



ネットワークガイドライン StorageGRID software

NetApp
December 03, 2025

目次

ネットワークガイドライン	1
ネットワークガイドライン	1
これらの指示について	1
開始する前に	1
StorageGRIDネットワークの種類	2
交通の種類	2
ネットワーク インターフェイス	3
グリッド ネットワーク	4
管理者ネットワーク	4
クライアント ネットワーク	5
オプションのVLANネットワーク	6
ネットワークトポロジの例	6
グリッドネットワークトポロジ	6
管理者ネットワークトポロジ	7
クライアントネットワークトポロジ	9
3つのネットワークのトポロジ	11
ネットワーク要件	12
一般的なネットワーク要件	12
複数サイト向けの広域ネットワーク (WAN)	13
管理ノードとゲートウェイノードの接続	14
ネットワークアドレス変換 (NAT) の使用	14
ネットワーク固有の要件	14
ネットワークゲートウェイとルーター	14
サブネット	14
グリッド ネットワーク	15
管理者ネットワーク	16
クライアント ネットワーク	16
展開固有のネットワークに関する考慮事項	16
Linux の展開	16
プラットフォーム サービスとクラウド ストレージ プールのネットワークとポート	18
アプライアンスノード	19
ネットワークのインストールとプロビジョニング	20
ノードの初期展開	20
プライマリ管理ノードによる自動ノード登録	20
管理ネットワークまたはクライアントネットワークを無効にする	20
インストール後のガイドライン	20
ネットワークポートリファレンス	21
内部でのGridノードの通信	21
外部コミュニケーション	25

ネットワークガイドライン

ネットワークガイドライン

これらのガイドラインを使用して、StorageGRIDアーキテクチャとネットワークトポロジについて学習し、ネットワーク構成とプロビジョニングの要件を学習します。

これらの指示について

これらのガイドラインは、StorageGRIDノードを展開および構成する前に、StorageGRIDネットワークインフラストラクチャを作成するために使用できる情報を提供します。これらのガイドラインを使用すると、グリッド内のすべてのノード間、およびグリッドと外部のクライアントやサービス間で通信が確実に行われるようになります。

外部クライアントと外部サービスは、次のような機能を実行するためにStorageGRIDネットワークに接続する必要があります。

- オブジェクトデータの保存と取得
- メール通知を受け取る
- StorageGRID管理インターフェース（グリッドマネージャとテナントマネージャ）にアクセスします
- 監査共有にアクセスする（オプション）
- 次のようなサービスを提供します：
 - ネットワーク タイム プロトコル（NTP）
 - ドメインネームシステム（DNS）
 - キー管理サーバー（KMS）

これらの機能などのトラフィックを処理するには、StorageGRIDネットワークを適切に構成する必要があります。

開始する前に

StorageGRIDシステムのネットワークを構成するには、イーサネットスイッチング、TCP/IPネットワーク、サブネット、ネットワークルーティング、ファイアウォールに関する高度な経験が必要です。

ネットワークを構成する前に、StorageGRIDアーキテクチャについて理解しておいてください。["StorageGRIDについて学ぶ"](#)。

使用するStorageGRIDネットワークとそれらのネットワークの構成方法を決定したら、適切な手順に従ってStorageGRIDノードをインストールおよび構成できます。

アプライアンスノードをインストールする

- ["アプライアンスのハードウェアをインストールする"](#)

ソフトウェアベースのノードをインストールする

- ["Red Hat Enterprise LinuxにStorageGRIDをインストールする"](#)

- ["UbuntuまたはDebianにStorageGRIDをインストールする"](#)
- ["VMwareにStorageGRIDをインストールする"](#)

StorageGRIDソフトウェアの構成と管理

- ["StorageGRIDの管理"](#)
- ["リリースノート"](#)

StorageGRIDネットワークの種類

StorageGRIDシステム内のグリッド ノードは、グリッド トラフィック、管理トラフィック、および クライアント トラフィック を処理します。これら 3 種類のトラフィックを管理し、制御とセキュリティを提供するには、ネットワークを適切に構成する必要があります。

交通の種類

交通の種類	説明	ネットワークタイプ
グリッドトラフィック	グリッド内のすべてのノード間を移動する内部StorageGRIDトラフィック。すべてのグリッド ノードは、このネットワークを介して他のすべてのグリッド ノードと通信する必要があります。	グリッドネットワーク (必須)
管理者トラフィック	システムの管理とメンテナンスに使用されるトラフィック。	管理者ネットワーク (オプション) VLANネットワーク (オプション)
クライアントトラフィック	S3 クライアントからのすべてのオブジェクト ストレージ要求を含む、外部クライアント アプリケーションとグリッド間を移動するトラフィック。	クライアントネットワーク (オプション) VLANネットワーク (オプション)

ネットワークは次の方法で構成できます。

- グリッドネットワークのみ
- グリッドと管理ネットワーク
- グリッドとクライアントネットワーク
- グリッド、管理、クライアントネットワーク

グリッド ネットワークは必須であり、すべてのグリッド トラフィックを管理できます。管理ネットワークとクライアント ネットワークは、インストール時に含めることも、要件の変更に合わせて後で追加することもできます。管理ネットワークとクライアント ネットワークはオプションですが、これらのネットワークを使用して管理トラフィックとクライアント トラフィックを処理すると、グリッド ネットワークを分離して安全にすることができます。

内部ポートにはグリッド ネットワーク経由でのみアクセスできます。外部ポートはすべてのネットワーク タイプからアクセスできます。この柔軟性により、StorageGRID の展開を設計し、スイッチとファイアウォー

ルで外部 IP およびポート フィルタリングを設定するための複数のオプションが提供されます。見る["内部グリッドノード通信"](#)そして["外部コミュニケーション"](#)。

ネットワーク インターフェイス

StorageGRIDノードは、次の特定のインターフェイスを使用して各ネットワークに接続されます。

ネットワーク	インターフェイス名
グリッドネットワーク (必須)	eth0
管理者ネットワーク (オプション)	eth1
クライアントネットワーク (オプション)	eth2

仮想ポートまたは物理ポートをノード ネットワーク インターフェイスにマッピングする方法の詳細については、インストール手順を参照してください。

ソフトウェアベースのノード

- ["Red Hat Enterprise LinuxにStorageGRIDをインストールする"](#)
- ["UbuntuまたはDebianにStorageGRIDをインストールする"](#)
- ["VMwareにStorageGRIDをインストールする"](#)

アプライアンスノード

- ["SG6160 ストレージアプライアンス"](#)
- ["SGF6112 ストレージアプライアンス"](#)
- ["SG6000ストレージアプライアンス"](#)
- ["SG5800 ストレージアプライアンス"](#)
- ["SG5700 ストレージアプライアンス"](#)
- ["SG110およびSG1100サービス アプライアンス"](#)
- ["SG100およびSG1000サービス アプライアンス"](#)

各ノードのネットワーク情報

ノード上で有効にするネットワークごとに以下を構成する必要があります。

- IPアドレス
- サブネット マスク
- ゲートウェイのIPアドレス

各グリッド ノード上の 3 つのネットワークごとに、IP アドレス/マスク/ゲートウェイの組み合わせを 1 つだけ構成できます。ネットワークのゲートウェイを構成しない場合は、IP アドレスをゲートウェイ アドレスとして使用する必要があります。

高可用性グループ

高可用性 (HA) グループは、グリッドまたはクライアント ネットワーク インターフェイスに仮想 IP (VIP) アドレスを追加する機能を提供します。詳細については、以下を参照してください。 ["高可用性グループの管理"](#)。

グリッド ネットワーク

グリッド ネットワークが必要です。これは、すべての内部StorageGRIDトラフィックに使用されます。グリッド ネットワークは、すべてのサイトおよびサブネットにわたるグリッド内のすべてのノード間の接続を提供します。グリッド ネットワーク上のすべてのノードは、他のすべてのノードと通信できる必要があります。グリッド ネットワークは複数のサブネットで構成できます。NTP などの重要なグリッド サービスを含むネットワークも、グリッド サブネットとして追加できます。



StorageGRID は、ノード間のネットワーク アドレス変換 (NAT) をサポートしていません。

管理ネットワークとクライアント ネットワークが構成されている場合でも、グリッド ネットワークはすべての管理トラフィックとすべてのクライアント トラフィックに使用できます。ノードにクライアント ネットワークが構成されていない限り、グリッド ネットワーク ゲートウェイがノードのデフォルト ゲートウェイになります。



グリッド ネットワークを構成するときは、オープン インターネット上のクライアントなどの信頼できないクライアントからネットワークが保護されていることを確認する必要があります。

グリッド ネットワーク ゲートウェイの次の要件と詳細に注意してください。

- グリッド サブネットが複数ある場合は、グリッド ネットワーク ゲートウェイを構成する必要があります。
- グリッド構成が完了するまで、グリッド ネットワーク ゲートウェイはノードのデフォルト ゲートウェイになります。
- グローバル グリッド ネットワーク サブネット リストに設定されているすべてのサブネットへのすべてのノードに対して、静的ルートが自動的に生成されます。
- クライアント ネットワークが追加されると、グリッド構成が完了すると、デフォルト ゲートウェイはグリッド ネットワーク ゲートウェイからクライアント ネットワーク ゲートウェイに切り替わります。

管理者ネットワーク

管理ネットワークはオプションです。設定すると、システム管理およびメンテナンス トラフィックに使用できます。管理ネットワークは通常はプライベート ネットワークであり、ノード間でルーティング可能である必要はありません。

管理ネットワークを有効にするグリッド ノードを選択できます。

管理ネットワークを使用する場合、管理およびメンテナンスのトラフィックはグリッド ネットワークを通過する必要がありません。管理ネットワークの一般的な用途は次のとおりです。

- Grid Manager および Tenant Manager ユーザー インターフェイスへのアクセス。
- NTP サーバー、DNS サーバー、外部キー管理サーバー (KMS)、Lightweight Directory Access Protocol (LDAP) サーバーなどの重要なサービスへのアクセス。

- 管理ノード上の監査ログへのアクセス。
- メンテナンスとサポートのためのセキュア シェル プロトコル (SSH) アクセス。

管理ネットワークは、内部グリッド トラフィックには使用されません。管理ネットワーク ゲートウェイが提供され、管理ネットワークが複数の外部サブネットと通信できるようになります。ただし、管理ネットワーク ゲートウェイはノードのデフォルト ゲートウェイとして使用されることはありません。

管理ネットワーク ゲートウェイの次の要件と詳細に注意してください。

- 管理ネットワーク サブネットの外部から接続を行う場合、または複数の管理ネットワーク サブネットが構成されている場合は、管理ネットワーク ゲートウェイが必要です。
- ノードの管理ネットワーク サブネット リストに設定されているサブネットごとに静的ルートが作成されます。

クライアント ネットワーク

クライアント ネットワークはオプションです。設定すると、S3 などのクライアント アプリケーションにグリッド サービスへのアクセスを提供するために使用されます。StorageGRIDデータを外部リソース (クラウド ストレージ プールやStorageGRID CloudMirror レプリケーション サービスなど) からアクセスできるようにする場合は、外部リソースでもクライアント ネットワークを使用できます。グリッド ノードは、クライアント ネットワーク ゲートウェイを介して到達可能な任意のサブネットと通信できます。

どのグリッド ノードでクライアント ネットワークを有効にするかを選択できます。すべてのノードが同じクライアント ネットワーク上にある必要はなく、ノードがクライアント ネットワークを介して相互に通信することはありません。グリッドのインストールが完了するまで、クライアント ネットワークは動作しません。

セキュリティを強化するために、ノードのクライアント ネットワーク インターフェイスを信頼できないものとして指定し、クライアント ネットワークで許可される接続をより制限することができます。ノードのクライアント ネットワーク インターフェイスが信頼されていない場合、インターフェイスは CloudMirror レプリケーションで使用されるような送信接続を受け入れますが、ロード バランサーのエンドポイントとして明示的に構成されたポート上の受信接続のみを受け入れます。見る"[ファイアウォール制御を管理する](#)"そして"[ロードバランサーのエンドポイントを構成する](#)"。

クライアント ネットワークを使用する場合、クライアント トラフィックはグリッド ネットワークを通過する必要がありません。グリッド ネットワーク トラフィックは、安全でルーティング不可能なネットワークに分離できます。多くの場合、次のノード タイプがクライアント ネットワークで構成されます。

- ゲートウェイ ノード。これらのノードは、StorageGRIDロード バランサー サービスへのアクセスと、グリッドへの S3 クライアント アクセスを提供するためです。
- ストレージ ノード。これらのノードは、S3 プロトコル、クラウド ストレージ プール、および CloudMirror レプリケーション サービスへのアクセスを提供するためです。
- 管理ノードは、テナント ユーザーが管理ネットワークを使用しなくてもテナント マネージャーに接続できるようにします。

クライアント ネットワーク ゲートウェイについては、次の点に注意してください。

- クライアント ネットワークが構成されている場合は、クライアント ネットワーク ゲートウェイが必要です。
- グリッド構成が完了すると、クライアント ネットワーク ゲートウェイがグリッド ノードのデフォルト ルートになります。

オプションのVLANネットワーク

必要に応じて、クライアントトラフィックおよび一部の種類の管理トラフィックに仮想 LAN (VLAN) ネットワークを使用することもできます。ただし、グリッドトラフィックでは VLAN インターフェイスを使用できません。ノード間の内部StorageGRIDトラフィックは、常に eth0 上のグリッドネットワークを使用する必要があります。

VLAN の使用をサポートするには、ノード上の 1 つ以上のインターフェイスをスイッチのトランク インターフェイスとして設定する必要があります。グリッドネットワーク インターフェイス (eth0) またはクライアントネットワーク インターフェイス (eth2) をトランクとして構成したり、ノードにトランク インターフェイスを追加したりできます。

eth0 がトランクとして設定されている場合、グリッドネットワークトラフィックは、スイッチで設定されているとおりにトランク ネイティブ インターフェイスを介して流れます。同様に、eth2 がトランクとして設定され、クライアントネットワークも同じノード上に設定されている場合、クライアントネットワークはスイッチ上に設定されているトランク ポートのネイティブ VLAN を使用します。

VLAN ネットワークでは、SSH、グリッド マネージャー、テナント マネージャー トラフィックなどに使用される受信管理トラフィックのみがサポートされます。NTP、DNS、LDAP、KMS、クラウドストレージプールなどに使用される送信トラフィックは、VLAN ネットワーク経由ではサポートされません。



VLAN インターフェイスは、管理ノードとゲートウェイ ノードにのみ追加できます。ストレージ ノードへのクライアントまたは管理者のアクセスには VLAN インターフェイスを使用できません。

見る"[VLANインターフェイスを構成する](#)"手順とガイドラインについてはこちらをご覧ください。

VLAN インターフェイスは HA グループでのみ使用され、アクティブ ノードで VIP アドレスが割り当てられます。見る"[高可用性グループの管理](#)"手順とガイドラインについてはこちらをご覧ください。

ネットワークトポロジの例

グリッドネットワークトポロジ

最も単純なネットワーク トポロジは、グリッド ネットワークのみを構成することによって作成されます。

グリッド ネットワークを構成するときは、各グリッド ノードの eth0 インターフェイスのホスト IP アドレス、サブネット マスク、およびゲートウェイ IP アドレスを確立します。

構成中に、すべてのグリッド ネットワーク サブネットをグリッド ネットワーク サブネット リスト (GNSL) に追加する必要があります。このリストにはすべてのサイトのすべてのサブネットが含まれており、NTP、DNS、LDAP などの重要なサービスへのアクセスを提供する外部サブネットも含まれる場合があります。

インストール時に、グリッド ネットワーク インターフェイスは GNSL 内のすべてのサブネットに静的ルートを適用し、ノードのデフォルト ルートをグリッド ネットワーク ゲートウェイに設定します (構成されている場合)。クライアント ネットワークが存在せず、グリッド ネットワーク ゲートウェイがノードのデフォルト ルートである場合、GNSL は必要ありません。グリッド内の他のすべてのノードへのホスト ルートも生成されます。

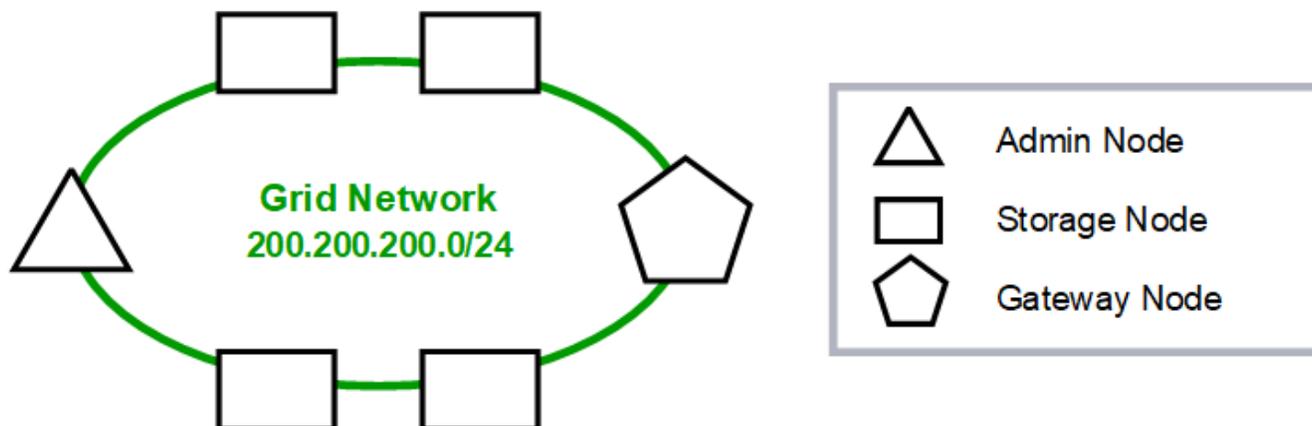
この例では、S3 クライアント要求や管理およびメンテナンス機能に関連するトラフィックを含め、すべての

トラフィックが同じネットワークを共有します。



このトポロジは、外部から利用できない単一サイトの展開、概念実証またはテストの展開、またはサードパーティのロード バランサーがクライアント アクセス境界として機能する場合に適しています。可能な場合は、グリッド ネットワークを内部トラフィック専用を使用する必要があります。管理ネットワークとクライアント ネットワークの両方に、内部サービスへの外部トラフィックをブロックする追加のファイアウォール制限があります。外部クライアント トラフィックにグリッド ネットワークを使用することはサポートされていますが、この使用方法では保護層が少なくなります。

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
Nodes	Grid Network	
	IP/mask	Gateway
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes	Type	From
All	0.0.0.0/0 → 200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24 → eth0	Link	Interface IP/mask

管理者ネットワークトポロジ

管理者ネットワークを持つことはオプションです。管理ネットワークとグリッド ネット

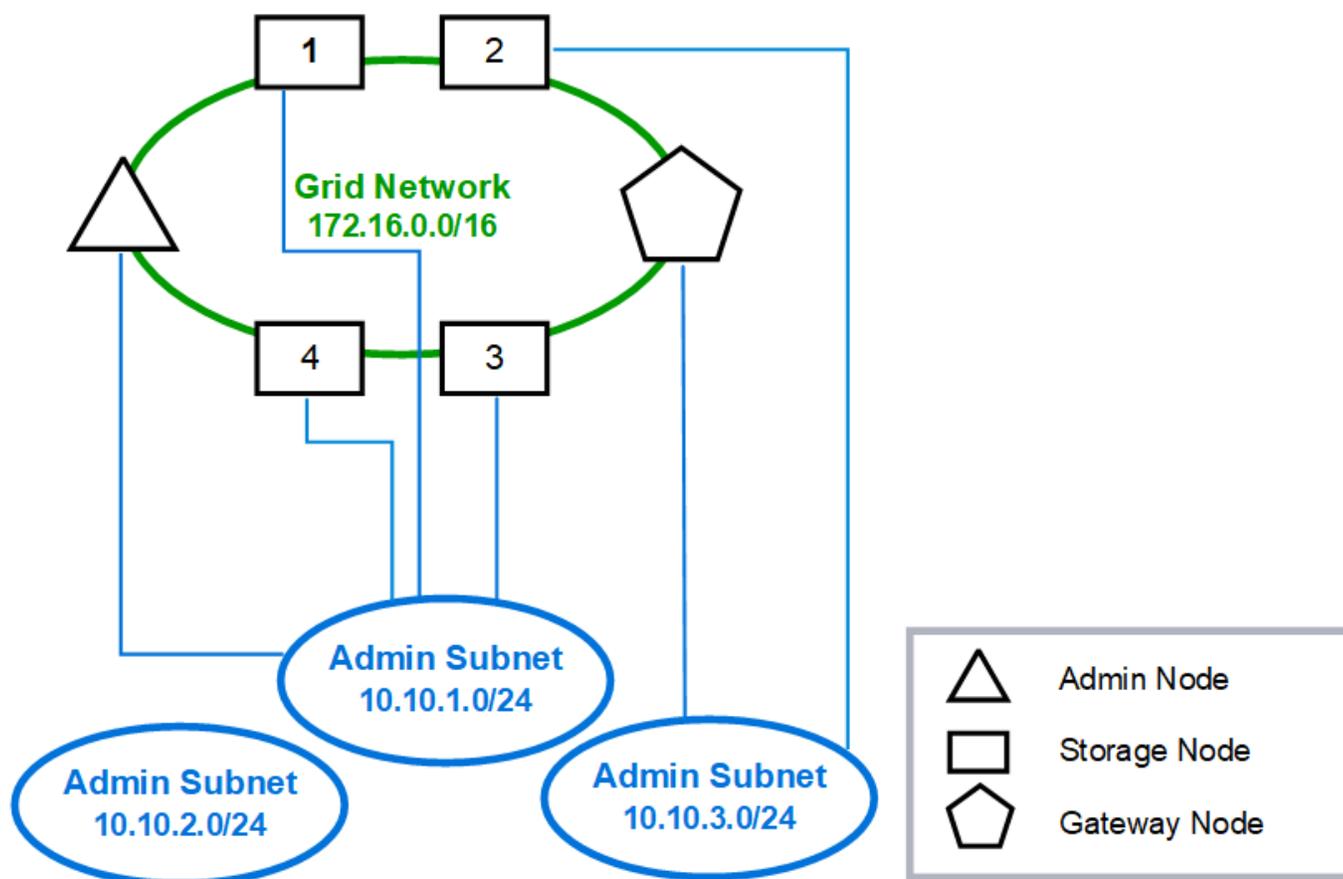
ワークを使用する 1 つの方法は、各ノードに対してルーティング可能なグリッド ネットワークと境界付き管理ネットワークを構成することです。

管理ネットワークを構成するときは、各グリッド ノードの eth1 インターフェイスのホスト IP アドレス、サブネット マスク、およびゲートウェイ IP アドレスを確立します。

管理ネットワークは各ノードに固有であり、複数のサブネットで構成できます。各ノードは、管理外部サブネット リスト (AESL) を使用して構成できます。AESL には、各ノードの管理ネットワーク経由で到達可能なサブネットがリストされます。AESL には、NTP、DNS、KMS、LDAP など、グリッドが管理ネットワーク経由でアクセスするすべてのサービスのサブネットも含める必要があります。AESL 内の各サブネットに静的ルートが適用されます。

この例では、グリッド ネットワークは S3 クライアント要求とオブジェクト管理に関連するトラフィックに使用され、管理ネットワークは管理機能に使用されます。

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	IP/mask	Gateway	IP/mask	Gateway
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes	Type	From
All	0.0.0.0/0 → 172.16.200.1	Default	Grid Network gateway
Admin,	172.16.0.0/16 → eth0	Static	GNSL
Storage 1,	10.10.1.0/24 → eth1	Link	Interface IP/mask
3, and 4	10.10.2.0/24 → 10.10.1.1	Static	AESL
	10.10.3.0/24 → 10.10.1.1	Static	AESL
Storage 2,	172.16.0.0/16 → eth0	Static	GNSL
Gateway	10.10.1.0/24 → 10.10.3.1	Static	AESL
	10.10.2.0/24 → 10.10.3.1	Static	AESL
	10.10.3.0/24 → eth1	Link	Interface IP/mask

クライアントネットワークトポロジ

クライアント ネットワークを持つことはオプションです。クライアント ネットワークを使用すると、クライアント ネットワーク トラフィック (S3 など) をグリッド内部トラフィックから分離できるため、グリッド ネットワークのセキュリティが強化されます。管理ネットワークが構成されていない場合、管理トラフィックはクライアント ネットワークまたはグリッド ネットワークのいずれかで処理できます。

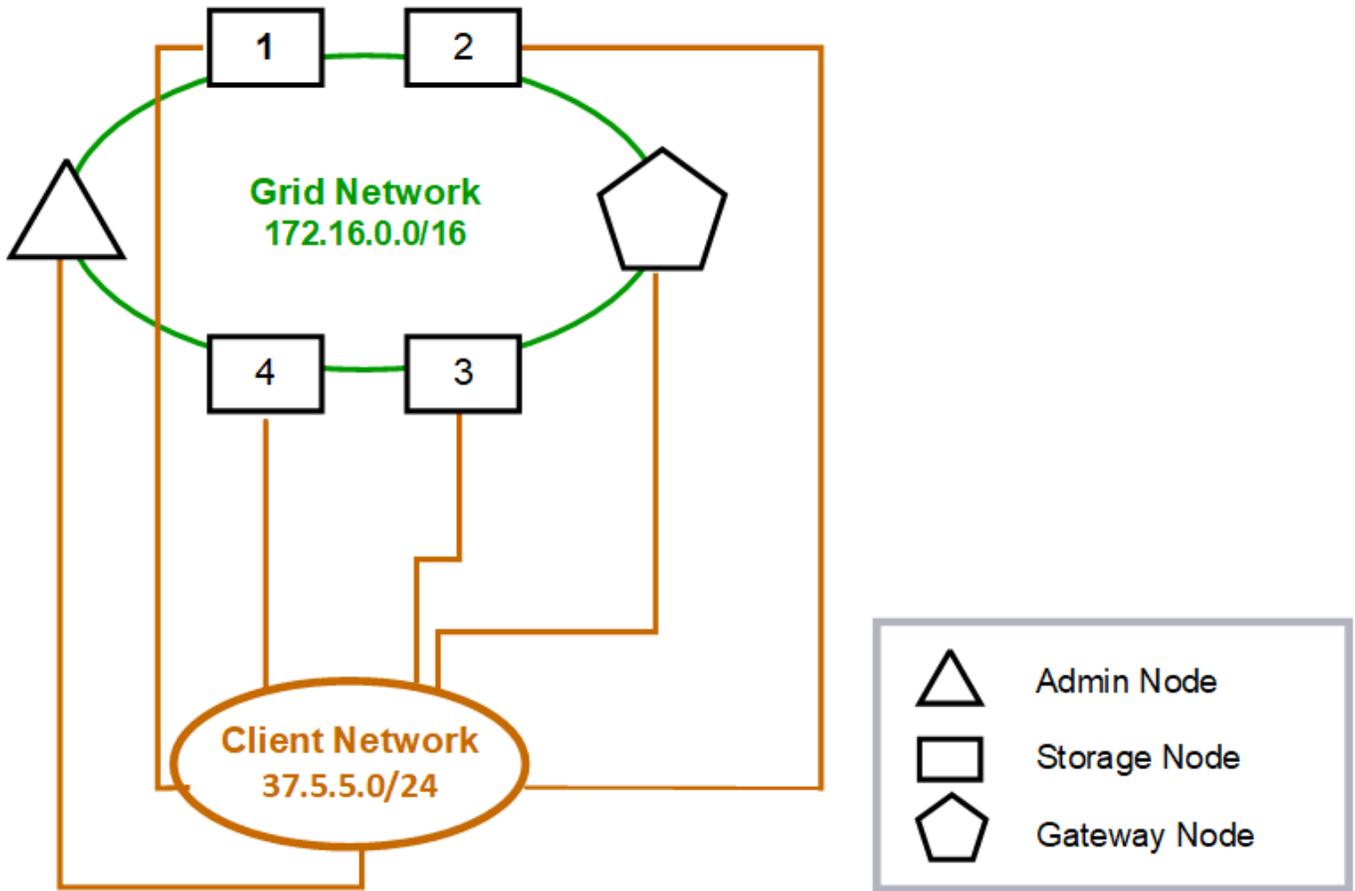
クライアント ネットワークを構成するときは、構成されたノードの eth2 インターフェイスのホスト IP アドレス、サブネット マスク、およびゲートウェイ IP アドレスを確立します。各ノードのクライアント ネットワークは、他のノードのクライアント ネットワークから独立できます。

インストール中にノードのクライアント ネットワークを構成すると、インストールが完了すると、ノードのデフォルト ゲートウェイがグリッド ネットワーク ゲートウェイからクライアント ネットワーク ゲートウェイに切り替わります。後でクライアント ネットワークが追加されると、ノードのデフォルト ゲートウェイも同様に切り替わります。

この例では、クライアント ネットワークは S3 クライアント要求と管理機能に使用され、グリッド ネットワ

ークは内部オブジェクト管理操作専用になります。

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes		Type	From
All	0.0.0.0/0	→ 37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→ eth0	Link	Interface IP/mask
	37.5.5.0/24	→ eth2	Link	Interface IP/mask

関連情報

"ノードネットワーク構成を変更する"

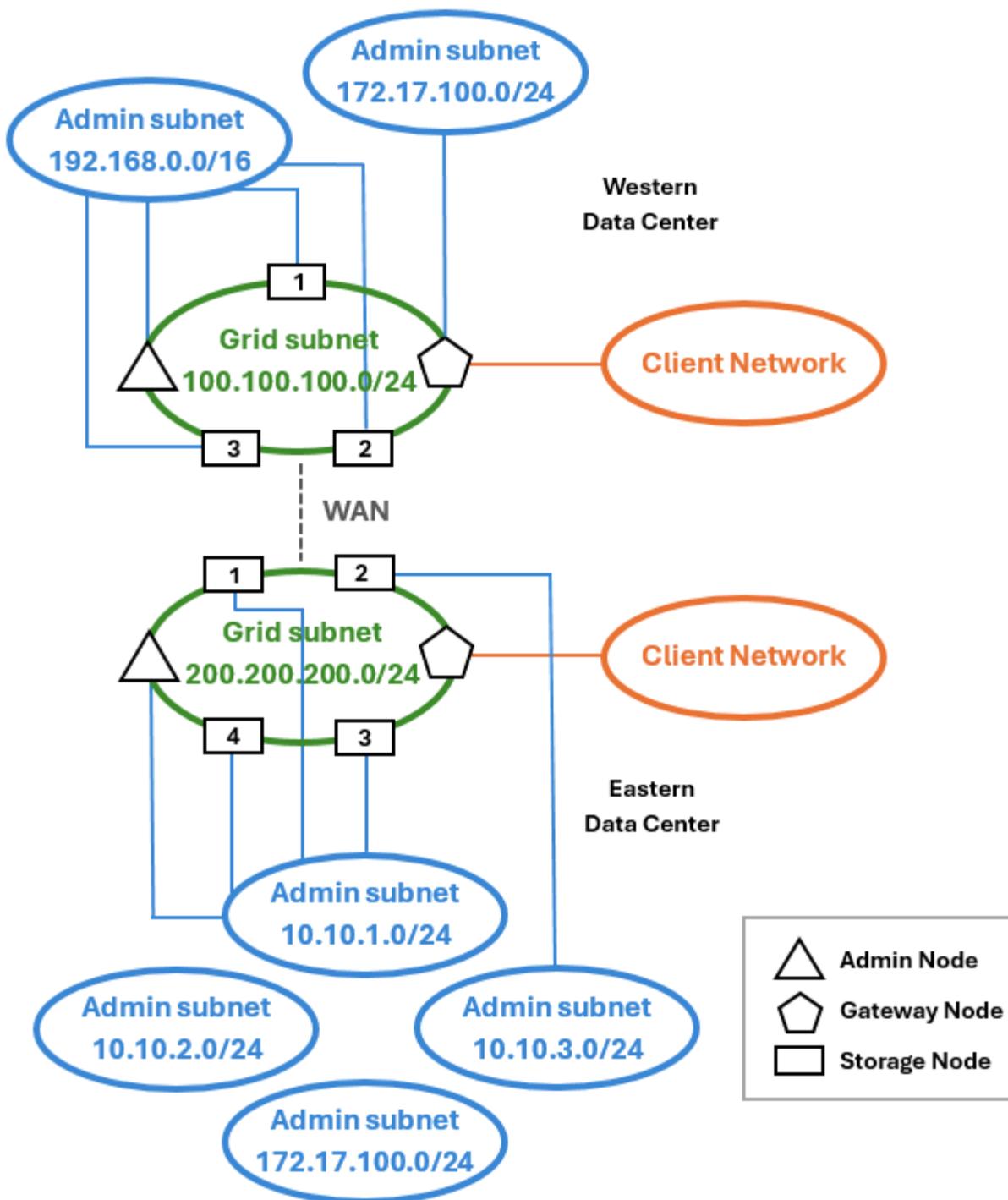
3つのネットワークのトポロジ

これら3つのネットワークすべてを、プライベートグリッドネットワーク、境界付きサイト固有の管理ネットワーク、およびオープンクライアントネットワークで構成されるネットワークトポロジに構成できます。ロードバランサエンドポイントと信頼されていないクライアントネットワークを使用すると、必要に応じてセキュリティを強化できます。

この例では、

- グリッドネットワークは、内部オブジェクト管理操作に関連するネットワークトラフィックに使用されます。
- 管理ネットワークは、管理機能に関連するトラフィックに使用されます。
- クライアントネットワークは、S3クライアント要求に関連するトラフィックに使用されます。

トポロジの例: グリッド、管理、クライアントネットワーク



ネットワーク要件

現在のネットワーク インフラストラクチャと構成が、計画されているStorageGRIDネットワーク設計をサポートできることを確認する必要があります。

一般的なネットワーク要件

すべてのStorageGRIDデプロイメントは、次の接続をサポートできる必要があります。

これらの接続は、ネットワーク トポロジの例に示されているように、グリッド ネットワーク、管理ネットワーク、またはクライアント ネットワーク、あるいはこれらのネットワークの組み合わせを介して行われます。

- 管理接続: 通常は SSH を介して、管理者からノードへの受信接続。 Grid Manager、Tenant Manager、StorageGRID Appliance Installer への Web ブラウザ アクセス。

- **NTP** サーバー接続: 着信 UDP 応答を受信する発信 UDP 接続。

プライマリ管理ノードから少なくとも 1 つの NTP サーバーにアクセスできる必要があります。

- **DNS** サーバー接続: 着信 UDP 応答を受信する発信 UDP 接続。
- **LDAP/Active Directory** サーバー接続: ストレージ ノード上の Identity サービスからの送信 TCP 接続。
- * AutoSupport*: 管理ノードから次のいずれかへのアウトバウンドTCP接続 `support.netapp.com`または顧客が設定したプロキシ。
- 外部キー管理サーバー: ノード暗号化が有効になっている各アプライアンス ノードからの送信 TCP 接続。
- S3 クライアントからの受信 TCP 接続。
- CloudMirror レプリケーションなどのStorageGRIDプラットフォーム サービスまたは Cloud Storage Pools からの送信要求。

StorageGRID は、デフォルトのルーティング ルールを使用してプロビジョニングされた NTP サーバーまたは DNS サーバーのいずれにも接続できない場合、DNS サーバーおよび NTP サーバーの IP アドレスが指定されている限り、すべてのネットワーク (グリッド、管理、およびクライアント) への接続を自動的に試行します。どのネットワーク上でも NTP サーバーまたは DNS サーバーにアクセスできる場合、StorageGRID は追加のルーティング ルールを自動的に作成し、今後のすべての接続試行でそのネットワークが使用されるようになります。



自動的に検出されたホスト ルートを使用することもできますが、通常は、自動検出が失敗した場合に備えて接続を確保するために、DNS ルートと NTP ルートを手動で構成する必要があります。

デプロイメント中にオプションの管理ネットワークとクライアント ネットワークを構成する準備ができていない場合、構成手順中にグリッド ノードを承認するときにこれらのネットワークを構成できます。さらに、インストール後にIP変更ツール ("[IPアドレスを設定する](#)")。

VLAN インターフェイス経由では、S3 クライアント接続と SSH、Grid Manager、および Tenant Manager 管理接続のみがサポートされます。NTP、DNS、LDAP、AutoSupport、KMS サーバーなどへの送信接続は、クライアント、管理、またはグリッド ネットワーク インターフェイスを直接経由する必要があります。インターフェイスが VLAN インターフェイスをサポートするトランクとして設定されている場合、このトラフィックはスイッチで設定されているインターフェイスのネイティブ VLAN を介して流れます。

複数サイト向けの広域ネットワーク (WAN)

複数のサイトでStorageGRIDシステムを構成する場合、クライアント トラフィックを考慮する前に、サイト間の WAN 接続で各方向に最低 25 Mbit/秒の帯域幅が必要です。サイト間のデータ複製または消去コーディング、ノードまたはサイトの拡張、ノードの回復、およびその他の操作や構成には、追加の帯域幅が必要になります。

実際の最小 WAN 帯域幅要件は、クライアントのアクティビティと ILM 保護スキームによって異なります。最

小 WAN 帯域幅要件の見積もりについては、NetAppプロフェッショナル サービス コンサルタントにお問い合わせください。

管理ノードとゲートウェイノードの接続

管理ノードは、オープンインターネット上のクライアントなどの信頼できないクライアントから常に保護される必要があります。信頼できないクライアントがグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワーク上の管理ノードにアクセスできないようにする必要があります。

高可用性グループに追加する予定の管理ノードとゲートウェイ ノードは、静的 IP アドレスを使用して構成する必要があります。詳細については、以下を参照してください。"[高可用性グループの管理](#)"。

ネットワークアドレス変換 (NAT) の使用

グリッド ノード間またはStorageGRIDサイト間のグリッド ネットワークでは、ネットワーク アドレス変換 (NAT) を使用しないでください。グリッド ネットワークにプライベート IPv4 アドレスを使用する場合、それらのアドレスはすべてのサイトのすべてのグリッド ノードから直接ルーティング可能である必要があります。ただし、必要に応じて、ゲートウェイ ノードにパブリック IP アドレスを提供する場合など、外部クライアントとグリッド ノード間で NAT を使用できます。NAT を使用してパブリック ネットワーク セグメントをブリッジすることは、グリッド内のすべてのノードに対して透過的なトンネリング アプリケーションを使用する場合にのみサポートされます。つまり、グリッド ノードはパブリック IP アドレスを認識する必要はありません。

ネットワーク固有の要件

各StorageGRIDネットワーク タイプの要件に従ってください。

ネットワークゲートウェイとルーター

- 設定されている場合、特定のネットワークのゲートウェイは、特定のネットワークのサブネット内にある必要があります。
- 静的アドレス指定を使用してインターフェイスを構成する場合は、0.0.0.0 以外のゲートウェイ アドレスを指定する必要があります。
- ゲートウェイがない場合は、ゲートウェイ アドレスをネットワーク インターフェイスの IP アドレスに設定するのがベスト プラクティスです。

サブネット



各ネットワークは、ノード上の他のネットワークと重複しない独自のサブネットに接続されている必要があります。

デプロイメント中に、グリッド マネージャーによって次の制限が適用されます。これらは、展開前のネットワーク計画を支援するためにここに提供されています。

- どのネットワーク IP アドレスのサブネット マスクも、255.255.255.254 または 255.255.255.255 (CIDR 表記では /31 または /32) にすることはできません。
- ネットワーク インターフェイスの IP アドレスとサブネット マスク (CIDR) によって定義されたサブネットは、同じノードに構成されている他のインターフェイスのサブネットと重複することはできません。

- どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも、次の IPv4 アドレスを含むサブネットを使用しないでください。
 - 192.168.130.101
 - 192.168.131.101
 - 192.168.130.102
 - 192.168.131.102
 - 198.51.100.2
 - 198.51.100.4

たとえば、どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも次のサブネット範囲を使用しないでください。

- 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
 - 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
 - 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。
- 各ノードのグリッド ネットワーク サブネットを GNSL に含める必要があります。
 - 管理ネットワーク サブネットは、グリッド ネットワーク サブネット、クライアント ネットワーク サブネット、または GNSL 内のどのサブネットとも重複できません。
 - AESL 内のサブネットは、GNSL 内のサブネットと重複できません。
 - クライアント ネットワーク サブネットは、グリッド ネットワーク サブネット、管理ネットワーク サブネット、GNSL 内のサブネット、または AESL 内のサブネットと重複することはできません。

グリッド ネットワーク

- デプロイメント時には、各グリッド ノードをグリッド ネットワークに接続し、ノードのデプロイメント時に指定したネットワーク構成を使用してプライマリ管理ノードと通信する必要があります。
- 通常のグリッド操作中、各グリッド ノードはグリッド ネットワークを介して他のすべてのグリッド ノードと通信する必要があります。



グリッド ネットワークは各ノード間で直接ルーティング可能である必要があります。ノード間のネットワーク アドレス変換 (NAT) はサポートされていません。

- グリッド ネットワークが複数のサブネットで作成されている場合は、それらをグリッド ネットワーク サブネット リスト (GNSL) に追加します。GNSL 内のサブネットごとに、すべてのノードに静的ルートが作成されます。
- グリッド ネットワーク インターフェイスが VLAN インターフェイスをサポートするトランクとして構成されている場合、トランク ネイティブ VLAN は、グリッド ネットワーク トラフィックに使用される VLAN である必要があります。すべてのグリッド ノードは、トランク ネイティブ VLAN 経由でアクセスする必要があります。

管理者ネットワーク

管理ネットワークはオプションです。管理ネットワークを構成する予定の場合は、次の要件とガイドラインに従ってください。

管理ネットワークの一般的な用途には、管理接続、AutoSupport、KMS、およびグリッド ネットワークまたはクライアント ネットワーク経由でこれらの接続が提供されない場合の NTP、DNS、LDAP などの重要なサーバーへの接続が含まれます。



必要なネットワーク サービスとクライアントにアクセスできる限り、管理ネットワークと AESL は各ノードに対して一意にすることができます。



外部サブネットからの受信接続を有効にするには、管理ネットワーク上に少なくとも 1 つのサブネットを定義する必要があります。静的ルートは、AESL 内の各サブネットの各ノードで自動的に生成されます。

クライアント ネットワーク

クライアント ネットワークはオプションです。クライアント ネットワークを構成する予定の場合は、次の考慮事項に注意してください。

- クライアント ネットワークは、S3 クライアントからのトラフィックをサポートするように設計されています。設定されている場合、クライアント ネットワーク ゲートウェイはノードのデフォルト ゲートウェイになります。
- クライアント ネットワークを使用する場合は、明示的に構成されたロード バランサのエンドポイントでのみ受信クライアント トラフィックを受け入れることで、StorageGRID を敵対的な攻撃から保護できます。見る"[ロードバランサのエンドポイントを構成する](#)"。
- クライアント ネットワーク インターフェイスが VLAN インターフェイスをサポートするためにトランクとして構成されている場合は、クライアント ネットワーク インターフェイス (eth2) を構成する必要があるかどうかを検討します。設定されている場合、クライアント ネットワーク トラフィックは、スイッチで設定されているとおりにトランク ネイティブ VLAN を介して流れます。

関連情報

["ノードネットワーク構成を変更する"](#)

展開固有のネットワークに関する考慮事項

Linux の展開

効率性、信頼性、セキュリティを実現するために、StorageGRIDシステムはコンテナ エンジンのコレクションとして Linux 上で実行されます。StorageGRIDシステムでは、コンテナ エンジン関連のネットワーク構成は必要ありません。

コンテナ ネットワーク インターフェイスには、VLAN または仮想イーサネット (veth) ペアなどの非結合デバイスを使用します。ノード構成ファイルでこのデバイスをネットワーク インターフェイスとして指定します。



ボンドまたはブリッジデバイスをコンテナネットワークインターフェースとして直接使用しないでください。これを行うと、コンテナ名前空間内のボンドおよびブリッジデバイスで macvlan を使用する際のカーネルの問題により、ノードの起動が妨げられる可能性があります。

インストール手順については、"[Red Hat Enterprise Linux](#)"または"[Ubuntu](#)または[Debian](#)"デプロイメント。

コンテナ エンジン デプロイメントのホスト ネットワーク構成

コンテナ エンジン プラットフォームでStorageGRID の展開を開始する前に、各ノードが使用するネットワーク (グリッド、管理、クライアント) を決定します。各ノードのネットワーク インターフェイスが正しい仮想または物理ホスト インターフェイス上に構成され、各ネットワークに十分な帯域幅があることを確認する必要があります。

物理ホスト

グリッド ノードをサポートするために物理ホストを使用している場合:

- すべてのホストが各ノード インターフェイスに対して同じホスト インターフェイスを使用していることを確認します。この戦略により、ホスト構成が簡素化され、将来のノード移行が可能になります。
- 物理ホスト自体の IP アドレスを取得します。



ホスト上の物理インターフェイスは、ホスト自体と、ホスト上で実行されている 1 つ以上のノードによって使用できます。このインターフェイスを使用してホストまたはノードに割り当てられる IP アドレスはすべて一意である必要があります。ホストとノードは IP アドレスを共有できません。

- ホストに必要なポートを開きます。
- StorageGRIDで VLAN インターフェイスを使用する場合は、必要な VLAN へのアクセスを提供する 1 つ以上のトランク インターフェイスがホストに必要です。これらのインターフェイスは、eth0、eth2、または追加インターフェイスとしてノード コンテナに渡すことができます。トランクまたはアクセス インターフェイスを追加するには、次を参照してください。
 - **RHEL** (ノードをインストールする前): "[ノード構成ファイルを作成する](#)"
 - **Ubuntu** または **Debian** (ノードをインストールする前): "[ノード構成ファイルを作成する](#)"
 - **RHEL**、**Ubuntu**、または **Debian** (ノードをインストールした後): "[Linux: ノードにトランクまたはアクセスインターフェイスを追加する](#)"

最小帯域幅の推奨事項

次の表は、StorageGRIDノードのタイプとネットワークのタイプごとに、最小 LAN 帯域幅の推奨事項を示しています。各物理ホストまたは仮想ホストに、そのホストで実行する予定のStorageGRIDノードの合計数と合計タイプに対する最小帯域幅要件を満たすのに十分なネットワーク帯域幅をプロビジョニングする必要があります。

ノードの種類	ネットワークの種類		
	Grid	管理者	クライアント

ノードの種類	ネットワークの種類		
	最小LAN帯域幅	管理者	10Gbps
1Gbps	1Gbps	ゲートウェイ	10Gbps
1Gbps	10Gbps	ストレージ	10Gbps
1Gbps	10Gbps	アーカイブ	10Gbps



この表には、共有ストレージへのアクセスに必要な SAN 帯域幅は含まれていません。イーサネット (iSCSI または FCoE) 経由でアクセスされる共有ストレージを使用している場合は、十分な SAN 帯域幅を提供するために、各ホストに個別の物理インターフェイスをプロビジョニングする必要があります。ボトルネックの発生を回避するには、特定のホストの SAN 帯域幅が、そのホストで実行されているすべてのストレージ ノードの合計ストレージ ノード ネットワーク帯域幅とほぼ一致する必要があります。

この表を使用して、各ホストで実行する予定のStorageGRIDノードの数とタイプに基づいて、各ホストでプロビジョニングするネットワーク インターフェイスの最小数を決定します。

たとえば、単一のホストで1つの管理ノード、1つのゲートウェイ ノード、および1つのストレージ ノードを実行するには、次のようにします。

- 管理ノードでグリッドネットワークと管理ネットワークを接続する (10 + 1 = 11 Gbps が必要)
- ゲートウェイノードでグリッドとクライアントネットワークを接続する (10 + 10 = 20 Gbps が必要)
- ストレージノード上のグリッドネットワークを接続する (10 Gbps が必要)

このシナリオでは、少なくとも $11 + 20 + 10 = 41$ Gbps のネットワーク帯域幅を提供する必要があります。これは、2つの 40 Gbps インターフェイスまたは5つの 10 Gbps インターフェイスで対応でき、トランクとして集約され、ホストを含む物理データセンターのローカルのグリッド、管理、およびクライアント サブネットを伝送する3つ以上の VLAN で共有される可能性があります。

StorageGRID の導入に備えて、StorageGRIDクラスタ内のホスト上の物理リソースとネットワーク リソースを構成するための推奨方法については、以下を参照してください。

- ["ホストネットワークを構成する \(Red Hat Enterprise Linux\)"](#)
- ["ホストネットワークを構成する \(UbuntuまたはDebian\) "](#)

プラットフォーム サービスとクラウド ストレージ プールのネットワークとポート

StorageGRIDプラットフォーム サービスまたは Cloud Storage Pools を使用する予定の場合は、宛先エンドポイントに到達できるようにグリッド ネットワークとファイアウォールを構成する必要があります。

プラットフォームサービスのためのネットワークング

記載の通り["テナント向けプラットフォームサービスの管理"](#)そして["プラットフォームサービスの管理"](#)プラットフォーム サービスには、検索統合、イベント通知、CloudMirror レプリケーションを提供する外部サービス

が含まれます。

プラットフォーム サービスでは、StorageGRID ADC サービスをホストするストレージ ノードから外部サービス エンドポイントへのアクセスが必要です。アクセスを提供する例は次のとおりです：

- ADC サービスを備えたストレージ ノードで、ターゲット エンドポイントにルーティングする AESL エントリを使用して一意の管理ネットワークを構成します。
- クライアント ネットワークによって提供されるデフォルト ルートに依存します。デフォルトルートを使用する場合は、"[信頼できないクライアントネットワーク機能](#)"着信接続を制限します。

クラウド ストレージ プールのネットワーク

クラウド ストレージ プールでは、ストレージ ノードから、Amazon S3 Glacier や Microsoft Azure Blob ストレージなどの使用される外部サービスによって提供されるエンドポイントへのアクセスも必要です。詳細については、"[クラウドストレージプールとは](#)"。

プラットフォーム サービスとクラウド ストレージ プールのポート

デフォルトでは、プラットフォーム サービスと Cloud Storage Pool の通信では次のポートが使用されます。

- **80:** で始まるエンドポイントURIの場合 http
- **443:** エンドポイントURIが https

エンドポイントを作成または編集するときに、別のポートを指定できます。見る"[ネットワークポートリファレンス](#)"。

非透過プロキシサーバーを使用する場合は、"[ストレージプロキシ設定を構成する](#)"インターネット上のエンドポイントなどの外部エンドポイントにメッセージを送信できるようにします。

VLANとプラットフォームサービスとクラウドストレージプール

プラットフォーム サービスまたはクラウド ストレージ プールには VLAN ネットワークは使用できません。宛先エンドポイントは、グリッド、管理、またはクライアント ネットワーク経由で到達可能である必要があります。

アプライアンスノード

スループット、冗長性、フェイルオーバーの要件を満たすポート ボンド モードを使用するように、StorageGRIDアプライアンス上のネットワーク ポートを構成できます。

StorageGRIDアプライアンスの 10/25 GbE ポートは、グリッド ネットワークおよびクライアント ネットワークへの接続用に、固定または集約ボンド モードで構成できます。

1 GbE 管理ネットワーク ポートは、管理ネットワークへの接続用に独立モードまたはアクティブ バックアップ モードで構成できます。

アプライアンスのポート ボンド モードに関する情報を参照してください。

- "[ポートボンドモード \(SG6160\)](#) "
- "[ポートボンドモード \(SGF6112\)](#) "

- "ポートボンドモード (SG6000-CNコントローラ) "
- "ポートボンドモード (SG5800コントローラ) "
- "ポートボンドモード (E5700SGコントローラ) "
- "ポートボンドモード (SG110およびSG1100) "
- "ポートボンドモード (SG100およびSG1000) "

ネットワークのインストールとプロビジョニング

ノードの展開およびグリッド構成中に、グリッド ネットワークとオプションの管理ネットワークおよびクライアント ネットワークがどのように使用されるかを理解する必要があります。

ノードの初期展開

ノードを初めてデプロイするときは、ノードをグリッド ネットワークに接続し、プライマリ管理ノードにアクセスできることを確認する必要があります。グリッド ネットワークが分離されている場合は、グリッド ネットワークの外部から構成およびインストールにアクセスできるように、プライマリ管理ノード上に管理ネットワークを構成できます。

ゲートウェイが構成されたグリッド ネットワークは、デプロイメント中にノードのデフォルト ゲートウェイになります。デフォルト ゲートウェイを使用すると、グリッドが構成される前に、別のサブネット上のグリッド ノードがプライマリ管理ノードと通信できるようになります。

必要に応じて、NTP サーバーを含むサブネットや、グリッド マネージャーまたは API へのアクセスを必要とするサブネットも、グリッド サブネットとして構成できます。

プライマリ管理ノードによる自動ノード登録

ノードがデプロイされると、グリッド ネットワークを使用して、ノード自体がプライマリ管理ノードに登録されます。その後、グリッドマネージャを使用して、`configure-storagegrid.py`グリッドを構成し、登録されたノードを承認するための Python スクリプトまたはインストール API。グリッド構成時に、複数のグリッドサブネットを構成できます。グリッド構成が完了すると、グリッド ネットワーク ゲートウェイを介したこれらのサブネットへの静的ルートが各ノードに作成されます。

管理ネットワークまたはクライアントネットワークを無効にする

管理ネットワークまたはクライアントネットワークを無効にしたい場合は、ノード承認プロセス中にそれらの構成を削除するか、インストールが完了した後にIP変更ツールを使用することができます ("IPアドレスを設定する")。

インストール後のガイドライン

グリッド ノードの展開と構成が完了したら、DHCP アドレス指定とネットワーク構成の変更に関する次のガイドラインに従います。

- IP アドレスの割り当てに DHCP が使用されている場合は、使用されているネットワーク上の各 IP アドレスに対して DHCP 予約を構成します。

DHCP を設定できるのは、展開フェーズ中のみです。構成中に DHCP を設定することはできません。



グリッド ネットワーク構成が DHCP によって変更されるとノードが再起動します。DHCP の変更が複数のノードに同時に影響する場合は、停止が発生する可能性があります。

- グリッド ノードの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを変更する場合は、IP の変更手順を使用する必要があります。見る["IP アドレスを設定する"](#)。
- ルーティングやゲートウェイの変更などのネットワーク構成の変更を行うと、プライマリ管理ノードおよびその他のグリッド ノードへのクライアント接続が失われる可能性があります。適用されたネットワークの変更に応じて、これらの接続を再確立する必要がある場合があります。

ネットワークポートリファレンス

内部でのGridノードの通信

StorageGRID内部ファイアウォールは、グリッド ネットワーク上の特定のポートへの着信接続を許可します。接続は、ロード バランサーのエンドポイントによって定義されたポートでも受け入れられます。



NetApp、グリッド ノード間のインターネット制御メッセージ プロトコル (ICMP) トラフィックを有効にすることを推奨しています。ICMP トラフィックを許可すると、グリッド ノードに到達できない場合のフェイルオーバー パフォーマンスが向上します。

ICMP と表に記載されているポートに加えて、StorageGRID は仮想ルータ冗長プロトコル (VRRP) を使用します。VRRP は、IP プロトコル番号 112 を使用するインターネット プロトコルです。StorageGRID は、ユニキャスト モードでのみ VRRP を使用します。VRRPは次の場合にのみ必要です。["高可用性グループ"](#)設定されています。

Linuxベースのノードのガイドライン

エンタープライズ ネットワーク ポリシーによってこれらのポートへのアクセスが制限されている場合は、デプロイメント構成パラメータを使用してデプロイメント時にポートを再マップできます。ポートの再マッピングとデプロイメント構成パラメータの詳細については、以下を参照してください。

- ["Red Hat Enterprise LinuxにStorageGRIDをインストールする"](#)
- ["UbuntuまたはDebianにStorageGRIDをインストールする"](#)

VMwareベースのノードのガイドライン

VMware ネットワーク外部のファイアウォール制限を定義する必要がある場合にのみ、次のポートを構成します。

エンタープライズ ネットワーク ポリシーによってこれらのポートへのアクセスが制限されている場合は、VMware vSphere Web Client を使用してノードを展開するときにポートを再マップするか、グリッド ノードの展開を自動化するときに構成ファイル設定を使用できます。ポートの再マッピングとデプロイメント構成パラメータの詳細については、以下を参照してください。["VMwareにStorageGRIDをインストールする"](#)。

アプライアンスノードのガイドライン

企業のネットワーク ポリシーによってこれらのポートへのアクセスが制限されている場合は、StorageGRID アプライアンス インストーラを使用してポートを再マップできます。見る ["オプション: アプライアンスのネットワークポートを再マップする"](#)。

StorageGRID内部ポート

ポート	TCPまたはUDP	から	に	詳細
22	TCP	プライマリ管理ノード	すべてのノード	メンテナンス手順では、プライマリ管理ノードはポート 22 で SSH を使用して他のすべてのノードと通信する必要があります。他のノードからの SSH トラフィックを許可するかどうかはオプションです。
80	TCP	家電製品	プライマリ管理ノード	StorageGRIDアプライアンスがプライマリ管理ノードと通信してインストールを開始するために使用されます。
123	UDP	すべてのノード	すべてのノード	ネットワーク タイム プロトコル サービス。各ノードは NTP を使用して他のすべてのノードと時刻を同期します。
443	TCP	すべてのノード	プライマリ管理ノード	インストールやその他のメンテナンス手順中にプライマリ管理ノードにステータスを伝達するために使用されます。
1055	TCP	すべてのノード	プライマリ管理ノード	インストール、拡張、回復、およびその他の保守手順のための内部トラフィック。
1139	TCP	ストレージノード	ストレージノード	ストレージ ノード間の内部トラフィック。
1501	TCP	すべてのノード	ADC 搭載ストレージノード	内部トラフィックのレポート、監査、および構成。
1502	TCP	すべてのノード	ストレージノード	S3 および Swift 関連の内部トラフィック。
1504	TCP	すべてのノード	管理ノード	NMS サービスのレポートと構成の内部トラフィック。
1505	TCP	すべてのノード	管理ノード	AMS サービスの内部トラフィック。

ポート	TCPまたはUDP	から	に	詳細
1506	TCP	すべてのノード	すべてのノード	サーバーステータスの内部トラフィック。
1507	TCP	すべてのノード	ゲートウェイノード	ロードバランサーの内部トラフィック。
1508	TCP	すべてのノード	プライマリ管理ノード	構成管理の内部トラフィック。
1511	TCP	すべてのノード	ストレージノード	メタデータの内部トラフィック。
5353	UDP	すべてのノード	すべてのノード	インストール、拡張、リカバリ時のフルグリッド IP の変更やプライマリ管理ノードの検出に使用されるマルチキャスト DNS (mDNS) サービスを提供します。 注: このポートの構成はオプションです。
7001	TCP	ストレージノード	ストレージノード	Cassandra TLS ノード間クラスター通信。
7443	TCP	すべてのノード	プライマリ管理ノード	インストール、拡張、回復、その他の保守手順、およびエラー レポートのための内部トラフィック。
8011	TCP	すべてのノード	プライマリ管理ノード	インストール、拡張、回復、およびその他の保守手順のための内部トラフィック。
8443	TCP	プライマリ管理ノード	アプライアンスノード	メンテナンス モード手順に関連する内部トラフィック。
9042	TCP	ストレージノード	ストレージノード	Cassandra クライアント ポート。
9999	TCP	すべてのノード	すべてのノード	複数のサービスの内部トラフィック。メンテナンス手順、メトリック、ネットワークの更新が含まれます。
10226	TCP	ストレージノード	プライマリ管理ノード	StorageGRIDアプライアンスによって、E シリーズSANtricity System Manager からプライマリ管理ノードにAutoSupportパッケージを転送するために使用されます。

ポート	TCPまたはUDP	から	に	詳細
10342	TCP	すべてのノード	プライマリ管理ノード	インストール、拡張、回復、およびその他の保守手順のための内部トラフィック。
18000	TCP	管理/ストレージノード	ADC 搭載ストレージノード	アカウント サービスの内部トラフィック。
18001	TCP	管理/ストレージノード	ADC 搭載ストレージノード	アイデンティティ フェデレーションの内部トラフィック。
18002	TCP	管理/ストレージノード	ストレージノード	オブジェクト プロトコルに関連する内部 API トラフィック。
18003	TCP	管理/ストレージノード	ADC 搭載ストレージノード	プラットフォームは内部トラフィックをサービスします。
18017	TCP	管理/ストレージノード	ストレージノード	Cloud Storage Pools の Data Mover サービスの内部トラフィック。
18019	TCP	すべてのノード	すべてのノード	消失訂正符号化とレプリケーションのためのチャックサービス内部トラフィック
18082	TCP	管理/ストレージノード	ストレージノード	S3 関連の内部トラフィック。
18083	TCP	すべてのノード	ストレージノード	Swift 関連の内部トラフィック。
18086	TCP	すべてのノード	ストレージノード	LDR サービスに関連する内部トラフィック。
18200	TCP	管理/ストレージノード	ストレージノード	クライアント要求に関する追加の統計。
19000	TCP	管理/ストレージノード	ADC 搭載ストレージノード	Keystoneサービスの内部トラフィック。

関連情報

["外部コミュニケーション"](#)

外部コミュニケーション

クライアントは、コンテンツを取り込んで取得するためにグリッド ノードと通信する必要があります。使用されるポートは、選択したオブジェクト ストレージ プロトコルによって異なります。これらのポートはクライアントからアクセスできる必要があります。

港へのアクセス制限

企業のネットワーク ポリシーによっていずれかのポートへのアクセスが制限されている場合は、次のいずれかを実行できます。

- 使用"[ロードバランサエンドポイント](#)"ユーザー定義のポートでのアクセスを許可します。
- ノードをデプロイするときにポートを再マップします。ただし、ロード バランサーのエンドポイントを再マップしないでください。StorageGRIDノードのポート再マッピングに関する情報を参照してください。
 - "[Red Hat Enterprise Linux 上のStorageGRIDのポート再マップ キー](#)"
 - "[Ubuntu または Debian 上のStorageGRIDのポート再マップ キー](#)"
 - "[VMware 上のStorageGRIDのポートの再マップ](#)"
 - "[オプション: アプライアンスのネットワークポートを再マップする](#)"

外部通信に使用されるポート

次の表は、ノードへのトラフィックに使用されるポートを示しています。



このリストには、次のように設定される可能性のあるポートは含まれていません。"[ロードバランサエンドポイント](#)"。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
22	TCP	SSH	サービスラップトップ	すべてのノード	コンソール ステップを含む手順では、SSH またはコンソール アクセスが必要です。オプションで、ポート 22 の代わりにポート 2022 を使用することもできます。
25	TCP	SMTP	管理ノード	メールサーバー	アラートおよび電子メールベースのAutoSupportに使用されます。「電子メールサーバー」ページを使用して、デフォルトのポート設定 25 を上書きできます。
53	TCP/UDP	DNS	すべてのノード	DNSサーバー	DNS に使用されます。
67	UDP	DHCP	すべてのノード	DHCPサービス	オプションで、DHCP ベースのネットワーク構成をサポートするために使用されます。静的に構成されたグリッドでは、dhclient サービスは実行されません。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
68	UDP	DHCP	DHCPサービス	すべてのノード	オプションで、DHCP ベースのネットワーク構成をサポートするために使用されます。静的 IP アドレスを使用するグリッドでは、dhclient サービスは実行されません。
80	TCP	HTTP	ブラウザ	管理ノード	ポート 80 は、管理ノード ユーザー インターフェイスのポート 443 にリダイレクトされます。
80	TCP	HTTP	ブラウザ	家電製品	ポート 80 は、StorageGRIDアプライアンス インストーラのポート 8443 にリダイレクトされます。
80	TCP	HTTP	ADC 搭載ストレージノード	AWS	HTTP を使用する AWS またはその他の外部サービスに送信されるプラットフォーム サービス メッセージに使用されます。テナントは、エンドポイントを作成するときに、デフォルトの HTTP ポート設定 80 を上書きできます。
80	TCP	HTTP	ストレージノード	AWS	HTTP を使用する AWS ターゲットに送信される Cloud Storage Pools リクエスト。グリッド管理者は、クラウド ストレージ プールを構成するときに、デフォルトの HTTP ポート設定 80 を上書きできます。
111	TCP/UDP	RPCバインド	NFSクライアント	管理ノード	NFS ベースの監査エクスポート (ポートマップ) で使用されます。 注: このポートは、NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 注: NFS のサポートは非推奨となっており、将来のリリースでは削除される予定です。
123	UDP	NTP	プライマリNTPノード	外部NTP	ネットワーク タイム プロトコル サービス。プライマリ NTP ソースとして選択されたノードは、外部 NTP タイム ソースとクロック時刻も同期します。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
161	TCP/UDP	SNMP	SNMPクライアント	すべてのノード	<p>SNMP ポーリングに使用されます。すべてのノードは基本情報を提供します。管理ノードはアラート データも提供します。設定するとデフォルトで UDP ポート 161 になります。</p> <p>注: このポートは必須であり、SNMP が構成されている場合にのみノード ファイアウォールで開かれます。SNMP を使用する予定の場合は、代替ポートを設定できます。</p> <p>注: StorageGRIDでの SNMP の使用については、NetApp のアカウント担当者にお問い合わせください。</p>
162	TCP/UDP	SNMP通知	すべてのノード	通知先	<p>送信 SNMP 通知とトラップはデフォルトで UDP ポート 162 に設定されます。</p> <p>注: このポートは、SNMP が有効になっていて、通知先が設定されている場合にのみ必要です。SNMP を使用する予定の場合は、代替ポートを設定できます。</p> <p>注: StorageGRIDでの SNMP の使用については、NetApp のアカウント担当者にお問い合わせください。</p>
389	TCP/UDP	LDAP	ADC 搭載ストレージノード	アクティブディレクトリ/LDAP	Identity Federation の Active Directory または LDAP サーバーに接続するために使用されます。
443	TCP	HTTPS	ブラウザ	管理ノード	<p>Web ブラウザおよび管理 API クライアントが Grid Manager および Tenant Manager にアクセスするために使用します。</p> <p>注意: Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。参照"ファイアウォール制御を構成する"特権 IP アドレスを構成します。</p>
443	TCP	HTTPS	管理ノード	Active Directory	シングル サインオン (SSO) が有効な場合に、Active Directory に接続する管理ノードによって使用されます。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
443	TCP	HTTPS	ADC 搭載ストレージノード	AWS	HTTPS を使用する AWS またはその他の外部サービスに送信されるプラットフォーム サービス メッセージに使用されます。テナントは、エンドポイントを作成するときに、デフォルトの HTTP ポート設定 443 を上書きできません。
443	TCP	HTTPS	ストレージノード	AWS	HTTPS を使用する AWS ターゲットに送信される Cloud Storage Pools リクエスト。グリッド管理者は、クラウド ストレージ プールを構成するときに、デフォルトの HTTPS ポート設定 443 を上書きできます。
903	TCP	NFS	NFSクライアント	管理ノード	NFSベースの監査エクスポートで使用される (rpc.mountd)。 注: このポートは、NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 注: NFS のサポートは非推奨となっており、将来のリリースでは削除される予定です。
2022	TCP	SSH	サービスラップトップ	すべてのノード	コンソール ステップを含む手順では、SSH またはコンソール アクセスが必要です。オプションで、ポート 2022 の代わりにポート 22 を使用することもできます。
2049	TCP	NFS	NFSクライアント	管理ノード	NFS ベースの監査エクスポート (nfs) で使用されます。 注: このポートは、NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 注: NFS のサポートは非推奨となっており、将来のリリースでは削除される予定です。
5353	UDP	mDNS	すべてのノード	すべてのノード	インストール、拡張、リカバリ時のフルグリッド IP の変更やプライマリ管理ノードの検出に使用されるマルチキャスト DNS (mDNS) サービスを提供します。 注: このポートの構成はオプションです。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
5696	TCP	KMIP	アプライアンス	キオスク	StorageGRIDアプライアンス インストーラの KMS 構成ページで別のポートが指定されていない限り、ノード暗号化用に構成されたアプライアンスからキー管理サーバ (KMS) へのキー管理相互運用性プロトコル (KMIP) 外部トラフィック。
8022	TCP	SSH	サービスラップトップ	すべてのノード	ポート 8022 の SSH は、サポートとトラブルシューティングのために、アプライアンスおよび仮想ノード プラットフォーム上の基本オペレーティング システムへのアクセスを許可します。このポートは Linux ベース (ベアメタル) ノードでは使用されず、グリッド ノード間または通常の操作中にアクセスできる必要はありません。
8443	TCP	HTTPS	ブラウザ	管理ノード	オプション。Web ブラウザおよび管理 API クライアントが Grid Manager にアクセスするために使用します。Grid Manager と Tenant Manager の通信を分離するために使用できます。 注意: Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。参照 "ファイアウォール制御を構成する" 特権 IP アドレスを構成します。
8443	TCP	HTTPS	ブラウザ	家電製品	Web ブラウザおよび管理 API クライアントがStorageGRIDアプライアンス インストーラにアクセスするために使用します。 注: ポート 443 は、StorageGRIDアプライアンス インストーラのポート 8443 にリダイレクトされます。
9022	TCP	SSH	サービスラップトップ	家電製品	サポートとトラブルシューティングのために、事前構成モードでStorageGRIDアプライアンスへのアクセスを許可します。このポートは、グリッド ノード間または通常の操作中にアクセスできる必要はありません。

ポート	TCPまたはUDP	プロトコル	から	に	詳細
9091	TCP	HTTPS	外部Grafanaサービス	管理ノード	StorageGRID Prometheus サービスへの安全なアクセスのために外部 Grafana サービスによって使用されます。 注: このポートは、証明書ベースの Prometheus アクセスが有効になっている場合にのみ必要です。
9092	TCP	カフカ	ADC 搭載ストレージノード	Kafka クラスタ	Kafka クラスタに送信されるプラットフォーム サービス メッセージに使用されます。テナントは、エンドポイントを作成するときに、デフォルトの Kafka ポート設定 9092 を上書きできます。
9443	TCP	HTTPS	ブラウザ	管理ノード	オプション。Web ブラウザおよび管理 API クライアントがテナント マネージャにアクセスするために使用します。Grid Manager と Tenant Manager の通信を分離するために使用できます。
18082	TCP	HTTPS	S3クライアント	ストレージノード	S3 クライアント トラフィックをストレージノードに直接送信します (HTTPS)。
18083	TCP	HTTPS	Swiftクライアント	ストレージノード	Swift クライアント トラフィックをストレージノードに直接送信します (HTTPS)。
18084	TCP	HTTP	S3クライアント	ストレージノード	S3 クライアント トラフィックをストレージノードに直接送信します (HTTP)。
18085	TCP	HTTP	Swiftクライアント	ストレージノード	Swift クライアント トラフィックをストレージノードに直接送信します (HTTP)。
23000-23999	TCP	HTTPS	クロスグリッドアプリケーションのソースグリッド上のすべてのノード	クロスグリッドアプリケーションの宛先グリッド上の管理ノードとゲートウェイノード	この範囲のポートは、グリッド フェデレーション接続用に予約されています。特定の接続の両方のグリッドは同じポートを使用します。

著作権に関する情報

Copyright © 2025 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。