



ISCSI-Service-Management

ONTAP 9

NetApp
January 08, 2026

Inhalt

ISCSI-Service-Management	1
ISCSI-Service-Management	1
Wie iSCSI auf dem Host implementiert wird	1
Funktionsweise der iSCSI-Authentifizierung	1
Verwalten der iSCSI-Initiator-Sicherheit	2
Isolierung von iSCSI-Endpunkten	2
Fügen Sie den Adressbereich des Initiators hinzu	2
Entfernen Sie den Adressbereich des Initiators	2
Erfahren Sie mehr über die CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP	3
Richtlinien für die Verwendung der CHAP-Authentifizierung	4
Die Verwendung von Zugriffslisten für iSCSI-Schnittstellen zur Begrenzung von Initiator-Schnittstellen kann Performance und Sicherheit erhöhen	4
Internet Storage Name Service (iSNS) in ONTAP	5
Was macht ein iSNS-Server	5
Interaktion von SVMs mit einem iSNS-Server	5
Befehle zum Verwalten von iSNS	7

ISCSI-Service-Management

ISCSI-Service-Management

Sie können die Verfügbarkeit des iSCSI-Dienstes auf den logischen iSCSI-Schnittstellen der SVM (Storage Virtual Machine) mit den `vserver iscsi interface enable` `vserver iscsi interface disable` Befehlen oder managen.

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

Wie iSCSI auf dem Host implementiert wird

iSCSI kann auf dem Host mithilfe von Hardware oder Software implementiert werden.

Sie können iSCSI auf eine der folgenden Arten implementieren:

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

Die iSCSI-Protokollverarbeitung wird weiterhin von der Host-Software durchgeführt.

Funktionsweise der iSCSI-Authentifizierung

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um eine iSCSI-Sitzung zu starten. Das Storage-System erlaubt dann entweder die Login-Anfrage oder lehnt sie ab oder stellt fest, dass keine Anmeldung erforderlich ist.

iSCSI-Authentifizierungsmethoden:

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

Sie können ein CHAP-Kennwort festlegen oder ein hexadezimalen Geheimkennwort generieren. Es gibt zwei Typen von CHAP-Benutzernamen und -Passwörtern:

- Inbound – das Storage-System authentifiziert den Initiator.

Eingehende Einstellungen sind erforderlich, wenn Sie die CHAP-Authentifizierung verwenden.

- Outbound – Dies ist eine optionale Einstellung, die es dem Initiator ermöglicht, das Speichersystem zu authentifizieren.

Sie können Outbound-Einstellungen nur verwenden, wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren.

- Deny- der Initiator wird dem Zugriff auf das Speichersystem verweigert.

- Keine – das Storage-System erfordert keine Authentifizierung für den Initiator.

Sie können die Liste der Initiatoren und deren Authentifizierungsmethoden definieren. Sie können auch eine Standardauthentifizierungsmethode definieren, die für Initiatoren gilt, die nicht in dieser Liste enthalten sind.

Verwandte Informationen

["Multipathing-Optionen für Windows mit Data ONTAP: Fibre Channel und iSCSI"](#)

Verwalten der iSCSI-Initiator-Sicherheit

ONTAP bietet eine Reihe von Funktionen zum Verwalten der Sicherheit für iSCSI-Initiatoren. Sie können eine Liste der iSCSI-Initiatoren und die Authentifizierungsmethode für jeden definieren, die Initiatoren und ihre zugehörigen Authentifizierungsmethoden in der Authentifizierungsliste anzeigen, Initiatoren aus der Authentifizierungsliste hinzufügen oder entfernen sowie die Standard-Authentifizierungsmethode für iSCSI-Initiatoren definieren, die nicht in der Liste enthalten sind.

Isolierung von iSCSI-Endpunkten

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

Alle iSCSI-Initiatoren müssen die Ursprung-IP-Adressen bereitstellen, wenn eine Sitzung oder Verbindung zu einem Ziel eingerichtet wird. Durch diese neue Funktion wird verhindert, dass sich ein Initiator beim Cluster anmelden kann, wenn die Ursprung-IP-Adresse nicht unterstützt oder unbekannt ist und somit ein eindeutiges Identifikationsschema bereitgestellt wird. Jeder Initiator, der von einer nicht unterstützten oder unbekannten IP-Adresse stammt, wird seine Anmeldung auf der iSCSI-Sitzungsebene abgelehnt. Dies verhindert, dass der Initiator auf beliebige LUNs oder Volumes innerhalb des Clusters zugreift.

Implementieren Sie diese neue Funktion mit zwei neuen Befehlen, um bereits vorhandene Einträge zu verwalten.

Fügen Sie den Adressbereich des Initiators hinzu

Verbessern Sie die Sicherheitsverwaltung von iSCSI-Initiatoren, indem Sie einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security add-initiator-address-range` Befehl hinzufügen.

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

Entfernen Sie den Adressbereich des Initiators

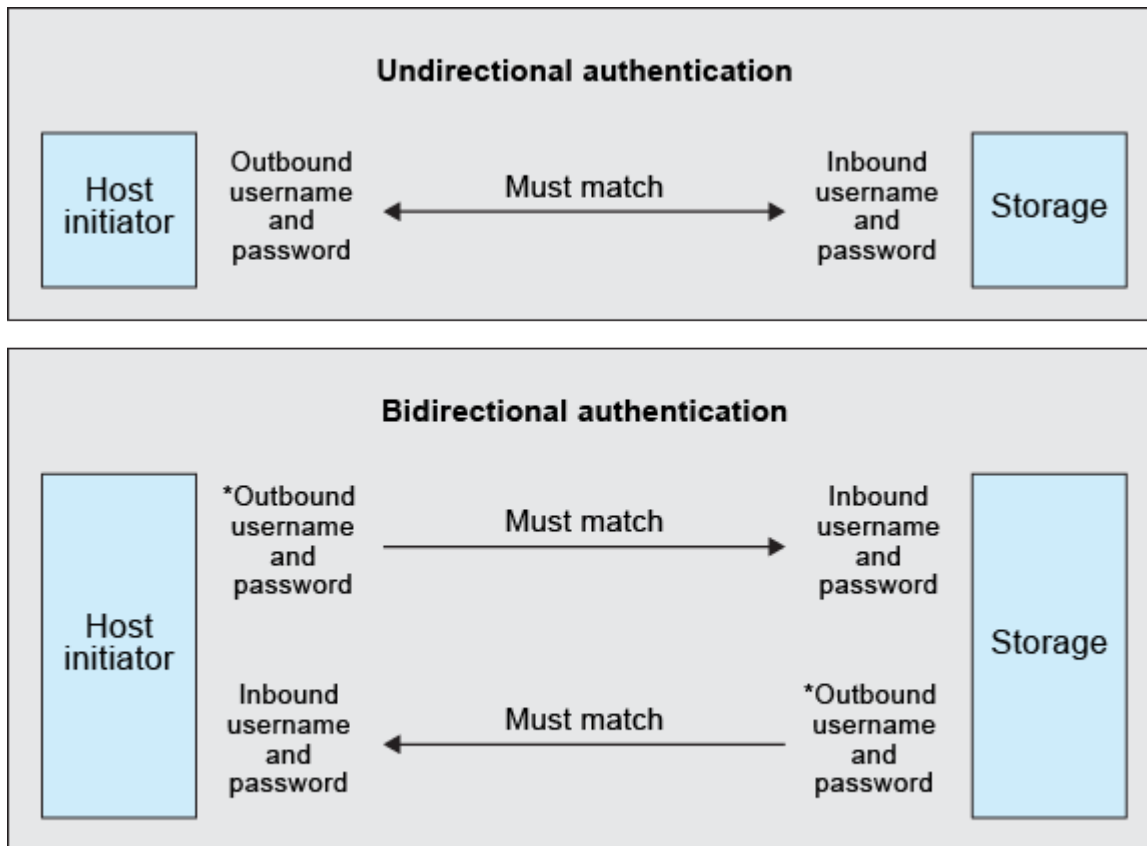
Entfernen Sie einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security remove-initiator-address-range` Befehl.

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

Erfahren Sie mehr über die CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP

Das Challenge Handshake Authentication Protocol (CHAP) ermöglicht die authentifizierte Kommunikation zwischen iSCSI-Initiatoren und Zielen. Wenn Sie CHAP-Authentifizierung verwenden, definieren Sie sowohl auf dem Initiator als auch auf dem Speichersystem CHAP-Benutzernamen und -Kennwörter.

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um die Sitzung zu starten. Die Anmeldeanforderung umfasst den CHAP-Benutzernamen und den CHAP-Algorithmus des Initiators. Das Speichersystem reagiert mit einer CHAP-Herausforderung. Der Initiator liefert eine CHAP-Antwort. Das Storage-System überprüft die Antwort und authentifiziert den Initiator. Das CHAP-Passwort wird zur Berechnung der Antwort verwendet.



*The outbound username and password for the host initiator must be different from the outbound username and password for the storage.

Authentifizierung	Abgehender Anruf	Eingehend	Übereinstimmen?
Unidirektional	Benutzername und Kennwort des Hostinitiators	Speicherbenutzername und Kennwort	Muss übereinstimmen
Bidirektional	Benutzername und Kennwort des Hostinitiators	Speicherbenutzername und Kennwort	Muss übereinstimmen
Bidirektional	Speicherbenutzername und Kennwort	Benutzername und Kennwort des Hostinitiators	Muss übereinstimmen

Der ausgehende Benutzername und das Kennwort für den Hostinitiator müssen sich vom ausgehenden Benutzernamen und Kennwort für das Speichersystem unterscheiden.

Richtlinien für die Verwendung der CHAP-Authentifizierung

Befolgen Sie diese Richtlinien, wenn Sie die CHAP-Authentifizierung verwenden.

- Wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für ausgehende CHAP-Einstellungen auf dem Initiator verwenden. Wenn Sie außerdem einen ausgehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, um die bidirektionale Authentifizierung zu aktivieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für eingehende CHAP-Einstellungen auf dem Initiator verwenden.
- Sie können nicht denselben Benutzernamen und dasselbe Kennwort für ein- und ausgehende Einstellungen auf dem Speichersystem verwenden.
- CHAP-Benutzernamen können 1 bis 128 Bytes betragen.

Das System lässt keine Null-Benutzernamen zu.

- CHAP-Passwörter (Schlüssel) können 1 bis 512 Bytes betragen.

Passwörter können Hexadezimalwerte oder Zeichenfolgen sein. Bei Hexadezimalwerten sollten Sie den Wert mit dem Präfix „0x“ oder „0X“ eingeben.

Das System lässt kein Nullkennwort zu.

ONTAP ermöglicht die Verwendung von Sonderzeichen, nicht englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Secrets). Dies unterliegt jedoch Host-Einschränkungen. Wenn einer dieser Server von Ihrem spezifischen Host nicht erlaubt ist, können diese nicht verwendet werden.



Der Microsoft iSCSI-Software-Initiator beispielsweise erfordert, dass die CHAP-Passwörter für Initiator und Ziel mindestens 12 Bytes betragen, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Kennwortlänge beträgt 16 Byte, unabhängig davon, ob IPsec verwendet wird.

Weitere Einschränkungen finden Sie in der Dokumentation des Initiators.

Die Verwendung von Zugriffslisten für iSCSI-Schnittstellen zur Begrenzung von Initiator-Schnittstellen kann Performance und Sicherheit erhöhen

MITHILFE VON iSCSI-Schnittstellenzutrittslisten kann die Anzahl der LIFs in einer SVM begrenzt werden, auf die ein Initiator zugreifen kann. Dies erhöht die Performance und Sicherheit.

Wenn ein Initiator eine Erkennungssitzung mit einem iSCSI- `SendTargets` Befehl startet, erhält er die IP-Adressen, die dem LIF (Netzwerkschnittstelle) in der Zugriffsliste zugeordnet sind. Standardmäßig haben alle

Initiatoren Zugriff auf alle iSCSI LIFs in der SVM. Mithilfe der Zugriffsliste können Sie die Anzahl der LIFs in einer SVM, auf die ein Initiator Zugriff hat, einschränken.

Internet Storage Name Service (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 speichert Informationen über aktive iSCSI-Geräte im Netzwerk, einschließlich ihrer IP-Adressen, iSCSI-Knotennamen IQN's 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 den Initiator und das Ziel aktiviert haben, können Sie die Management-LIF für eine Storage Virtual Machine (SVM) verwenden, um alle iSCSI-LIFs für diese SVM auf dem iSNS-Server zu registrieren. Nach Abschluss der Registrierung kann der iSCSI-Initiator den iSNS-Server abfragen, um alle LIFs für diese bestimmte SVM zu ermitteln.

Wenn Sie sich für die Verwendung eines iSNS-Dienstes entscheiden, müssen Sie sicherstellen, dass Ihre Storage Virtual Machines (SVMs) ordnungsgemäß bei einem Internet Storage Name Service (iSNS)-Server registriert sind.

Wenn Sie keinen iSNS-Server im Netzwerk haben, müssen Sie jedes Ziel manuell so konfigurieren, dass es für den Host sichtbar ist.

Was macht ein iSNS-Server

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

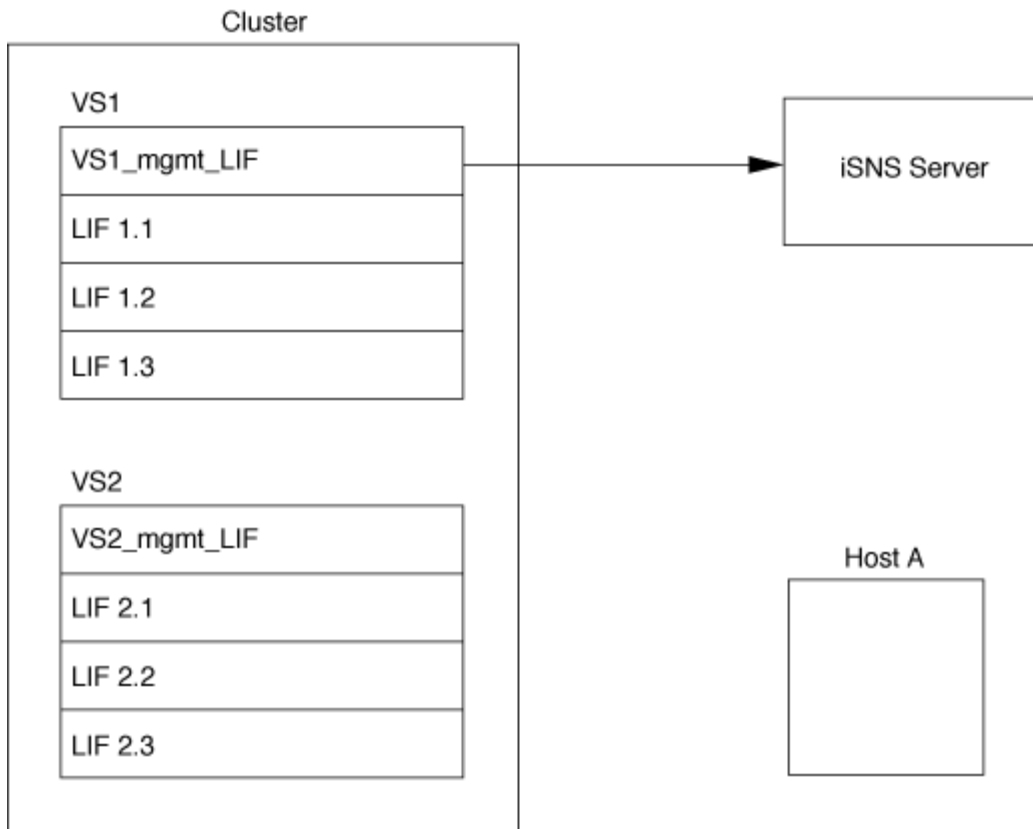
Das iSNS-Protokoll ermöglicht die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem IP-Speichernetzwerk. Ein iSCSI-Initiator kann den iSNS-Server abfragen, um iSCSI-Zielgeräte zu ermitteln.

NetApp bietet keine iSNS Server an oder verkauft diese weiter. Sie können diese Server von einem von NetApp unterstützten Anbieter beziehen.

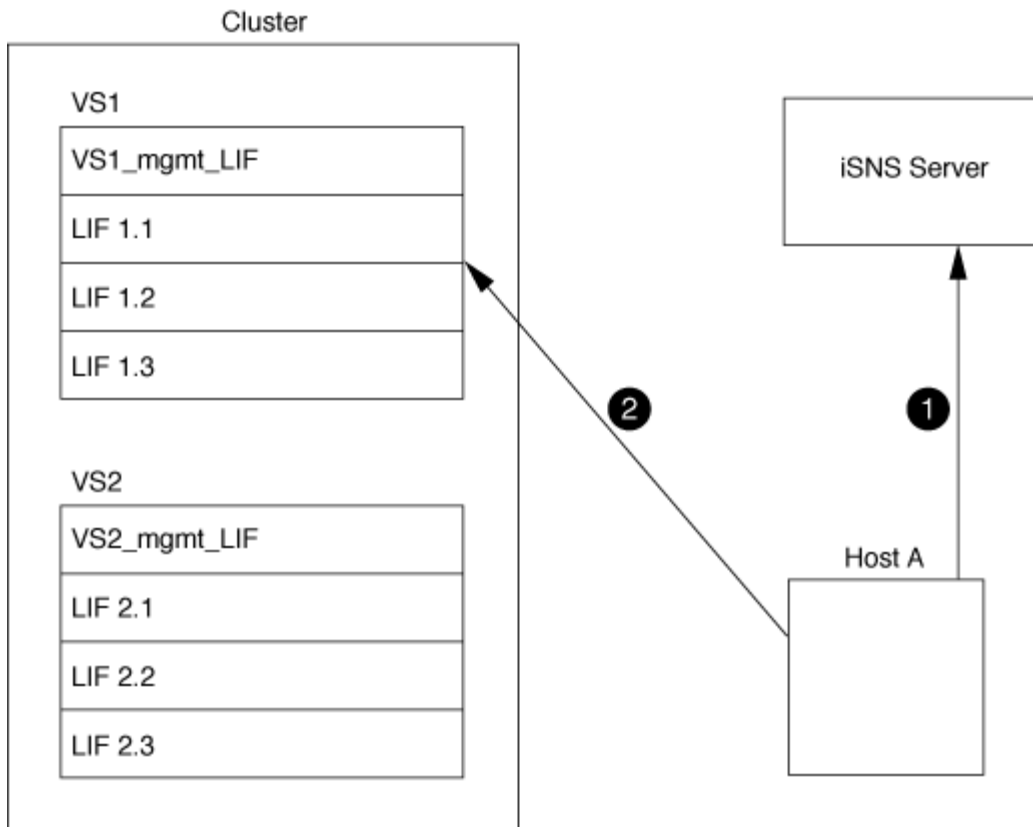
Interaktion von SVMs mit einem iSNS-Server

Der iSNS-Server kommuniziert über die SVM-Management-LIF mit jeder Storage Virtual Machine (SVM). Die Management-LIF registriert alle iSCSI-Zielknotennamen, -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 enthält der iSNS-Server 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 nutzen zu können.



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 Erkennung der LIFs für „VS1“ abgeschlossen hat, kann Host A wie in Schritt 2 gezeigt eine Verbindung zu jedem der LIFs in „VS1“ herstellen. Host A erkennt keine der LIFs in „VS2“, bis sich die Management-LIF „VS2_mgmt_LIF“ für „VS2“ beim iSNS-Server registriert hat.



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

Nach der anfänglichen Konfiguration 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 Zeitpunkt, an dem ONTAP das Update an den iSNS-Server sendet, kann es zu einer Verzögerung von einigen Minuten kommen. Sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server erzwingen: `vserver iscsi isns update`. Erfahren Sie mehr über `vserver iscsi isns update` in der ["ONTAP-Befehlsreferenz"](#).

Befehle zum Verwalten von iSNS

ONTAP bietet Befehle zur Verwaltung Ihres iSNS-Service.

Ihr Ziel ist	Befehl
Konfigurieren Sie einen iSNS-Dienst	<code>vserver iscsi isns create</code>
Starten Sie einen iSNS-Dienst	<code>vserver iscsi isns start</code>
Ändern eines iSNS-Dienstes	<code>vserver iscsi isns modify</code>
iSNS-Servicekonfiguration anzeigen	<code>vserver iscsi isns show</code>

Aktualisierung der registrierten iSNS-Informationen erzwingen	<code>vserver iscsi isns update</code>
Stoppen Sie einen iSNS-Dienst	<code>vserver iscsi isns stop</code>
Entfernen Sie einen iSNS-Dienst	<code>vserver iscsi isns delete</code>
Zeigen Sie die man-Page für einen Befehl an	<code>man <i>command name</i></code>

Erfahren Sie mehr über `vserver iscsi isns` 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 IRGEND EINER 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.