Das SP/BMC-Netzwerk konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/system-admin/isolate-management-traffic-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

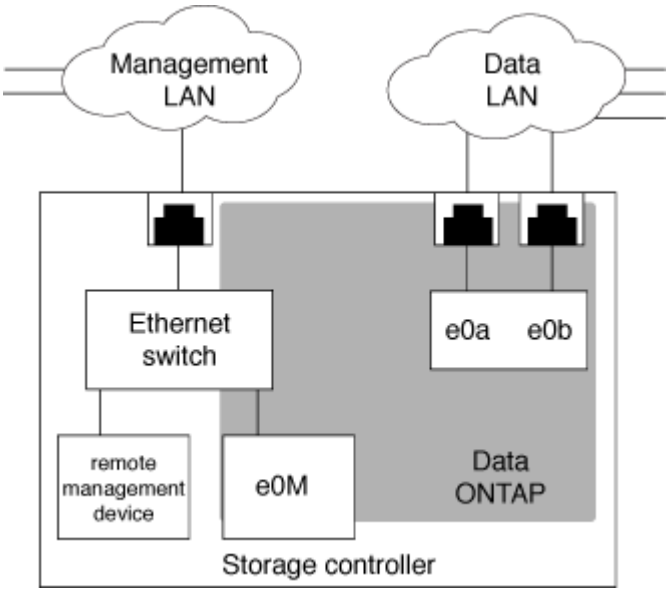
Das SP/BMC-Netzwerk konfigurieren 1
ONTAP Verwaltungsdatenverkehr im Netzwerk isolieren 1
Informationen zur ONTAP SP/ BMC Netzwerkkonfiguration 1
Automatische Netzwerkkonfiguration für ONTAP SP/BMC aktivieren 3
Das ONTAP SP/BMC Netzwerk manuell konfigurieren 4
Die ONTAP Service Processor API-Konfiguration anpassen 6

Das SP/BMC-Netzwerk konfigurieren

ONTAP Verwaltungsdatenverkehr im Netzwerk isolieren

Es gilt als Best Practice, SP/BMC und die e0M Managementoberfläche in einem Subnetz zu konfigurieren, das ausschließlich für den Management-Datenverkehr vorgesehen ist. Die Übertragung von Datenverkehr über das Managementnetzwerk kann zu Leistungseinbußen und Routing-Problemen führen.

Der Management-Ethernet-Port der meisten Storage Controller (gekennzeichnet durch ein Schraubenschlüssel-Symbol auf der Rückseite des Gehäuses) ist mit einem internen Ethernet-Switch verbunden. Der interne Switch stellt die Verbindung zu SP/BMC und zur e0M Managementoberfläche her, die für den Zugriff auf das Speichersystem über TCP/IP-Protokolle wie Telnet, SSH und SNMP genutzt werden kann.



Wenn Sie sowohl das Fernverwaltungsgerät als auch e0M verwenden möchten, müssen Sie diese im selben IP-Subnetz konfigurieren. Da es sich um Schnittstellen mit geringer Bandbreite handelt, ist es am besten, SP/BMC und e0M in einem für den Managementdatenverkehr reservierten Subnetz zu konfigurieren.

Wenn Sie den Management-Datenverkehr nicht isolieren können oder Ihr dediziertes Management-Netzwerk ungewöhnlich groß ist, sollte das Netzwerkverkehrsaufkommen so gering wie möglich gehalten werden. Übermäßiger eingehender Broadcast- oder Multicast-Datenverkehr kann die Leistung von SP/BMC beeinträchtigen.

Einige Storage-Controller, wie beispielsweise der AFF A800, verfügen über zwei externe Ports, einen für BMC und den anderen für e0M. Für diese Controller besteht keine Anforderung, BMC und e0M im selben IP-Subnetz zu konfigurieren.

Informationen zur ONTAP SP/ BMC Netzwerkkonfiguration

Sie können die automatische Netzwerkkonfiguration auf Clusterebene für den SP (empfohlen) aktivieren. Es besteht auch die Möglichkeit, die automatische

Netzwerkkonfiguration des SP deaktiviert zu lassen (Standardeinstellung) und die SP-Netzwerkkonfiguration manuell auf Knotenebene zu verwalten. Für beide Fälle sind einige Aspekte zu berücksichtigen.

Dieses Thema gilt sowohl für den SP als auch für den BMC.

Die automatische SP-Netzwerkkonfiguration ermöglicht es dem SP, Adressressourcen (einschließlich IP-Adresse, Subnetzmaske und Gateway-Adresse) aus dem angegebenen Subnetz zu verwenden, um sein Netzwerk automatisch einzurichten. Mit der automatischen SP-Netzwerkkonfiguration ist keine manuelle Zuweisung von IP-Adressen für den SP jedes Knotens erforderlich. Standardmäßig ist die automatische SP-Netzwerkkonfiguration deaktiviert, da für die Aktivierung zunächst das für die Konfiguration zu verwendende Subnetz im Cluster definiert sein muss.

Wenn die SP automatische Netzwerkkonfiguration aktiviert wird, gelten die folgenden Szenarien und Überlegungen:

- Wenn der SP noch nie konfiguriert wurde, wird das SP-Netzwerk automatisch auf Basis des für die automatische SP-Netzwerkkonfiguration angegebenen Subnetzes konfiguriert.
- Wenn der SP zuvor manuell konfiguriert wurde oder die bestehende SP-Netzwerkkonfiguration auf einem anderen Subnetz basiert, wird das SP-Netzwerk aller Knoten im Cluster auf Grundlage des Subnetzes neu konfiguriert, das Sie in der automatischen SP-Netzwerkkonfiguration angeben.

  Die Neukonfiguration kann dazu führen, dass dem SP eine andere Adresse zugewiesen wird, was Auswirkungen auf Ihre DNS-Konfiguration und deren Fähigkeit zur Auflösung von SP-Hostnamen haben kann. Infolgedessen könnte eine Aktualisierung Ihrer DNS-Konfiguration erforderlich sein.

- Ein Knoten, der dem Cluster beitritt, verwendet das angegebene Subnetz, um sein SP-Netzwerk automatisch zu konfigurieren.
- Der `system service-processor network modify`Befehl ermöglicht keine Änderung der SP IP-Adresse.

  Wenn die automatische SP Netzwerkkonfiguration aktiviert ist, erlaubt der Befehl nur das Aktivieren oder Deaktivieren der SP Netzwerkschnittstelle.

  - Wenn die automatische SP-Netzwerkkonfiguration zuvor aktiviert war, führt das Deaktivieren der SP-Netzwerkschnittstelle dazu, dass die zugewiesene Adressressource freigegeben und dem Subnetz zurückgegeben wird.
  - Wenn die SP-Netzwerkschnittstelle deaktiviert und anschließend wieder aktiviert wird, kann der SP möglicherweise mit einer anderen Adresse neu konfiguriert werden.

Wenn die automatische SP-Netzwerkkonfiguration deaktiviert ist (Standardeinstellung), gelten die folgenden Szenarien und Überlegungen:

- Wenn der SP noch nie konfiguriert wurde, verwendet die SP-IPv4-Netzwerkkonfiguration standardmäßig IPv4 DHCP, und IPv6 ist deaktiviert.

  Ein Knoten, der dem Cluster beitritt, verwendet standardmäßig ebenfalls IPv4 DHCP für seine SP-Netzwerkkonfiguration.

- Der `system service-processor network modify`Befehl ermöglicht die Konfiguration der SP-IP-Adresse eines Knotens.

  Eine Warnmeldung erscheint, wenn versucht wird, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind. Das Ignorieren der Warnung und das Fortfahren mit

der manuellen Adresszuweisung kann zu einer Situation mit doppelten Adressen führen.

Wenn die SP automatische Netzwerkkonfiguration nach vorheriger Aktivierung deaktiviert wird, gelten die folgenden Szenarien und Überlegungen:

- Wenn die automatische SP-Netzwerkkonfiguration die IPv4-Adressfamilie deaktiviert hat, verwendet das SP IPv4-Netzwerk standardmäßig DHCP, und der `system service-processor network modify` Befehl ermöglicht die Anpassung der SP IPv4-Konfiguration für einzelne Knoten.
- Wenn die automatische SP-Netzwerkkonfiguration die IPv6-Adressfamilie deaktiviert hat, ist auch das SP IPv6-Netzwerk deaktiviert, und der `system service-processor network modify` Befehl ermöglicht das Aktivieren und Ändern der SP IPv6-Konfiguration für einzelne Nodes.

Automatische Netzwerkkonfiguration für ONTAP SP/BMC aktivieren

Die Aktivierung der automatischen Netzwerkkonfiguration für den SP wird gegenüber der manuellen Konfiguration des SP Netzwerks bevorzugt. Da die automatische Netzwerkkonfiguration des SP clusterweit gilt, ist keine manuelle Verwaltung des SP Netzwerks für einzelne Knoten erforderlich.

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

- Das Subnetz, das Sie für die SP automatische Netzwerkkonfiguration verwenden möchten, muss bereits im Cluster definiert sein und darf keine Ressourcenkonflikte mit der SP Netzwerkschnittstelle aufweisen.

  Der `network subnet show` Befehl zeigt Subnetzinformationen für den Cluster an.

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

  Der Parameter, der die Subnetzzuordnung erzwingt (der `-force-update-lif-associations` Parameter der `network subnet` Befehle), wird nur auf Netzwerk-LIFs und nicht auf der SP Netzwerkschnittstelle unterstützt.

- Wenn IPv6-Verbindungen für den SP verwendet werden sollen, muss IPv6 für ONTAP bereits konfiguriert und aktiviert sein.

  Der `network options ipv6 show` Befehl zeigt den aktuellen Status der IPv6-Einstellungen für ONTAP an. Weitere Informationen zu `network options ipv6 show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Geben Sie die IPv4- oder IPv6-Adressfamilie und den Namen des Subnetzes an, das der SP verwenden soll, indem Sie den `system service-processor network auto-configuration enable` Befehl verwenden.
2. Die automatische SP-Netzwerkkonfiguration kann mit dem `system service-processor network auto-configuration show` Befehl angezeigt werden.
3. Wenn anschließend die SP IPv4 oder IPv6 Netzwerkschnittstelle für alle Knoten, die sich im Quorum befinden, deaktiviert oder wieder aktiviert werden soll, ist der `system service-processor network modify` Befehl mit den Parametern `-address-family` [`IPv4`|`IPv6`] und `-enable` [`true`|`false`] zu verwenden.

Wenn die automatische SP-Netzwerkkonfiguration aktiviert ist, kann die SP-IP-Adresse eines Knotens, der sich im Quorum befindet, nicht geändert werden. Es kann lediglich die SP-IPv4- oder SP-IPv6-Netzwerkschnittstelle aktiviert oder deaktiviert werden.

Befindet sich ein Knoten außerhalb des Quorums, kann die SP-Netzwerkkonfiguration des Knotens, einschließlich der SP-IP-Adresse, durch Ausführen von `system service-processor network modify` auf dem Knoten geändert werden, wobei zu bestätigen ist, dass die automatische SP-Netzwerkkonfiguration für den Knoten überschrieben werden soll. Wenn der Knoten dem Quorum wieder beitritt, erfolgt die automatische SP-Neukonfiguration für den Knoten basierend auf dem angegebenen Subnetz.

Das ONTAP SP/BMC Netzwerk manuell konfigurieren

Wenn keine automatische Netzwerkkonfiguration für den SP eingerichtet ist, muss das SP Netzwerk eines Knotens manuell konfiguriert werden, damit der SP über eine IP-Adresse erreichbar ist.

Bevor Sie beginnen

Wenn IPv6-Verbindungen für den SP verwendet werden sollen, muss IPv6 für ONTAP bereits konfiguriert und aktiviert sein. Die `network options ipv6` Befehle verwalten die IPv6-Einstellungen für ONTAP. Weitere Informationen zu `network options ipv6` finden sich in der "ONTAP-Befehlsreferenz".

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Der SP kann so konfiguriert werden, dass er IPv4, IPv6 oder beides verwendet. Die SP IPv4 Konfiguration unterstützt statische und DHCP-Adressierung, und die SP IPv6 Konfiguration unterstützt nur statische Adressierung.

Wenn die automatische SP-Netzwerkkonfiguration eingerichtet ist, ist keine manuelle Konfiguration des SP-Netzwerks für einzelne Knoten erforderlich, und der `system service-processor network modify` Befehl ermöglicht lediglich das Aktivieren oder Deaktivieren der SP-Netzwerkschnittstelle.

Schritte

1. Das SP Netzwerk für einen Node kann mit dem `system service-processor network modify` Befehl konfiguriert werden.
   - Der `-address-family`Parameter gibt an, ob die IPv4- oder die IPv6-Konfiguration des SP geändert wird.
   - Der `-enable` Parameter aktiviert die Netzwerkschnittstelle der angegebenen IP-Adressfamilie.
   - Der `-dhcp`Parameter gibt an, ob die Netzwerkkonfiguration vom DHCP-Server oder die von Ihnen angegebene Netzwerkadresse verwendet wird.

     DHCP kann (durch Einstellen von `-dhcp` auf `v4`) nur aktiviert werden, wenn IPv4 verwendet wird. DHCP kann für IPv6-Konfigurationen nicht aktiviert werden.

   - Der `-ip-address`Parameter gibt die öffentliche IP-Adresse für den SP an.

     Eine Warnmeldung erscheint, wenn versucht wird, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind. Das Ignorieren der Warnung und das Fortsetzen der manuellen Adresszuweisung kann zu einer doppelten Adresszuweisung führen.

- Der `-netmask`Parameter gibt die Subnetzmaske für den SP (bei Verwendung von IPv4) an.
- Der `-prefix-length` Parameter gibt die Netzwerkpräfixlänge der Subnetzmaske für den SP (bei Verwendung von IPv6) an.
- Der `-gateway`Parameter gibt die Gateway-IP-Adresse für den SP an.

2. Das SP Netzwerk für die verbleibenden Knoten im Cluster wird konfiguriert, indem Schritt 1 wiederholt wird.
3. Die SP-Netzwerkkonfiguration kann angezeigt und der SP Einrichtungsstatus überprüft werden, indem der `system service-processor network show` Befehl mit den `-instance` oder `-field setup-status` Parametern verwendet wird.

   Der SP Setup-Status für einen Knoten kann einer der folgenden sein:

   - `not-setup` — Nicht konfiguriert
   - `succeeded` — Konfiguration erfolgreich
   - `in-progress` Konfiguration läuft
   - `failed` — Konfiguration fehlgeschlagen

Beispiel für die Konfiguration des SP Netzwerks

Das folgende Beispiel konfiguriert den SP eines Knotens für die Verwendung von IPv4, aktiviert den SP und zeigt die SP Netzwerkkonfiguration an, um die Einstellungen zu überprüfen:

```
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::>
```

Die ONTAP Service Processor API-Konfiguration anpassen

Die SP-API ist eine sichere Netzwerk-API, die ONTAP die Kommunikation mit dem SP über das Netzwerk ermöglicht. Es besteht die Möglichkeit, den vom SP-API-Service verwendeten Port zu ändern, die für die interne Kommunikation genutzten Zertifikate zu erneuern oder den Service vollständig zu deaktivieren. Eine Änderung der Konfiguration ist nur in seltenen Fällen erforderlich.

Über diese Aufgabe

- Der SP API-Service verwendet standardmäßig Port `50000`.

  Sie können den Portwert ändern, wenn Sie sich beispielsweise in einer Netzwerkumgebung befinden, in der Port `50000` von einer anderen Netzwerkanwendung für die Kommunikation verwendet wird oder wenn Sie zwischen dem Datenverkehr anderer Anwendungen und dem vom SP API-Service erzeugten Datenverkehr unterscheiden möchten.

- Die für den SP API-Service verwendeten SSL- und SSH-Zertifikate sind intern im Cluster und werden nicht extern verteilt.

  Im unwahrscheinlichen Fall, dass die Zertifikate kompromittiert werden, ist eine Erneuerung möglich.

- Der SP API-Service ist standardmäßig aktiviert.

  Das Deaktivieren des SP API-Service ist nur in seltenen Fällen erforderlich, beispielsweise in einem privaten LAN, in dem der SP nicht konfiguriert oder verwendet wird und der Dienst deaktiviert werden soll.

  Wenn der SP API-Service deaktiviert ist, akzeptiert die API keine eingehenden Verbindungen. Zusätzlich stehen Funktionen wie netzwerkbasierte SP-Firmware-Updates und die netzwerkbasierte SP „down system“-Revisionsprotokollsammlung nicht mehr zur Verfügung. Das System wechselt zur Verwendung der seriellen Schnittstelle.

Schritte

1. Zur erweiterten Berechtigungsstufe wird mit dem `set -privilege advanced` Befehl gewechselt.
2. Die SP API-Service-Konfiguration anpassen:

Wenn Sie möchten…	Der folgende Befehl kann verwendet werden…
Den vom SP API-Service verwendeten Port ändern	`system service-processor api-service modify` mit dem `-port {49152..65535}` Parameter

Wenn Sie möchten…	Der folgende Befehl kann verwendet werden…
Die SSL- und SSH-Zertifikate, die vom SP API-Service für die interne Kommunikation verwendet werden, erneuern.	• Für ONTAP 9.5 oder höher verwenden `system service-processor api-service renew-internal-certificate` • Für ONTAP 9.4 und frühere Versionen • `system service-processor api-service renew-certificates` Wird kein Parameter angegeben, werden nur die Hostzertifikate (einschließlich der Client- und Serverzertifikate) erneuert. Wenn der `-renew-all true` Parameter angegeben wird, werden sowohl die Hostzertifikate als auch das Root-CA-Zertifikat erneuert.
Kommunikation	
Deaktivieren oder erneutes Aktivieren des SP API-Service	`system service-processor api-service modify` mit dem `-is-enabled {true`

3. Die SP API-Service-Konfiguration wird mit dem `system service-processor api-service show` Befehl angezeigt.

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.