



SP / BMCネットワークの設定

ONTAP 9

NetApp
January 23, 2026

目次

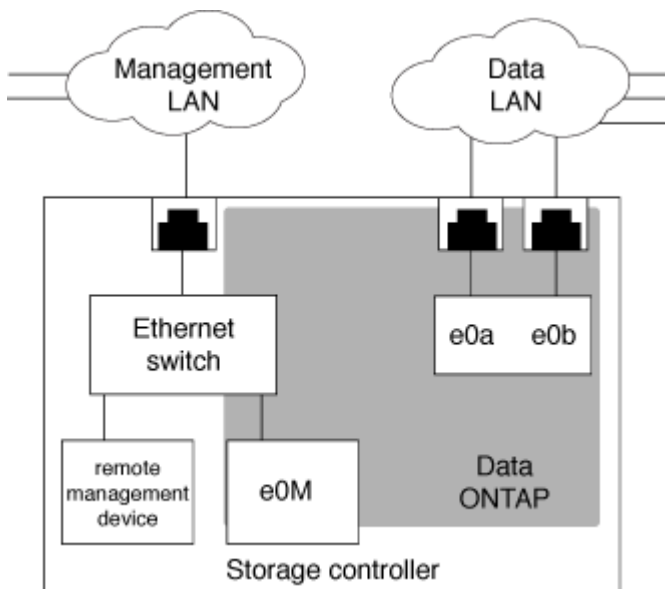
SP / BMCネットワークの設定	1
ネットワーク内のONTAP管理トラフィックを分離する	1
ONTAP SP/BMCネットワーク構成について学ぶ	1
ONTAP SP/BMC自動ネットワーク構成を有効にする	3
ONTAP SP/BMCネットワークを手動で設定する	4
ONTAPサービスプロセッサAPI構成を変更する	6

SP / BMCネットワークの設定

ネットワーク内のONTAP管理トラフィックを分離する

SP / BMCおよびe0M管理インターフェイスは、管理トラフィック専用のサブネットに設定することを推奨します。管理ネットワーク経由でデータトラフィックを処理すると、パフォーマンスの低下やルーティングの問題が発生する可能性があります。

ほとんどのストレージコントローラの管理イーサネットポート（シャーシ背面にあるレンチマークの付いたポート）は、内部イーサネットスイッチに接続されます。内部スイッチによって提供されるSP / BMCおよびe0M管理インターフェイスへの接続を使用すれば、Telnet、SSH、SNMPなどのTCP/IPプロトコルを介してストレージシステムにアクセスできます。



リモート管理デバイスとe0Mの両方を使用する場合は、同じIPサブネット上に設定する必要があります。これらは低帯域幅のインターフェイスであるため、SP / BMCおよびe0Mは管理トラフィック専用のサブネットに設定することを推奨します。

管理トラフィックを分離できない場合や、専用の管理ネットワークの規模が非常に大きい場合は、ネットワークトラフィックの量をできるだけ少なく抑える必要があります。入力ブロードキャストやマルチキャストトラフィックが多すぎると、SP / BMCのパフォーマンスが低下する可能性があります。



AFF A800などの一部のストレージコントローラには外部ポートが2つあり、1つはBMC用、もう1つはe0M用です。これらのコントローラを使用する場合、BMCとe0Mを同じIPサブネットに設定する必要はありません。

ONTAP SP/BMCネットワーク構成について学ぶ

SPのクラスタレベルの自動ネットワーク設定を有効にすることができます（推奨）。また、SPの自動ネットワーク設定を無効（デフォルト）のままにして、ノードレベルでSPネットワーク設定を手動で管理することもできます。それぞれのケースには、いくつかの考慮事項があります。



このトピックは、SPとBMCの両方に適用されます。

SP自動ネットワーク構成を使用すると、SPは指定されたサブネットのアドレスリソース（IPアドレス、サブネットマスク、ゲートウェイアドレスなど）を使用して、ネットワークを自動的に設定できます。SP自動ネットワーク構成を使用すると、各ノードのSPにIPアドレスを手動で割り当てる必要がなくなります。デフォルトでは、SP自動ネットワーク構成は無効になっています。これは、構成を有効にするには、まずクラスタ内で構成に使用するサブネットを定義する必要があるためです。

SP自動ネットワーク構成を有効にすると、次のシナリオと考慮事項が適用されます：

- SP が一度も設定されていない場合、SP ネットワークは SP 自動ネットワーク設定に指定されたサブネットに基づいて自動的に設定されます。
- SPが以前に手動で設定されていた場合、または既存のSPネットワーク設定が別のサブネットに基づいている場合は、クラスタ内のすべてのノードのSPネットワークが、SP自動ネットワーク設定で指定したサブネットに基づいて再構成されます。

再構成によりSPに異なるアドレスが割り当てられる可能性があり、DNS設定とSPホスト名の解決能力に影響が出る可能性があります。そのため、DNS設定の更新が必要になる場合があります。

- クラスタに参加するノードには、指定したサブネットを使用してSPネットワークが自動的に設定されます。
- `system service-processor network modify` コマンドでは SP IP アドレスを変更することはできません。

SP自動ネットワーク構成が有効になっている場合、このコマンドではSPネットワーク インターフェイスの有効化または無効化のみが可能です。

- SP自動ネットワーク構成が以前に有効になっていた場合、SPネットワーク インターフェイスを無効にすると、割り当てられたアドレス リソースが解放され、サブネットに返されます。
- SPネットワーク インターフェイスを無効にしてから再度有効にすると、SPが別のアドレスで再構成される可能性があります。

SP自動ネットワーク構成が無効になっている場合（デフォルト）、次のシナリオと考慮事項が適用されます：

- SP が一度も設定されていない場合、SP IPv4 ネットワーク設定はデフォルトで IPv4 DHCP を使用し、IPv6 は無効になります。

クラスターに参加するノードも、デフォルトで SP ネットワーク構成に IPv4 DHCP を使用します。

- `system service-processor network modify` コマンドを使用すると、ノードのSP IPアドレスを設定できます。

サブネットに割り当てられているアドレスを使用してSPネットワークを手動で設定しようとする、警告メッセージが表示されます。警告を無視して手動でアドレスを割り当て続けると、アドレスが重複する可能性があります。

SP自動ネットワーク構成が以前に有効にされた後に無効にされた場合、次のシナリオと考慮事項が適用されます：

- SP自動ネットワーク構成でIPv4アドレス ファミリーが無効になっている場合、SP IPv4ネットワークはデフォルトでDHCPを使用するように設定され、`system service-processor network modify` コマンドを使用し

て個々のノードのSP IPv4構成を変更できます。

- SP自動ネットワーク構成でIPv6アドレス ファミリが無効になっている場合は、SP IPv6ネットワークも無効になり、`system service-processor network modify` コマンドを使用すると、個々のノードのSP IPv6構成を有効にして変更できます。

ONTAP SP/BMC自動ネットワーク構成を有効にする

SPネットワークを手動で設定するよりも、SPの自動ネットワーク設定を有効にすることを推奨します。SP自動ネットワーク設定はクラスタ全体で行われるため、個々のノードのSPネットワークを手動で管理する必要はありません。



この作業は、SPとBMCの両方に当てはまります。

- SP自動ネットワーク設定には、クラスタ内に定義済みで、SPネットワーク インターフェイスとリソースが競合しないサブネットを使用する必要があります。

`network subnet show` コマンドは、クラスタのサブネット情報を表示します。

`network subnet show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/network-subnet-show.html>["ONTAPコマンド リファレンス"^]を参照してください。

サブネットの関連付けを強制するパラメータ（`-force-update-lif-associations` コマンドの `network subnet` パラメータ）は、ネットワーク LIF でのみサポートされ、SP ネットワーク インターフェイスではサポートされません。

- SPにIPv6接続を使用する場合は、ONTAPに対してIPv6がすでに設定され、有効になっている必要があります。

`network options ipv6 show` コマンドは、ONTAPのIPv6設定の現在の状態を表示します。link:<https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html>["ONTAPコマンド リファレンス"^]の`network options ipv6 show`の詳細を確認してください。

手順

1. `system service-processor network auto-configuration enable` コマンドを使用して、SPが使用するサブネットのIPv4またはIPv6アドレスファミリと名前を指定します。
2. `system service-processor network auto-configuration show` コマンドを使用して SP 自動ネットワーク構成を表示します。
3. その後、クォーラム内のすべてのノードの SP IPv4 または IPv6 ネットワーク インターフェイスを無効にしたり再度有効にしたりする場合は、`system service-processor network modify` コマンドに`-address-family [IPv4|IPv6]`パラメータおよび`-enable [true|false]`パラメータを指定して使用します。

SP自動ネットワーク構成が有効になっている場合、クォーラム内のノードのSP IPアドレスを変更することはできません。SP IPv4またはIPv6ネットワークインターフェースの有効化または無効化のみ可能です。

ノードがクォーラム外にある場合、ノードから `system service-processor network modify` を実行し、そのノードの SP 自動ネットワーク構成を上書きすることを確認することで、SP IP アドレスを含むノードの SP ネットワーク構成を変更できます。ただし、ノードがクォーラムに参加すると、指定されたサブネットに基づいてノードの SP 自動再構成が実行されます。

ONTAP SP/BMCネットワークを手動で設定する

SPに自動ネットワーク構成が設定されていない場合は、IPアドレスを使用してSPにアクセスできるように、ノードのSPネットワークを手動で構成する必要があります。

開始する前に

SPでIPv6接続を使用する場合は、ONTAPでIPv6がすでに設定され、有効化されている必要があります。`network options ipv6` コマンドはONTAPのIPv6設定を管理します。["ONTAPコマンド リファレンス"](#)の`network options ipv6`の詳細を確認してください。



この作業は、SPとBMCの両方に当てはまります。

SPはIPv4、IPv6、またはその両方を使用するように設定できます。SPのIPv4設定では静的アドレス指定とDHCPアドレス指定がサポートされ、SPのIPv6設定では静的アドレス指定のみがサポートされます。

SP自動ネットワーク構成が設定されている場合は、個々のノードに対してSPネットワークを手動で構成する必要はなく、`system service-processor network modify` コマンドを使用してSPネットワーク インターフェイスを有効または無効にすることのみが可能です。

手順

1. `system service-processor network modify` コマンドを使用して、ノードのSPネットワークを構成します。

- `address-family` パラメータは、SPのIPv4構成またはIPv6構成のどちらを変更するかを指定します。
- `enable` パラメーターは、指定されたIPアドレスファミリのネットワークインターフェイスを有効にします。
- `dhcp` パラメータは、DHCPサーバからのネットワーク構成を使用するか、指定したネットワークアドレスを使用するかを指定します。

IPv4を使用している場合のみ、DHCPを有効にできます（`dhcp` を `v4` に設定）。IPv6構成ではDHCPを有効にできません。

- `ip-address` パラメータは、SP のパブリック IP アドレスを指定します。

サブネットに割り当てられているアドレスを使用してSPネットワークを手動で設定しようとする、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、アドレスが重複して割り当てられる可能性があります。

- `netmask` パラメータは、SP のネットマスクを指定します（IPv4 を使用している場合）。
- `prefix-length` パラメータは、SPのサブネットマスクのネットワークプレフィックス長を指定します（IPv6を使用している場合）。

- `-gateway` パラメータは、SPのゲートウェイIPアドレスを指定します。
2. 手順1を繰り返して、クラスタ内の残りのノードのSPネットワークを設定します。
 3. `system service-processor network show` コマンドに `-instance` または `-field setup-status` パラメータを指定して、SPネットワーク構成を表示し、SPセットアップステータスを確認します。

ノードの SP セットアップ ステータスは次のいずれかになります：

- `not-setup` — 設定されていません
- `succeeded` — 構成に成功しました
- `in-progress` — 構成中
- `failed` — 構成に失敗しました

SPネットワークの構成例

次の例では、ノードのSPをIPv4を使用するように設定し、SPを有効にし、SPネットワーク設定を表示して設定を確認します：

```

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::>

```

ONTAPサービスプロセッサAPI構成を変更する

SP APIは、ONTAPがネットワーク経由でSPと通信できるようにするセキュアなネットワークAPIです。SP APIサービスが使用するポートの変更、サービスが内部通信に使用する証明書の更新、またはサービス全体の無効化を実行できます。設定の変更が必要になるのは、ごくまれな状況のみです。

タスク概要

- SP APIサービスはデフォルトでポート `50000` を使用します。

たとえば、ポート `50000` が別のネットワークアプリケーションによる通信に使用されているネットワーク設定の場合や、他のアプリケーションからのトラフィックとSP APIサービスによって生成されたトラフィックを区別する場合は、ポート値を変更できます。

- SP APIサービスで使用されるSSLおよびSSH証明書は、クラスター内部のものであり、外部には配布され

ません。

万が一、証明書が侵害された場合は、証明書を更新することができます。

- SP APIサービスはデフォルトで有効になっています。

SP APIサービスを無効にする必要があるのは、SPが構成または使用されていないプライベートLANでサービスを無効にしたい場合など、まれな状況のみです。

SP APIサービスが無効になっている場合、APIは着信接続を一切受け入れません。さらに、ネットワークベースのSPファームウェアアップデートやネットワークベースのSP「down system」ログ収集などの機能も利用できなくなります。システムはシリアル管理インターフェイスを使用するように切り替わります。

手順

1. ``set -privilege advanced`` コマンドを使用して、advanced権限レベルに切り替えます。
2. SP APIサービス設定を次のように変更します。

状況	次のコマンドを使用します...
SP APIサービスで使用するポートを変更する	<code>system service-processor api-service modify`と`-port {49152.65535}</code> パラメータ
SP APIサービスの内部通信に使用されるSSL証明書およびSSH証明書の更新	<ul style="list-style-type: none">• ONTAP 9.5以降の場合は <code>`system service-processor api-service renew-internal-certificate`</code> を使用します• ONTAP 9.4以前：• <code>system service-processor api-service renew-certificates</code> <p>パラメータが指定されていない場合は、ホスト証明書（クライアント証明書とサーバー証明書を含む）のみが更新されます。</p> <div><code>`-renew-all true`</code>パラメータを指定すると、ホスト証明書とルートCA証明書の両方が更新されます。</div>
comm	
SP APIサービスを無効化または再度有効化する	<code>system service-processor api-service modify`と`-is-enabled {true</code>

3. ``system service-processor api-service show`` コマンドを使用してSP APIサービス構成を表示します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。