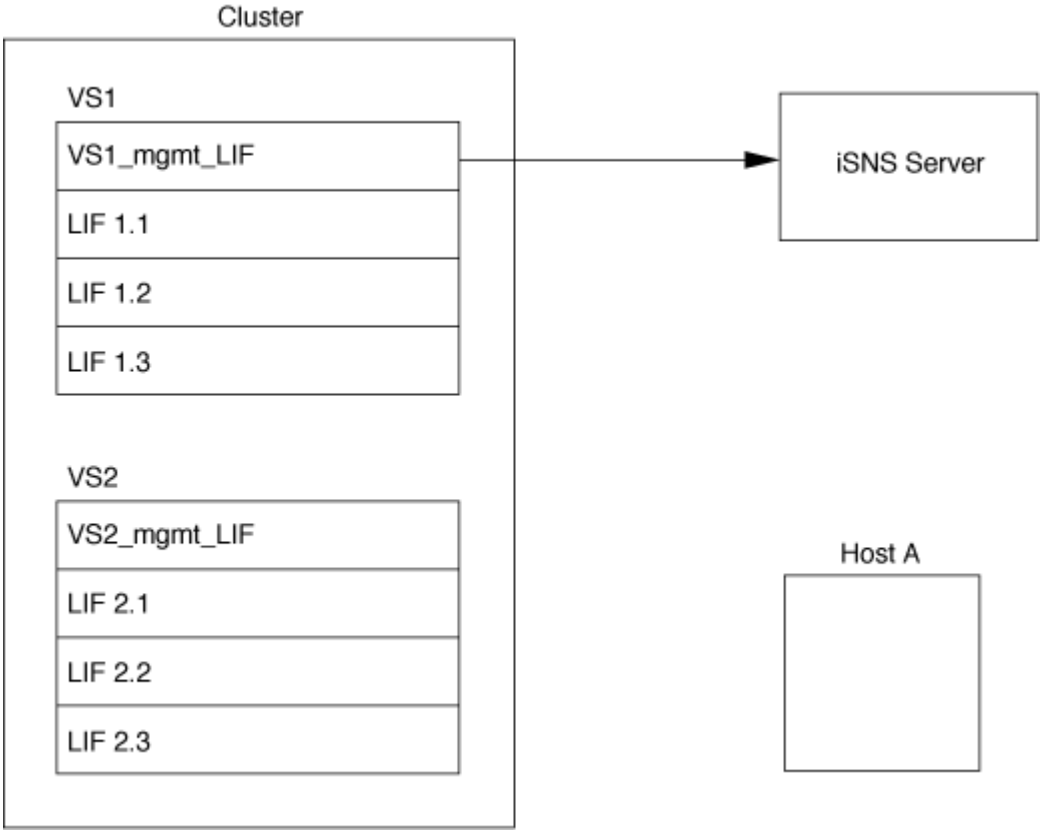
Das iSNS-Protokoll ermöglicht die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem IP-Speichernetzwerk. Ein iSCSI-Initiator kann den iSNS-Server abfragen, um iSCSI-Zielgeräte zu entdecken.

NetApp liefert oder vertreibt keine iSNS-Server. Sie können diese Server von einem von NetApp unterstützten Anbieter beziehen.

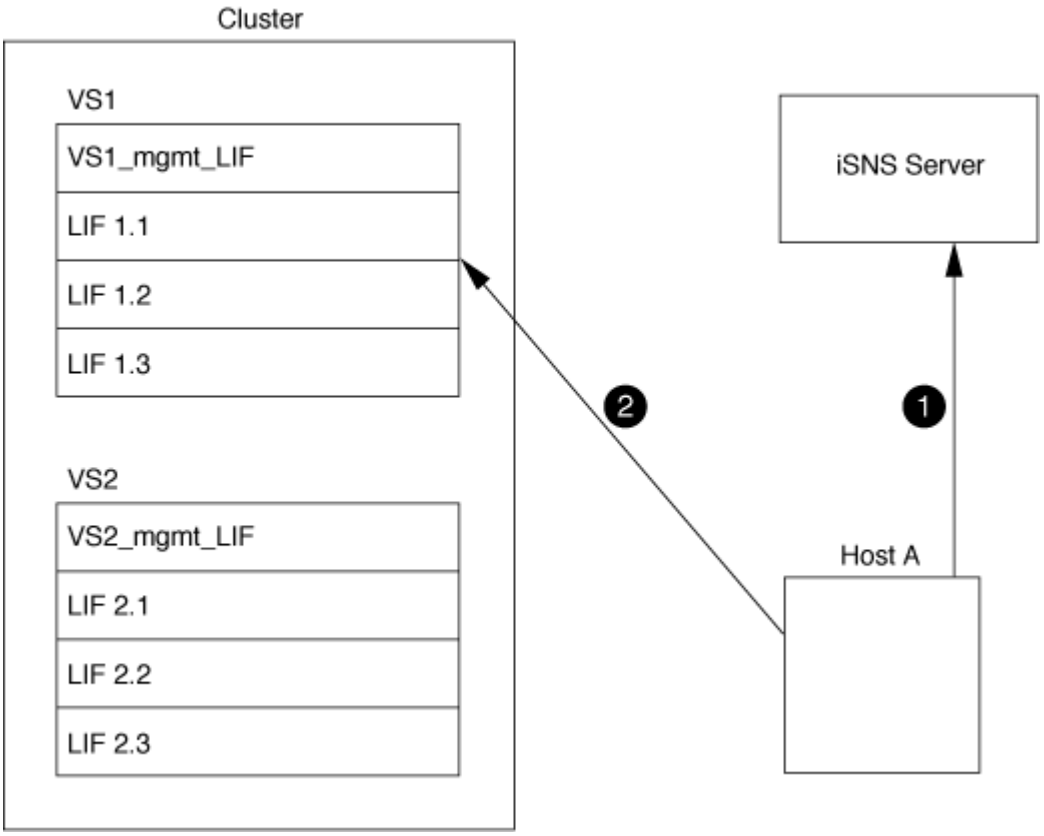
Wie SVMs mit einem iSNS-Server interagieren

Der iSNS-Server kommuniziert mit jeder Storage Virtual Machine (SVM) über die SVM-Management-LIF. Die Management-LIF registriert alle iSCSI-Ziel Node-Name, Alias und Portalinformationen beim iSNS-Service für eine bestimmte SVM.

Im folgenden Beispiel verwendet die SVM „`VS1`“ die SVM Management LIF „`VS1_mgmt_lif`“, um sich beim iSNS Server zu registrieren. Während der iSNS-Registrierung sendet eine SVM alle iSCSI LIFs über die SVM Management LIF an den iSNS Server. Nach Abschluss der iSNS-Registrierung verfügt der iSNS Server über eine Liste aller LIFs, die iSCSI in „`VS1`“ bereitstellen. Wenn ein Cluster mehrere SVMs enthält, muss sich jede SVM einzeln beim iSNS Server registrieren, um den iSNS Service zu nutzen.



Im nächsten Beispiel kann Host A, nachdem der iSNS-Server die Registrierung beim Ziel abgeschlossen hat, alle LIFs für „VS1“ über den iSNS-Server ermitteln, wie in Schritt 1 angegeben. Nachdem Host A die LIFs für „VS1“ ermittelt hat, kann Host A eine Verbindung zu jeder beliebigen LIF in „VS1“ herstellen, wie in Schritt 2 gezeigt. Host A kennt keine der LIFs in „VS2“, bis die Management-LIF „VS2_mgmt_LIF“ für „VS2“ sich beim iSNS-Server registriert hat.



Wenn Sie jedoch die Schnittstellenzugriffslisten definieren, kann der Host nur die in der Schnittstellenzugriffsliste definierten LIFs verwenden, um auf das Ziel zuzugreifen.

Nach der Erstkonfiguration von iSNS aktualisiert ONTAP den iSNS-Server automatisch, wenn sich die SVM-Konfigurationseinstellungen ändern.

Zwischen dem Zeitpunkt, zu dem Sie die Konfigurationsänderungen vornehmen, und dem Versand der Aktualisierung durch ONTAP an den iSNS-Server kann eine Verzögerung von einigen Minuten auftreten. Eine sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server kann erzwungen werden: `vserver iscsi isns update`. Weitere Informationen zu `vserver iscsi isns update` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung von iSNS

ONTAP stellt Befehle zur Verwaltung Ihres iSNS-Dienstes bereit.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Konfiguration eines iSNS-Dienstes	`vserver iscsi isns create`
Einen iSNS-Dienst starten	`vserver iscsi isns start`
Einen iSNS Dienst modifizieren	`vserver iscsi isns modify`
iSNS-Dienstkonfiguration anzeigen	`vserver iscsi isns show`
Eine Aktualisierung der registrierten iSNS-Informationen erzwingen	`vserver iscsi isns update`
Einen iSNS-Dienst beenden	`vserver iscsi isns stop`

Einen iSNS Dienst entfernen	`vserver iscsi isns delete`
Die Manpage für einen Befehl anzeigen	`man command name`

Weitere Informationen zu `vserver iscsi isns` finden sich in der "ONTAP-Befehlsreferenz".

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.