Netzwerkports überwachen

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/networking/monitor_the_health_of_network_ports.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Netzwerkports überwachen . . . 1
Den Zustand der ONTAP Netzwerkports überwachen . . . 1
Überwachung der Erreichbarkeit von ONTAP Netzwerk-Ports . . . 2
ONTAP Port-Nutzung auf einem Speichersystem . . . 6
Eingehender Datenverkehr . . . 6
Ausgehender Verkehr . . . 7
ONTAP interne Ports . . . 9

Netzwerkports überwachen

Den Zustand der ONTAP Netzwerkports überwachen

Die ONTAP Verwaltung von Netzwerkports umfasst eine automatische Zustandsüberwachung sowie eine Reihe von Zustandsmonitoren, die dabei unterstützen, Netzwerkports zu identifizieren, die möglicherweise nicht für das Hosting von LIFs geeignet sind.

Über diese Aufgabe

Stellt ein Health-Monitor fest, dass ein Netzwerkport fehlerhaft ist, warnt er Administratoren durch eine EMS-Meldung oder markiert den Port als beeinträchtigt. ONTAP vermeidet das Hosten von LIFs auf beeinträchtigten Netzwerkports, wenn für diesen LIF gesunde alternative Failover-Ziele vorhanden sind. Ein Port kann aufgrund eines Soft-Failure-Ereignisses wie Link-Flapping (Verbindungen wechseln schnell zwischen aktiv und inaktiv) oder Netzwerkpartitionierung beeinträchtigt werden:

- Netzwerk-Ports im Cluster-IPspace werden als beeinträchtigt markiert, wenn sie Link-Flapping oder einen Verlust der Layer-2-(L2-)Erreichbarkeit zu anderen Netzwerk-Ports in der Broadcast-Domäne aufweisen.
- Netzwerkports in Nicht-Cluster-IPspaces werden als beeinträchtigt markiert, wenn sie Link-Flapping aufweisen.

Folgende Verhaltensweisen eines beeinträchtigten Ports sind zu beachten:

- Ein beeinträchtigter Port kann nicht in ein VLAN oder eine Schnittstellengruppe aufgenommen werden.

  Wenn ein Mitgliedsport einer Schnittstellengruppe als beeinträchtigt markiert ist, die Schnittstellengruppe jedoch weiterhin als fehlerfrei gilt, können LIFs auf dieser Schnittstellengruppe gehostet werden.

- LIFs werden automatisch von beeinträchtigten Ports auf fehlerfreie Ports migriert.
- Während eines Failover-Ereignisses wird ein beeinträchtigter Port nicht als Failover-Ziel betrachtet. Wenn keine fehlerfreien Ports verfügbar sind, hosten beeinträchtigte Ports LIFs gemäß der normalen Failover-Richtlinie.
- Sie können keine LIF auf einem eingeschränkten Port erstellen, migrieren oder zurücksetzen.

  Sie können die `ignore-health-status` Einstellung des Netzwerkports auf `true` ändern. Anschließend kann eine LIF auf den fehlerfreien Ports gehostet werden.

Schritte

1. Melden Sie sich im erweiterten Berechtigungsmodus an:

   ```
   set -privilege advanced
   ```

2. Es kann geprüft werden, welche Systemüberwachungsfunktionen zur Überwachung des Netzwerkportzustands aktiviert sind:

   ```
   network options port-health-monitor show
   ```

Der Gesundheitszustand eines Ports wird durch den Wert der Health Monitors bestimmt.

Die folgenden Gesundheitsmonitore sind in ONTAP verfügbar und standardmäßig aktiviert:

- Link-Flapping Health Monitor: Überwacht Link-Flapping

  Wenn ein Port innerhalb von fünf Minuten mehr als einmal einen Verbindungsabbruch aufweist, wird dieser Port als beeinträchtigt markiert.

- L2 Reachability Health Monitor: Überwacht, ob alle Ports, die in derselben Broadcast-Domäne konfiguriert sind, L2-Erreichbarkeit zueinander haben.

  Dieser Health Monitor meldet L2-Erreichbarkeitsprobleme in allen IPspaces, allerdings werden nur die Ports im Cluster-IPspace als beeinträchtigt markiert.

- CRC Monitor: Überwacht die CRC-Statistiken der Ports

  Dieser Gesundheitsmonitor kennzeichnet einen Port nicht als beeinträchtigt, sondern generiert eine EMS-Meldung, wenn eine sehr hohe CRC-Fehlerrate festgestellt wird.

Weitere Informationen zu `network options port-health-monitor show` finden sich in der "ONTAP-Befehlsreferenz".

3. Die gewünschten Health Monitore für einen IPspace können mit dem `network options port-health-monitor modify` Befehl aktiviert oder deaktiviert werden.

   Weitere Informationen zu `network options port-health-monitor modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Detaillierter Zustand eines Ports:

   ```
   network port show -health
   ```

Die Befehlsausgabe zeigt den Gesundheitszustand des Ports, `ignore health status` die Einstellung und eine Liste der Gründe an, warum der Port als beeinträchtigt markiert ist.

Der Gesundheitszustand eines Ports kann `healthy` oder `degraded` sein.

Wenn die `ignore health status` Einstellung `true` ist, zeigt dies an, dass der Port-Integritätsstatus vom Administrator von `degraded` auf `healthy` geändert wurde.

Wenn die `ignore health status` Einstellung `false` ist, wird der Port-Gesundheitsstatus automatisch vom System bestimmt.

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

Überwachung der Erreichbarkeit von ONTAP Netzwerk-Ports

Die Erreichbarkeitsüberwachung ist in ONTAP 9.8 und höher integriert. Mit dieser Überwachung lässt sich erkennen, wenn die physische Netzwerktopologie nicht mit der

ONTAP Konfiguration übereinstimmt. In einigen Fällen kann ONTAP die Port-Erreichbarkeit wiederherstellen. In anderen Fällen sind zusätzliche Schritte erforderlich.

Über diese Aufgabe

Mit diesen Befehlen lassen sich Netzwerkfehlkonfigurationen überprüfen, diagnostizieren und beheben, die darauf zurückzuführen sind, dass die ONTAP Konfiguration weder mit der physischen Verkabelung noch mit der Netzwerk-Switch Konfiguration übereinstimmt.

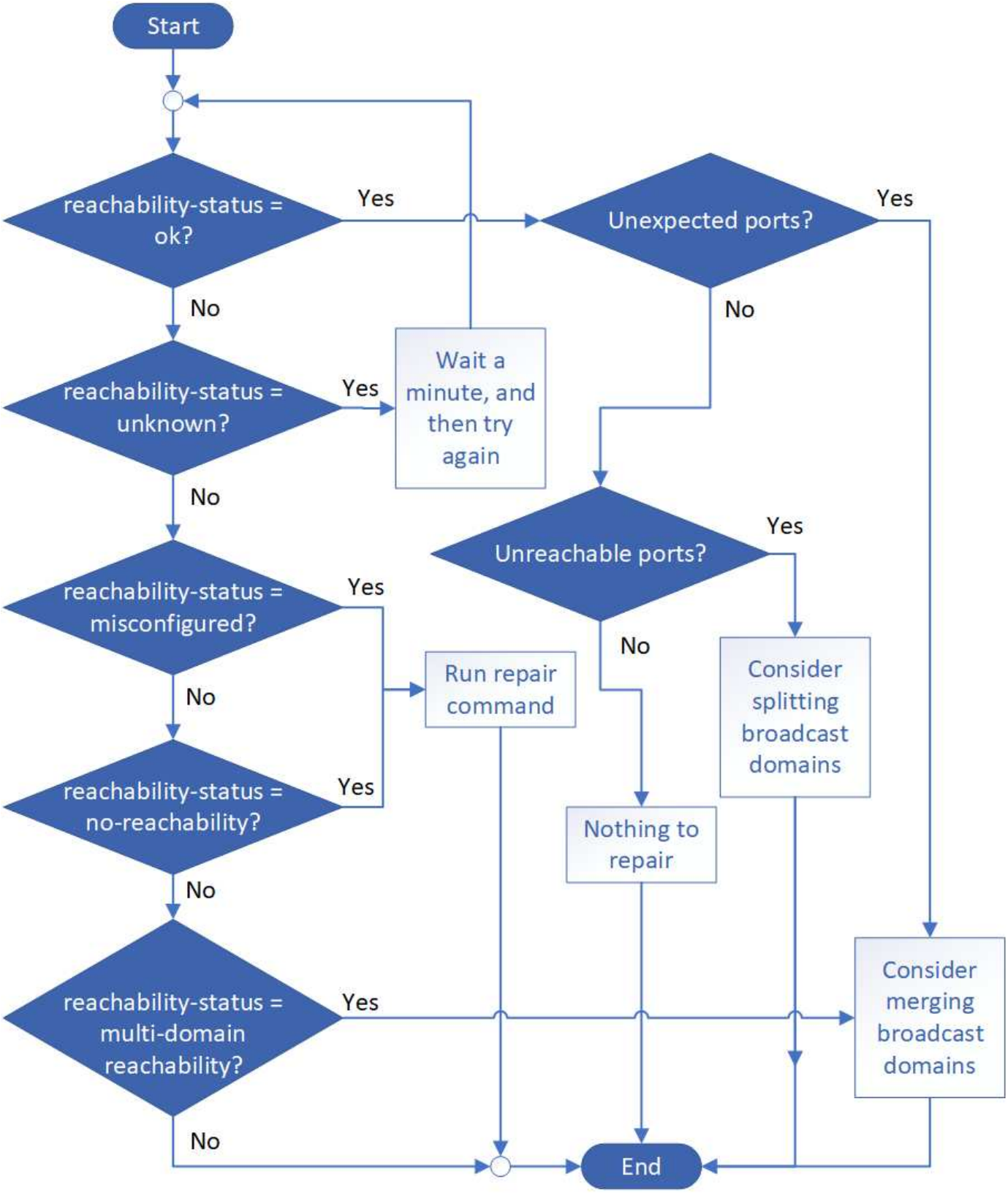
Schritt

1. Port-Erreichbarkeit anzeigen:

   ```
   network port reachability show
   ```

   Weitere Informationen zu `network port reachability show` finden sich in der "ONTAP-Befehlsreferenz".

2. Der folgende Entscheidungsbaum und die Tabelle geben Aufschluss darüber, ob ein nächster Schritt erforderlich ist.



Erreichbarkeitsstatus	Beschreibung

OK	Der Port verfügt über Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne. Wenn der Erreichbarkeitsstatus „ok“ ist, aber „unerwartete Ports“ vorhanden sind, kann das Zusammenführen einer oder mehrerer Broadcast-Domänen in Betracht gezogen werden. Weitere Informationen stehen in der folgenden Zeile *Unexpected ports*. Wenn der Erreichbarkeitsstatus „ok“ ist, aber „nicht erreichbare Ports“ vorhanden sind, kann das Aufteilen einer oder mehrerer Broadcast-Domänen in Erwägung gezogen werden. Weitere Informationen enthält die folgende Zeile *Nicht erreichbare Ports*. Wenn der Erreichbarkeitsstatus "ok" ist und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist Ihre Konfiguration korrekt.
Unerwartete Ports	Der Port ist über Layer 2 zu seiner zugewiesenen Broadcast-Domäne erreichbar; er ist jedoch auch über Layer 2 zu mindestens einer weiteren Broadcast-Domäne erreichbar. Die physische Konnektivität und die Switch-Konfiguration sollten überprüft werden, um festzustellen, ob sie fehlerhaft sind oder ob die dem Port zugewiesene Broadcast-Domäne mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden sich unter "Zusammenführen von Broadcast-Domänen".
Nicht erreichbare Ports	Wenn eine einzelne Broadcast-Domäne in zwei verschiedene Erreichbarkeitsgruppen aufgeteilt wurde, kann eine Broadcast-Domäne aufgeteilt werden, um die ONTAP Konfiguration mit der physischen Netzwerktopologie zu synchronisieren. Die Liste der nicht erreichbaren Ports definiert üblicherweise die Menge der Ports, die in eine andere Broadcast-Domäne aufgeteilt werden sollten, nachdem überprüft wurde, dass die physische und die Switch-Konfiguration korrekt sind. Weitere Informationen finden sich unter "Aufgeteilte Broadcast-Domänen".
Fehlkonfigurierte Erreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne, jedoch hat der Port Layer-2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Bei Ausführung des folgenden Befehls weist das System den Port der Broadcast-Domäne zu, zu der er erreichbar ist: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Reparatur der Port-Erreichbarkeit".
Unerreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu einer bestehenden Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Beim Ausführen des folgenden Befehls weist das System den Port einer neu automatisch erstellten Broadcast-Domäne im Default-IPspace zu: `network port reachability repair -node -port` Weitere Informationen finden Sie unter "Reparatur der Port-Erreichbarkeit". Weitere Informationen zu `network port reachability repair` finden sich in der "ONTAP-Befehlsreferenz".

Erreichbarkeit über mehrere Domänen hinweg	Der Port ist über Layer 2 zu seiner zugewiesenen Broadcast-Domäne erreichbar; er ist jedoch auch über Layer 2 zu mindestens einer weiteren Broadcast-Domäne erreichbar. Die physische Konnektivität und die Switch-Konfiguration sollten überprüft werden, um festzustellen, ob sie fehlerhaft sind oder ob die dem Port zugewiesene Broadcast-Domäne mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Zusammenführen von Broadcast-Domänen" oder "Reparatur der Port-Erreichbarkeit".
unbekannt	Wenn der Erreichbarkeitsstatus „unbekannt“ ist, einige Minuten abwarten und den Befehl erneut ausführen.

Nach der Reparatur eines Ports müssen verschobene LIFs und VLANs überprüft und behoben werden. Wenn der Port Teil einer Schnittstellengruppe war, ist es außerdem erforderlich, nachzuvollziehen, was mit dieser Schnittstellengruppe geschehen ist. Weitere Informationen finden sich unter "Reparatur der Port-Erreichbarkeit".

ONTAP Port-Nutzung auf einem Speichersystem

Mehrere bekannte Ports sind für die ONTAP Kommunikation mit bestimmten Diensten reserviert. Portkonflikte treten auf, wenn ein Portwert in Ihrer Speichernetzwerkumgebung mit dem Wert eines ONTAP Ports übereinstimmt.

Eingehender Datenverkehr

Der eingehende Datenverkehr auf Ihrem ONTAP Storage verwendet die folgenden Protokolle und Ports:

Protokoll	Port	Zweck
Alle ICMP	Alle	Die Instanz anpingen
TCP	22	Sicherer Shell-Zugriff auf die IP-Adresse der Cluster-Management-LIF oder einer Node-Management-LIF
TCP	80	Webzugriff auf die IP-Adresse der Cluster-Management-LIF
TCP/UDP	111	RPCBIND, Remote Procedure Call für NFS
UDP	123	NTP, Netzwerkzeitprotokoll
TCP	135	MSRPC, Microsoft Remote Procedure Call
TCP	139	NETBIOS-SSN, NetBIOS-Dienstsitzung für CIFS
TCP/UDP	161-162	SNMP, einfaches Netzwerkmanagementprotokoll
TCP	443	Sicherer Webseitenzugriff auf die IP-Adresse der Cluster-Management-LIF
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS über TCP mit NetBIOS Framing
TCP/UDP	635	NFS-Mount zur Interaktion mit einem entfernten Dateisystem, als ob es lokal wäre

TCP	749	Kerberos
UDP	953	Name Daemon
TCP/UDP	2049	NFS Server-Daemon
TCP	2050	NRV, NetApp Remote Volume Protocol
TCP	3260	iSCSI-Zugriff über die iSCSI-Daten-LIF
TCP/UDP	4045	NFS Sperrdaemon
TCP/UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-RPC-Rquotad
UDP	4444	KRB524, Kerberos 524
UDP	5353	Multicast DNS
TCP	10000	Datensicherung mit Network Data Management Protocol (NDMP)
TCP	11104	Cluster-Peering, bidirektionale Verwaltung von Intercluster-Verbindungssitzungen für SnapMirror
TCP	11105	Cluster-Peering, bidirektionaler SnapMirror Datentransfer über Intercluster-LIFs
SSL/TLS	30000	Akzeptiert sichere NDMP-Steuerungsverbindungen zwischen DMA und NDMP-Server über sichere Sockets (SSL/TLS). Sicherheitsscanner können eine Schwachstelle auf Port 30000 melden.

Ausgehender Verkehr

Der ausgehende Datenverkehr Ihres ONTAP Storage kann je nach Geschäftsanforderungen mithilfe einfacher oder erweiterter Regeln eingerichtet werden.

Grundlegende ausgehende Regeln

Alle Ports können für den gesamten ausgehenden Datenverkehr über ICMP-, TCP- und UDP-Protokolle verwendet werden.

Protokoll	Port	Zweck
Alle ICMP	Alle	Der gesamte ausgehende Verkehr
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte ausgehende Regeln

Falls Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie mithilfe der folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch ONTAP erforderlich sind.

Active Directory

Protokoll	Port	Quelle	Ziel	Zweck
TCP	88	Node Management LIF, Daten LIF (NFS, CIFS, iSCSI)	Active Directory Gesamtstruktur	Kerberos V Authentifizierung
UDP	137	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Namensdienst
UDP	138	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Datagrammdienst
TCP	139	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	NetBIOS Dienstsitzung
TCP	389	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	LDAP
UDP	389	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	LDAP
TCP	445	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS Framing
TCP	464	Knotenmanagement-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Kerberos V-Passwort ändern und festlegen (SET_CHANGE)
UDP	464	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Kerberos Schlüsselverwaltung
TCP	749	Node-Management-LIF, Daten-LIF (NFS, CIFS)	Active Directory Gesamtstruktur	Ändern und Festlegen des Kerberos V Passworts (RPCSEC_GSS)

AutoSupport

Protokoll	Port	Quelle	Ziel	Zweck
TCP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)

SNMP

Protokoll	Port	Quelle	Ziel	Zweck
TCP/UDP	162	Node Management-LIF	Monitor Server	Überwachung mittels SNMP-Traps

SnapMirror

Protokoll	Port	Quelle	Ziel	Zweck

TCP	11104	Intercluster-LIF	ONTAP Intercluster LIFs	Management von Intercluster-Verbindungssitzungen für SnapMirror

Sonstige Dienstleistungen

Protokoll	Port	Quelle	Ziel	Zweck
TCP	25	Node Management-LIF	Mailserver	SMTP-Benachrichtigungen können für AutoSupport verwendet werden
UDP	53	Node Management LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
UDP	67	Node Management-LIF	DHCP	DHCP-Server
UDP	68	Node Management-LIF	DHCP	DHCP Client für die erstmalige Einrichtung
UDP	514	Node Management-LIF	Syslog Server	Syslog Weiterleitungsnachrichten
TCP	5010	Intercluster-LIF	Backup-Endpunkt oder Restore-Endpunkt	Sicherungs- und Wiederherstellungsvorgänge für die Funktion „Backup to S3“
TCP	18600 bis 18699	Node Management-LIF	Zielserver	NDMP Kopie

ONTAP interne Ports

Die folgende Tabelle listet die von ONTAP intern verwendeten Ports und deren Funktionen auf. ONTAP nutzt diese Ports für verschiedene Funktionen, wie zum Beispiel für die Herstellung der Intracluster-LIF-Kommunikation.

Diese Liste ist nicht vollständig und kann je nach Umgebung variieren.

Port/Protokoll	Komponente/Funktion
514	Syslog
900	NetApp Cluster-RPC
902	NetApp Cluster-RPC
904	NetApp Cluster-RPC
905	NetApp Cluster-RPC
910	NetApp Cluster-RPC
911	NetApp Cluster-RPC
913	NetApp Cluster-RPC

914	NetApp Cluster-RPC
915	NetApp Cluster-RPC
918	NetApp Cluster-RPC
920	NetApp Cluster-RPC
921	NetApp Cluster-RPC
924	NetApp Cluster-RPC
925	NetApp Cluster-RPC
927	NetApp Cluster-RPC
928	NetApp Cluster-RPC
929	NetApp Cluster-RPC
930	Kernel-Services und Managementfunktionen (KSMF)
931	NetApp Cluster-RPC
932	NetApp Cluster-RPC
933	NetApp Cluster-RPC
934	NetApp Cluster-RPC
935	NetApp Cluster-RPC
936	NetApp Cluster-RPC
937	NetApp Cluster-RPC
939	NetApp Cluster-RPC
940	NetApp Cluster-RPC
951	NetApp Cluster-RPC
954	NetApp Cluster-RPC
955	NetApp Cluster-RPC
956	NetApp Cluster-RPC
958	NetApp Cluster-RPC
961	NetApp Cluster-RPC
963	NetApp Cluster-RPC
964	NetApp Cluster-RPC
966	NetApp Cluster-RPC
967	NetApp Cluster-RPC
975	Key Management Interoperability Protocol (KMIP)
982	NetApp Cluster-RPC
983	NetApp Cluster-RPC
5125	Alternativer Steuerport für Festplatte

5133	Alternativer Steuerport für Festplatte
5144	Alternativer Steuerport für Festplatte
65502	Node Scope SSH
65503	LIF-Sharing
7700	Cluster Session Manager (CSM)
7810	NetApp Cluster-RPC
7811	NetApp Cluster-RPC
7812	NetApp Cluster-RPC
7813	NetApp Cluster-RPC
7814	NetApp Cluster-RPC
7815	NetApp Cluster-RPC
7816	NetApp Cluster-RPC
7817	NetApp Cluster-RPC
7818	NetApp Cluster-RPC
7819	NetApp Cluster-RPC
7820	NetApp Cluster-RPC
7821	NetApp Cluster-RPC
7822	NetApp Cluster-RPC
7823	NetApp Cluster-RPC
7824	NetApp Cluster-RPC
7835-7839 und 7845-7849	TCP-Ports für die Kommunikation innerhalb des Clusters
8023	Node Scope TELNET
8443	ONTAP S3 NAS Port für Amazon FSx
8514	Node Scope RSH
9877	KMIP Client Port (nur interner lokaler Host)
10006	TCP-Port für HA-Interconnect-Kommunikation

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.