ネットワークのガイドライン
StorageGRID 11.7

NetApp
April 12, 2024

目次

ネットワークのガイドライン . . . 1
- ネットワークガイドライン：概要 . . . 1
- StorageGRID のネットワークタイプ . . . 2
- ネットワークトポロジの例 . . . 6
- ネットワーク要件 . . . 13
- ネットワーク固有の要件 . . . 14
- 環境固有のネットワークに関する考慮事項 . . . 16
- ネットワークのインストールとプロビジョニング . . . 19
- インストール後のガイドライン . . . 20
- ネットワークポートのリファレンス . . . 20

ネットワークのガイドライン

ネットワークガイドライン：概要

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び、ネットワークの設定とプロビジョニングの要件を確認してください。

これらの手順について

これらのガイドラインは、 StorageGRID ノードを導入して設定する前に、 StorageGRID ネットワークインフラの作成に使用できる情報を示しています。これらのガイドラインを使用して、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とサービス間で通信を確実に行うことができます。

外部クライアントや外部サービスは、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を格納し、読み出す
- E メール通知を受信
- StorageGRID 管理インターフェイス（ Grid Manager およびテナントマネージャ）へのアクセス
- 監査共有へのアクセス（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（ KMS ）

これらの機能を使用するトラフィックなどを処理するには、 StorageGRID ネットワークが適切に設定されている必要があります。

作業を開始する前に

StorageGRID システムのネットワークを設定するには、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、およびファイアウォールに関する高度な経験が必要です。

ネットワークを設定する前に、StorageGRID アーキテクチャを理解しておいてください（を参照）"StorageGRID の詳細をご覧ください"。

使用する StorageGRID ネットワークとその設定を決定したら、該当する手順に従って StorageGRID ノードを設置および設定できます。

ソフトウェアベースのノードをインストール

- "Red Hat Enterprise Linux または CentOS をインストールします"
- "Ubuntu または Debian をインストールします"
- "VMware をインストールする"

アプライアンスノードを設置

- "アプライアンスハードウェアを設置"

StorageGRID ソフトウェアを設定および管理する

- "StorageGRID の管理"
- "リリースノート"

StorageGRID のネットワークタイプ

StorageGRID システム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。この 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設定する必要があります。

トラフィックタイプ

トラフィックタイプ	説明	ネットワークの種類
グリッドトラフィック	グリッド内のすべてのノードの間で伝送される、内部 StorageGRID トラフィック。このネットワークを介して、すべてのグリッドノードが他のすべてのグリッド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（必須）
管理トラフィック	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 および Swift クライアントからのオブジェクトストレージ要求をすべて含む、外部のクライアントアプリケーションとグリッドの間で伝送されるトラフィック。	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設定できます。

- Grid ネットワークのみ
- グリッドネットワークと管理ネットワーク
- グリッドネットワークとクライアントネットワーク
- グリッドネットワーク、管理ネットワーク、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、インストール時に追加することも、あとで追加して要件の変化に対応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場合は、グリッドネットワークを分離してセキュリティを確保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。外部ポートには、すべてのタイプのネットワークからアクセスできます。この柔軟性により、 StorageGRID 展開の設計と、スイッチおよびファイアウォールでの外部 IP およびポートフィルタリングの設定に複数のオプションを使用できます。を参照して

ください "内部でのグリッドノードの通信" および "外部との通信"。

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のノードネットワークインターフェイスへのマッピングの詳細については、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 または CentOS をインストールします"
- "Ubuntu または Debian をインストールします"
- "VMware をインストールする"

アプライアンスノード

- "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"
- "SG5700 ストレージアプライアンス"
- "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

ノードで有効にするネットワークごとに、次の項目を設定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

各グリッドノードの 3 つのネットワークのそれぞれについて、 IP アドレス / マスク / ゲートウェイの組み合わせを 1 つだけ設定できます。ネットワークにゲートウェイを設定しない場合は、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。

ハイアベイラビリティグループ

ハイアベイラビリティ（ HA ）グループは、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の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、を参照してください "ハイアベイラビリティグループを管理します"。

Grid ネットワーク

グリッドネットワークは必須です。このネットワークは、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、グリッド内のすべてのノード間、すべてのサイトおよびサブネットを接続します。グリッドネットワーク上のすべてのノードが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 では、ノード間の Network Address Translation （ NAT; ネットワークアドレス変換）はサポートされません。

管理ネットワークとクライアントネットワークが設定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設定されていないかぎり、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設定するときは、オープンなインターネット上のネットワークなど、信頼されてい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に関する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設定する必要があります。
- グリッドの設定が完了するまでは、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。
- グローバルなグリッドネットワークサブネットリストで設定されているすべてのサブネットへの静的ルートが、すべてのノードに対して自動的に生成されます。
- クライアントネットワークを追加すると、グリッドの設定が完了した時点で、デフォルトゲートウェイがグリッドネットワークの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。

管理ネットワーク

管理ネットワークはオプションです。このオプションを設定すると、システムの管理トラフィックや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にす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、管理トラフィックとメンテナンストラフィックがグリッドネットワークを経由する必要はありません。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 のユーザインターフェイスにアクセスします。
- NTP サーバ、 DNS サーバ、外部キー管理サーバ（ KMS ）、 Lightweight Directory Access Protocol （ LDAP ）サーバ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。
- 保守とサポートのための Secure Shell Protocol （ SSH ）アクセス。

管理ネットワークが内部のグリッドトラフィックに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が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に関する次の要件および詳細事項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や複数の管理ネットワークサブネットを設定する場合は、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で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 や Swift などのクライアントアプリケーションからの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。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 StorageGRID データにアクセスできるようにする場合は、外部リソース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経由で到達できるすべてのサブネットと通信できます。

クライアント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。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、クライアントネットワーク経由で相互に通信することはありません。クライアントネットワークは、グリッドのインストールが完了するまで動作状態になりません。

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されていないものと指定し、クライアントネットワークで許可される接続をより厳しく制限できます。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、このインターフェイスは CloudMirror レプリケーションで使用される接続などのアウトバウンド接続を受け入れますが、ロードバランサエンドポイントとして明示的に設定されているポートのインバウンド接続だけを受け入れます。を参照してください "ファイアウォールコントロールを管理します" および "ロードバランサエンドポイントを設定する"。

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がグリッドネットワークを経由する必要はありません。グリッドネットワークトラフィックは、ルーティングされないセキュアなネットワークに分離できます。クライアントネットワークでは、多くの場合、次のノードタイプが設定されます。

- ゲートウェイノード。グリッドへの StorageGRID ロードバランササービスおよび S3 / Swift 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： S3 および Swift プロトコルへのアクセス、およびクラウドストレージプールと 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。
- 管理ノード。テナントユーザが管理ネットワークを使用せずに Tenant Manager に接続できるようにするために使用します。

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を設定する場合は、クライアントネットワークゲートウェイが必要です。
- グリッドの設定が完了すると、クライアントネットワークの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タイプの管理トラフィックに、仮想 LAN （ VLAN ）ネットワークを使用できます。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 で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、 1 つのノード上の 1 つ以上のインターフェイスをスイッチで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）をトランクとして設定するか、ノードにトランクインターフェイスを追加できます。

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たトランクのネイティブインターフェイスを経由します。同様に、 eth2 がトランクとして設定されていて、クライアントネットワークも同じノード上で構成されている場合、クライアントネットワークはスイッチ上で構成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 、 Grid Manager 、または Tenant Manager のトラフィックに使用するなどのインバウンド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のアウトバウンドトラフィックは、 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。ストレージノードまたはアーカイブノードへのクライアントアクセスまたは管理アクセスにVLANインターフェイスを使用することはできません。

を参照してください "VLAN インターフェイスを設定します" を参照してください。

VLAN インターフェイスは HA グループでのみ使用され、アクティブノード上の VIP アドレスに割り当てられます。を参照してください "ハイアベイラビリティグループを管理します" を参照してください。

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

グリッドネットワークのみを設定すると、最もシンプルなネットワークトポロジが作成されます。

グリッドネットワークを設定するときは、各グリッドノードの eth0 インターフェイスについて、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。

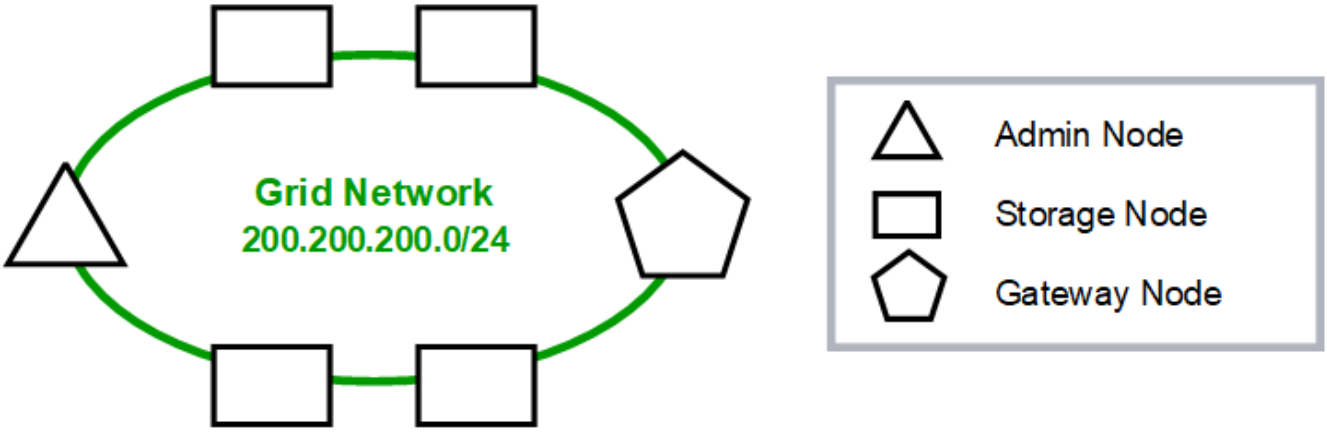
設定時に、グリッドネットワークサブネットリスト（ GNSL ）にすべてのグリッドネットワークサブネットを追加する必要があります。このリストには、すべてのサイトのすべてのサブネットが含まれ、 NTP 、 DNS 、 LDAP などの重要なサービスへのアクセスを提供する外部サブネットも含まれます。

インストール時に、グリッドネットワークのインターフェイスでは、 GNSL に含まれるすべてのサブネットに静的ルートが適用され、設定されている場合はノードのデフォルトルートがグリッドネットワークゲートウェイに設定されます。クライアントネットワークがなく、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 および Swift クライアント要求と管理機能およびメンテナンス機能に関連するトラフィックを含むすべてのトラフィックが、同じネットワークを共有しています。

このトポロジは、外部では使用できない単一サイト環境、コンセプトの実証環境、テスト環境、またはサードパーティのロードバランサ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にします。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ファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**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

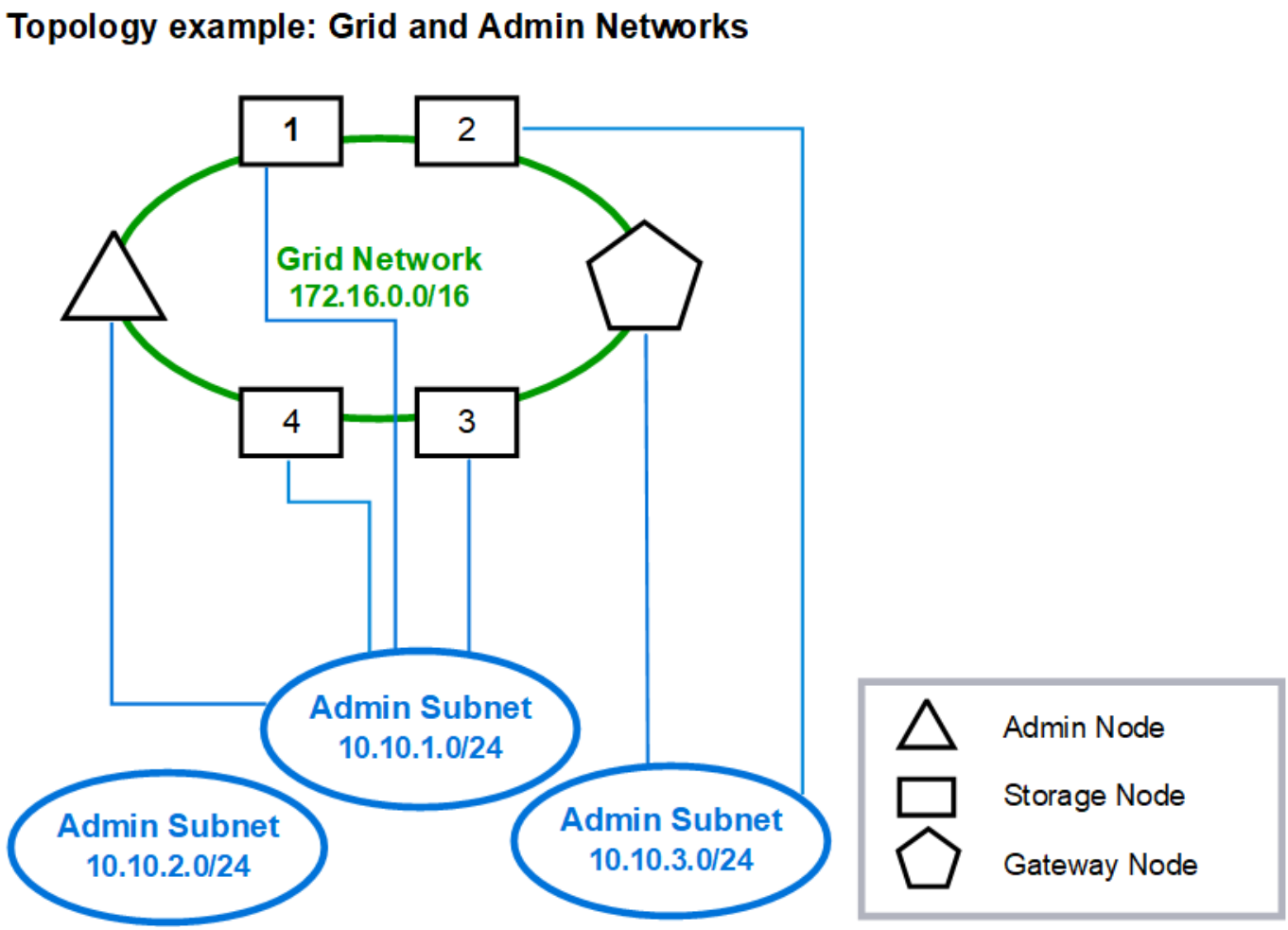
管理ネットワークトポロジ

管理ネットワークの使用はオプションです。管理ネットワークとグリッドネットワークを使用する方法の 1 つは、ノードごとにルーティング可能なグリッドネットワークと境界で保護された管理ネットワークを設定することです。

管理ネットワークを設定するときは、各グリッドノードの eth1 インターフェイスについて、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一意にすることができ、複数のサブネットで構成することができます。各ノードで Admin External Subnet List （ AESL ）を設定できます。AESL リストには、各ノードの管理ネットワーク経由で到達できるサブネットが表示されます。AESL には、 NTP 、 DNS 、 KMS 、 LDAP など、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 に含まれるサブネットごとに静的ルートが適用されます。

次の例では、 S3 および Swift 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グリッドネットワークが使用されています。一方、管理機能には管理ネットワークが使用されます。



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**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, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	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

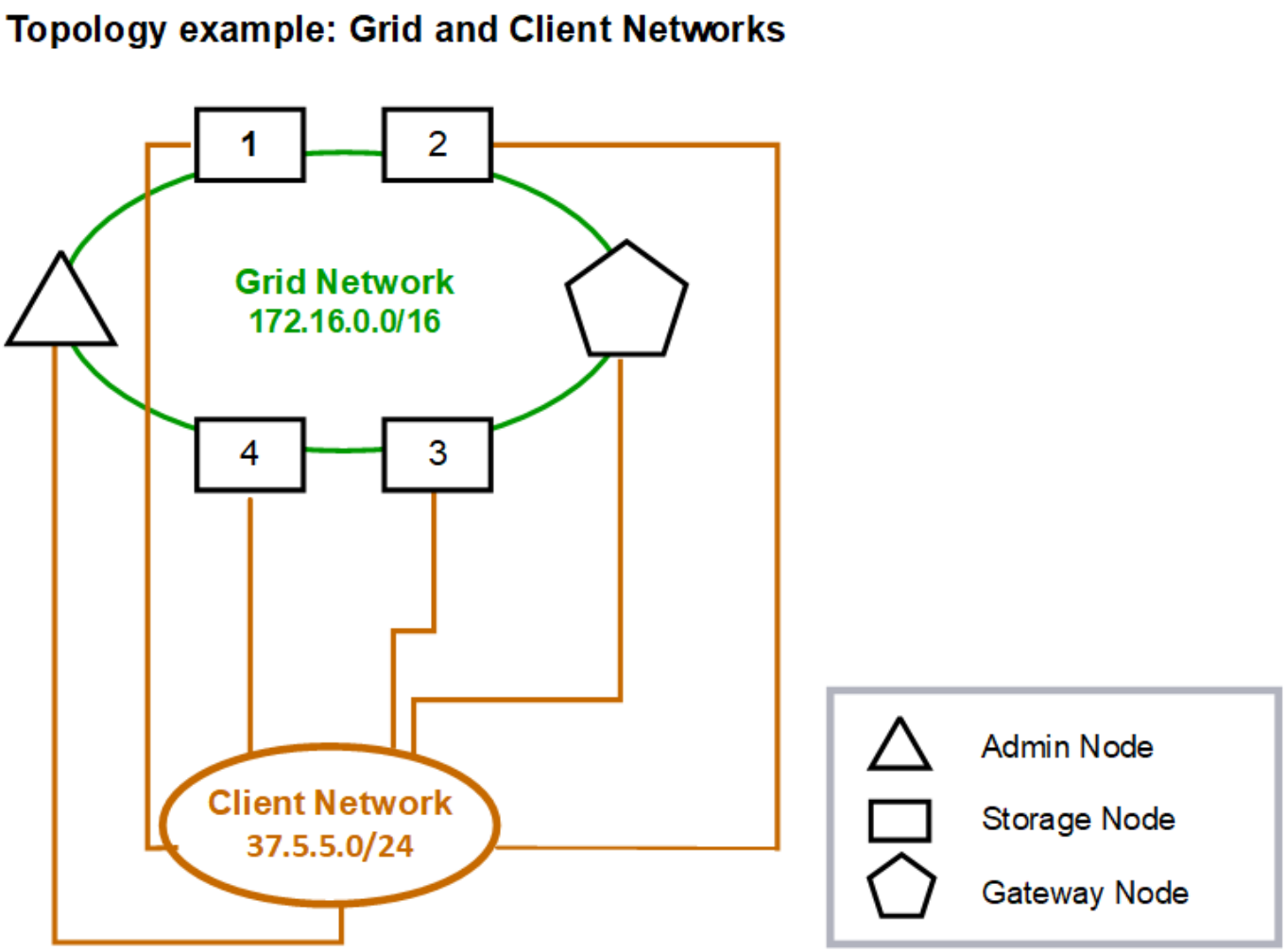
クライアントネットワークの使用はオプションです。クライアントネットワークを使用すると、クライアントネットワークのトラフィック（ S3 や Swift など）をグリッドの内部トラフィックから分離できるため、グリッドネットワークのセキュリティを強化できます。管理ネットワークが設定されていない場合、管理トラフィックはクライアントネットワークまたはグリッドネットワークのどちらでも処理できます。

クライアントネットワークを構成するときは、構成済みノードの eth2 インターフェイスについて、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とは独立している可能性があります。

インストール時にノードのクライアントネットワークを設定すると、インストールの完了時に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。クライアントネットワークをあとで追加した場合、ノードのデフォルトゲートウェイが同じように切り替わります。

次の例では、クライアントネットワークが S3 および Swift クライアント要求と管理機能に使用され、グリッ

ドネットワークが内部のオブジェクト管理処理専用となっています。



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	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

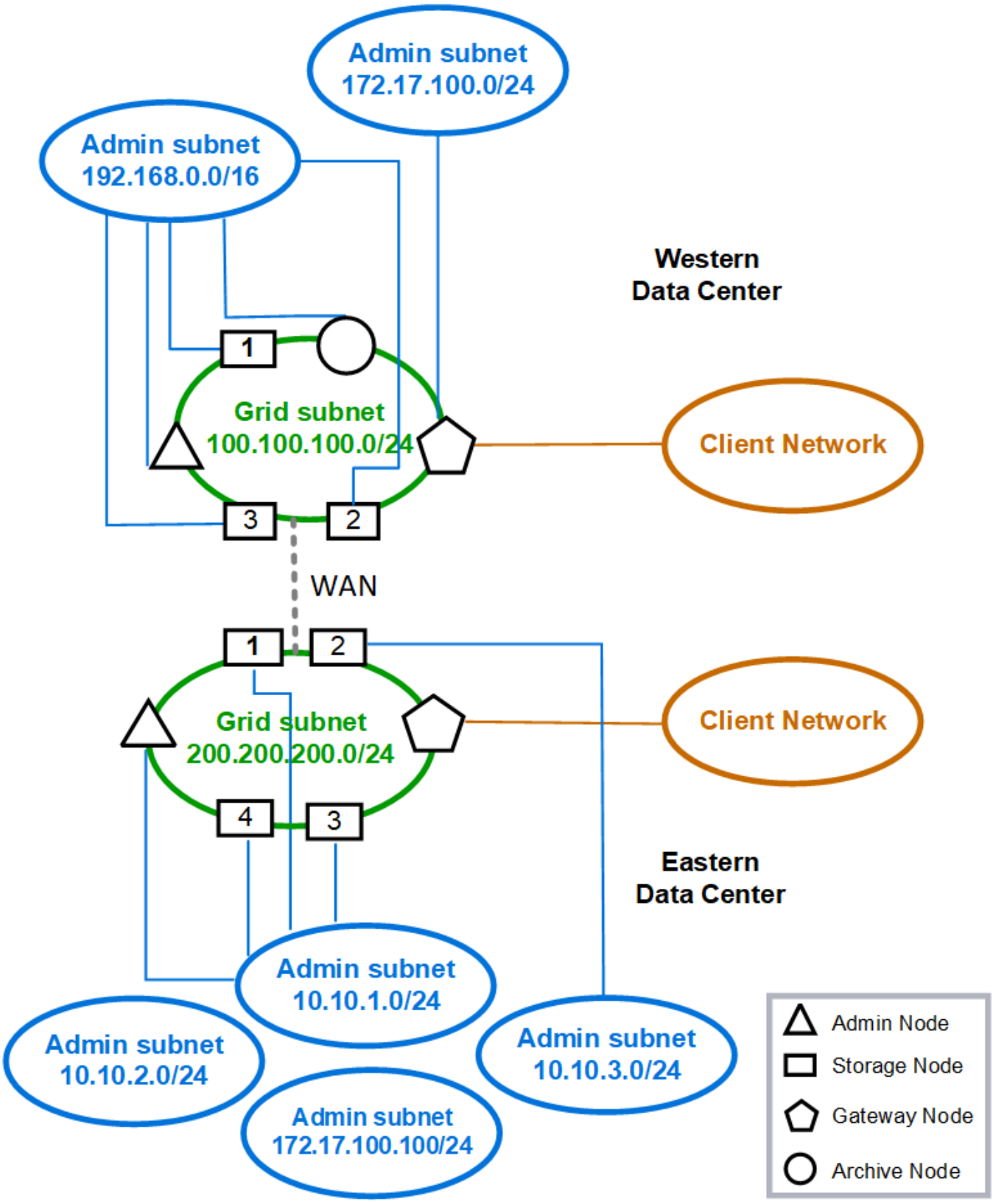
3 つのネットワークすべてのトポロジ

3 つのネットワークをすべて組み合わせて、プライベートグリッドネットワーク、サイトごとに境界を設定した管理ネットワーク、およびオープンな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を構成できます。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。

次の例では、

- グリッドネットワークは、内部のオブジェクト管理処理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 および Swift 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。

Topology example: Grid, Admin, and Client Networks



ネットワーク要件

計画した StorageGRID ネットワーク設計を、現在のネットワークインフラと構成が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 環境で次の接続がサポートされている必要があります。

これらの接続は、ネットワークトポロジの例に示すように、グリッドネットワーク、管理ネットワーク、クライアントネットワーク、またはこれらのネットワークの組み合わせを介して発生します。

- * 管理接続 * ：通常は SSH 経由で、管理者からノードへのインバウンド接続。Grid Manager 、テナントマネージャ、および StorageGRID アプライアンスインストーラへの Web ブラウザアクセス
- *NTP サーバ接続 *: 受信 UDP 応答を受信するアウトバウンド UDP 接続。

  プライマリ管理ノードが、少なくとも 1 つの NTP サーバにアクセスできる必要があります。
- *DNS サーバ接続 *: 受信 UDP 応答を受信するアウトバウンド UDP 接続。
- *LDAP/Active Directory サーバ接続 *: ストレージノード上のアイデンティティサービスからのアウトバウンド TCP 接続。
- * AutoSupport *：管理ノードからいずれかのノードへのアウトバウンド接続 `support.netapp.com` またはお客様が設定したプロキシ。
- * 外部キー管理サーバ * ：ノード暗号化が有効な各アプライアンスノードからのアウトバウンド TCP 接続。
- S3 および Swift クライアントからのインバウンド TCP 接続。
- CloudMirror レプリケーションやクラウドストレージプールなどの StorageGRID プラットフォームサービスからのアウトバウンド要求。

StorageGRID が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サーバまたはDNSサーバにアクセスできない場合は、DNSサーバとNTPサーバのIPアドレスが指定されているかぎり、すべてのネットワーク（グリッド、管理、クライアント）の接続が自動的に試行されます。NTP サーバまたは DNS サーバにネットワーク経由でアクセスできる場合は、 StorageGRID によって追加のルーティングルールが自動的に作成され、以降のすべてのネットワーク接続試行に使用されるようになります。

これらの自動検出されたホストルートは使用できますが、通常は、自動検出が失敗した場合に接続を確保するために、 DNS ルートと NTP ルートを手動で設定する必要があります。

導入時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設定する準備ができていない場合は、設定手順でグリッドノードを承認するときにそれらのネットワークを設定できます。また、インストール後に IP 変更ツールを使用してこれらのネットワークを設定することもできます（を参照） "IP アドレスを設定する"）。

VLAN インターフェイスでサポートされるのは、 S3 および Swift クライアント接続と、 SSH 、 Grid Manager 、および Tenant Manager 管理接続だけです。NTP 、 DNS 、 LDAP 、 AutoSupport 、 KMS サーバなどへのアウトバウンド接続 クライアント、管理、またはグリッドネットワークの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たインターフェイスのネイティブ VLAN を経由し

ます。

複数サイト用の **WAN** （ **Wide Area Network** ）

複数のサイトで StorageGRID システムを設定する場合は、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 接続の各方向の帯域幅が 25 Mbit/ 秒以上である必要があります。サイト間、ノードまたはサイトの拡張、ノードのリカバリ、その他の処理や構成のデータレプリケーションやイレイジャーコーディングでは、追加の帯域幅が必要になります。

WAN帯域幅の実際の最小要件は、クライアントアクティビティとILM保護方式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、ネットアッププロフェッショナルサービスの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、開いているインターネット上のノードなど、信頼されていないクライアントから常に保護する必要があります。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにする必要があります。

ハイアベイラビリティグループに追加する管理ノードとゲートウェイノードには静的 IP アドレスを設定する必要があります。詳細については、を参照してください "ハイアベイラビリティグループを管理します"。

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、Network Address Translation（NAT；ネットワークアドレス変換）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は、使用するアドレスに各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できる必要があります。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 アドレスを指定するなど、外部クライアントとグリッドノードの間で 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方法は、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採用する場合、つまりグリッドノードがパブリック IP アドレスを認識する必要がない場合にのみサポートされます。

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およびルータ

- 設定する場合、特定のネットワークのゲートウェイは、そのネットワークのサブネット内になければなりません。
- 静的アドレス指定を使用してインターフェイスを設定する場合は、 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ことを推奨します。

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、専用のサブネットに接続する必要があります。

導入時に、 Grid Manager によって次の制限事項が適用されます。これらの情報は、導入前のネットワーク計画に役立ちます。

- ネットワークIPアドレスのサブネットマスクを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、同じノードに設定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。
- 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のサブネットと重複することはできません。
- AESL内のサブネットは、GNSL内のどのサブネットとも重複できません。
- 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のサブネット、またはAESLのサブネットと重複することはできません。

Grid ネットワーク

- 導入時に、各グリッドノードがグリッドネットワークに接続され、ノード導入時に指定したネットワーク設定を使用してプライマリ管理ノードと通信できる必要があります。
- 通常のグリッド運用中は、各グリッドノードが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できる必要があります。

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できる必要があります。ノード間の Network Address Translation （ NAT ；ネットワークアドレス変換）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構成されている場合は、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 のサブネットごとに、すべてのノードにスタティック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設定されている場合は、トランクのネイティブ VLAN をグリッドネットワークトラフィックに使用する VLAN にする必要があります。すべてのグリッドノードに、トランクのネイティブ VLAN 経由でアクセスできる必要があります。

管理ネットワーク

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設定する場合は、次の要件および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のほか、重要なサーバ（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接続されていない場合）への接続があります。

必要なネットワークサービスおよびクライアントにアクセス可能であれば、管理ネットワークおよび AESL は各ノードで一意にすることができます。

外部サブネットからのインバウンド接続を有効にするには、管理ネットワークに少なくとも 1 つのサブネットを定義する必要があります。AESL に含まれる各サブネットの静的ルートがノードごとに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設定する場合は、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 および Swift 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。設定すると、クライアント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。
- クライアントネットワークを使用する場合は、明示的に設定されたロードバランサエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。を参照してください "ロードバランサエンドポイントを設定する"。
- 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トランクとして設定されている場合は、クライアントネットワークインターフェイス（ eth2 ）の設定が必要かどうかを検討してください。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たトランクネイティブ VLAN を経由します。

環境固有のネットワークに関する考慮事項

Linux の導入

効率性、信頼性、セキュリティのために、 StorageGRID システムはコンテナエンジンの集合として Linux 上で動作します。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 ペアや仮想イーサネット（ veth ）ペアなどの非ボンドデバイスを使用します。このデバイスをノード構成ファイルのネットワークインターフェイスとして指定してください。

ボンドデバイスや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イスとして直接使用しないでください。このようにすると、 macvlan を使用してコンテナネームスペース内のボンドデバイスとブリッジデバイスを使用するカーネル問題 が原因でノードの起動が妨げられる可能性があります。

のインストール手順を参照してください "Red Hat Enterprise Linux または CentOS" または "Ubuntu または Debian" 導入：

コンテナエンジン導入用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 の導入を開始する前に、各ノードで使用するネットワーク（グリッド、管理、クライアント）を決めます。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に設定されていること、および各ネットワークに十分な帯域幅があることを確認してください。

物理ホスト

物理ホストを使用してグリッドノードをサポートする場合は、次の手順を実行します。

- すべてのホストで各ノードインターフェイスに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。この方法により、ホストの構成が簡易化され、将来のノードの移行にも対応できます
- 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 つ以上のノードで使用できます。このインターフェイスを使用するホストまたはノードには、一意の IP アドレスを割り当てる必要があります。ホストとノードでIPアドレスを共有することはできません。

- 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トランクインターフェイスがホストに 1 つ以上必要です。これらのインターフェイスは、 eth0 、 eth2 、または追加の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。トランクインターフェイスまたはアクセスインターフェイスを追加するには、次の項を参照してください。
  - * RHEL または CentOS （ノードのインストール前） * ： "ノード構成ファイルを作成"
  - * 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"
  - * RHEL 、 CentOS 、 Ubuntu 、または Debian （ノードのインストール後） * ： "Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"

最小帯域幅の推奨値

次の表に、StorageGRID ノードのタイプとネットワークのタイプごとに推奨される最小LAN帯域幅を示します。それぞれの物理ホストまたは仮想ホストについて、そのホストで実行する StorageGRID ノードの総数とタイプに応じて、アグリゲートの最小帯域幅要件を満たすように十分なネットワーク帯域幅を確保する必要があります。

ノードのタイプ	ネットワークのタイプ		
	グリッド（ Grid ）	管理	クライアント
	最小**LAN**帯域幅	管理	10 Gbps
1 Gbps	1 Gbps	ゲートウェイ	10 Gbps
1 Gbps	10 Gbps	ストレージ	10 Gbps
1 Gbps	10 Gbps	Archive サービスの略	10 Gbps

> この表には、共有ストレージへのアクセスに必要な SAN の帯域幅は含まれていません。イーサネット経由（ iSCSI または FCoE ）でアクセスする共有ストレージを使用する場合は、各ホストで物理インターフェイスを別途プロビジョニングして十分な SAN の帯域幅を確保する必要があります。ボトルネックにならないように、各ホストの SAN の帯域幅として、そのホストで実行されるすべてのストレージノードの総ネットワーク帯域幅とほぼ同じ帯域幅を確保します。

上記の表を参照して、それぞれのホストに最小限必要なネットワークインターフェイスの数を確認します。これは、そのホストで実行する StorageGRID ノードの数とタイプで決まります。

たとえば、単一のホストで管理ノード、ゲートウェイノード、およびストレージノードを 1 つずつ実行するには、次の手順を実行します。

- 管理ノードにグリッドネットワークと管理ネットワークを接続する（必要な帯域幅： 10 + 1 = 11Gbps ）
- ゲートウェイノードにグリッドネットワークとクライアントネットワークを接続する（必要な帯域幅： 10 + 10 = 20Gbps ）
- ストレージノードにグリッドネットワークを接続する（必要な帯域幅： 10Gbps ）

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。 2 つの 40Gbps インターフェイスまたは 5 つの 10Gbps インターフェイスで対応できます。これらは潜在的にトランクに集約され、ホストを含む物理データセンターに対してローカルなグリッド、管理、およびクライアントのサブネットを伝送する 3 つ以上の VLAN によって共有されます。

StorageGRID クラスタのホストの物理リソースおよびネットワークリソースを設定して StorageGRID を導入する際の準備として、推奨される方法については、次の表を参照してください。

- "ホストネットワークの設定（ Red Hat Enterprise Linux または CentOS ）"
- "ホストネットワークの設定（ 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用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クラウドストレージプールを使用する場合は、デスティネーション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設定する必要があります。

プラットフォームサービス用のネットワーク

を参照してください "テナントのプラットフォームサービスを管理する" および "プラットフォームサービスとは"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には、 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。アクセスの提供例は次のとおりです。

- ADC サービスがある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設定します。
- クライアントネットワークが提供するデフォルトルートを使用します。デフォルトルートを使用する場合は、を使用できます "信頼されていないクライアントネットワーク機能" インバウンド接続を制限する。

クラウドストレージプールのネットワーク

また、クラウドストレージプールは、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する外部サービスが提供するエンドポイントへのアクセスを必要とします。詳細については、を参照してください "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クラウドストレージプールの通信に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`
- **442**：で始まるエンドポイントURI `https`

エンドポイントの作成時または編集時に別のポートを指定できます。を参照してください "ネットワークポートのリファレンス"。

非透過型プロキシサーバを使用する場合は、も使用する必要があります "ストレージプロキシを設定します" 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へのメッセージの送信を許可します。

VLAN および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VLANネットワークを使用することはできません。デスティネーションエンドポイントには、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経由でアクセスできる必要があります。

アプライアンスノード

StorageGRID アプライアンスのネットワークポートは、スループット、冗長性、およびフェイルオーバーの要件を満たすポートボンディングモードを使用するように設定できます。

StorageGRID アプライアンスの 10 / 25GbE 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、固定またはアグリゲートのボンディングモードで設定できます。

1GbE 管理ネットワークポートは、管理ネットワークへの接続に独立モードまたはアクティブ / バックアップモードを設定できます。

アプライアンスのポートボンディングモードに関する情報を参照してください。

- "ポートボンディングモード（SGF6112）"
- "ポートボンディングモード（SG6000-CNコントローラ）"
- "ポートボンディングモード（E5700SGコントローラ）"
- "ポートボンディングモード（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

ノードの導入時とグリッドの設定時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しておく必要があります。

ノードの初期導入

ノードを最初に導入するときは、ノードをグリッドネットワークに接続して、ノードがプライマリ管理ノード

にアクセスできるように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アクセスして設定とインストールを実行できるように、プライマリ管理ノードに管理ネットワークを設定できます。

ゲートウェイが設定されているグリッドネットワークは、導入時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、グリッドを設定する前に、別々のサブネットにある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 サーバを含むサブネットや Grid Manager または API へのアクセスを必要とするサブネットを、グリッドサブネットとして設定することもできます。

プライマリ管理ノードへの自動ノード登録

導入されたノードは、グリッドネットワークを使用して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、を使用できます `configure-storagegrid.py` Pythonスクリプト、またはインストールAPIを使用して、グリッドを設定し、登録済みのノードを承認します。グリッド設定時に、複数のグリッドサブネットを設定できます。グリッドの設定が完了すると、グリッドネットワークゲートウェイを経由する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します

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場合は、ノードの承認プロセス中にそれらのネットワークから設定を削除するか、インストールの完了後に IP 変更ツールを使用できます（を参照） "IP アドレスを設定する"）。

インストール後のガイドライン

グリッドノードの導入と設定が完了したら、 DHCP アドレスおよびネットワーク設定の変更について、次のガイドラインに従ってください。

- DHCP を使用して IP アドレスを割り当てた場合は、使用しているネットワーク上の各 IP アドレスに対して DHCP 予約を設定します。

  DHCP は導入フェーズでのみ設定できます。設定中にDHCPを設定することはできません。

  > IP アドレスが変わるとノードがリブートします。 DHCP アドレスの変更が同時に複数のノードに影響を及ぼす場合、原因 が停止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 変更手順を使用する必要があります。を参照してください "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、ネットワーク設定を変更すると、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。適用されるネットワークの変更によっては、これらの接続の再確立が必要になる場合があります。

ネットワークポートのリファレンス

ネットワークインフラが、グリッド内のノード間、および外部のクライアントやサービスとの間で内部通信および外部通信を可能にすることを確認する必要があります。内部および外部のファイアウォール、スイッチングシステム、およびルーティングシステム

全体へのアクセスが必要な場合があります。

に表示された詳細を使用します "内部でのグリッドノードの通信" および "外部との通信" 必要な各ポートの設定方法を確認します。

内部でのグリッドノードの通信

StorageGRID の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受信接続を許可します。ロードバランサエンドポイントで定義されたポートにも接続が許可されます。

> グリッドノード間で Internet Control Message Protocol （ ICMP ）トラフィックを有効にすることを推奨します。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。

StorageGRID では、 ICMP と表に記載されているポートに加えて、 Virtual Router Redundancy Protocol （ VRRP; 仮想ルータ冗長プロトコル）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 が必要なのは、の場合だけです "ハイアベイラビリティグループ" が設定されている。

Linux ベースのノードについてはガイドラインを参照してください

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで制限されている場合は、導入設定パラメータを使用して導入時にポートを再マッピングできます。ポートの再マッピングおよび導入設定パラメータの詳細については、次のサイトを参照してください。

- "Red Hat Enterprise Linux または CentOS をインストールします"
- "Ubuntu または Debian をインストールします"

VMware ベースのノードについてのガイドラインを参照してください

次のポートは、 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設定してください。

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーによって制限される場合は、ノードを導入する際に VMware vSphere Web Client を使用してポートを再マッピングするか、またはグリッドノードの導入を自動化する際に構成ファイルの設定を使用してポートを再マッピングできます。ポートの再マッピングおよび導入設定パラメータの詳細については、を参照してください"VMware 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

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで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ピングできます。を参照してください "オプション：アプライアンスのネットワークポートの再マッピング"。

StorageGRID の内部ポート

ポート	**tcp** または **udp** です	移動元	終了：	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がポート 22 で SSH を使用して他のすべてのノードと通信できる必要があります。他のノードからの SSH トラフィックの許可は任意です。
80	TCP	アプライアンス	プライマリ管理ノード	StorageGRID アプライアンスが、インストールを開始する目的でプライマリ管理ノードと通信するために使用します。
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。すべてのノードは、 NTP を使用して他のすべてのノードと時間を同期します。
443	TCP	すべてのノード	プライマリ管理ノード	インストールおよびその他のメンテナンス手順の実行中に、プライマリ管理ノードにステータスを通知するために使用します。
1055年	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、リカバリ、およびその他のメンテナンス手順用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 年	TCP	すべてのノード	ADC を採用するストレージノード	レポート、監査、および設定の内部トラフィック。
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および設定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。
1506.	TCP	すべてのノード	すべてのノード	サーバ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	設定管理の内部トラフィック。

ポート	**tcp** または **udp** です	移動元	終了：	詳細
1509.	TCP	すべてのノード	アーカイブノード	アーカイブノード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。
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、リカバリ、その他のメンテナンス手順、およびエラーレポート用の内部トラフィック。
8011だ	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、リカバリ、およびその他のメンテナンス手順用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の手順 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、指標、および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 アプライアンスが、 E シリーズの SANtricity System Manager からプライマリ管理ノードに AutoSupport メッセージを転送するために使用します。
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、リカバリ、およびその他のメンテナンス手順用の内部トラフィック。
11139	TCP	アーカイブ / ストレージノード	アーカイブ / ストレージノード	ストレージノードとアーカイブノード間の内部トラフィック。
18000 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	アカウントサービスの内部トラフィック。

ポート	**tcp** または **udp** です	移動元	終了：	詳細
18001	TCP	管理 / ストレージノード	ADC を採用するストレージノード	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 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	プラットフォームサービスの内部トラフィック。
18017 年	TCP	管理 / ストレージノード	ストレージノード	クラウドストレージプールの Data Mover サービスの内部トラフィック。
18019 年になります	TCP	ストレージノード	ストレージノード	イレイジャーコーディング用のチャンクサービスの内部トラフィック。
18082 年	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 年	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年	TCP	すべてのグリッドノード	すべてのストレージノード	LDRサービスに関連する内部トラフィック。
18200 年	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 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	Keystone サービスの内部トラフィック。

関連情報

"外部との通信"

外部との通信

クライアントは、コンテンツの取り込みと読み出しを行うためにグリッドノードと通信する必要があります。使用するポートは、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。

ポートへのアクセスを制限します

エンタープライズネットワークポリシーで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、を使用できます "ロードバランサエンドポイント" ユーザ定義のポートでアクセスを許可します。これで、を使用できます "信頼されていないクライアントネットワーク" ロードバランサエンドポイントポートでのみアクセスを許可する場合。

ポートの再マッピング

SMTP 、 DNS 、 SSH 、 DHCP などのシステムとプロトコルを使用するには、ノードを導入する際にポートを再マッピングする必要があります。ただし、ロードバランサエンドポイントを再マッピングしないでください。ポートの再マッピングの詳細については、インストール手順を参照してください。

- "Red Hat Enterprise Linux または CentOS をインストールします"
- "Ubuntu または Debian をインストールします"
- "VMware をインストールする"
- "オプション：アプライアンスのネットワークポートの再マッピング"

外部との通信に使用するポート

次の表に、ノードに着信するトラフィックに使用されるポートを示します。

このリストには、として設定されてい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" またはに使用されます "syslogサーバ"。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
22	TCP	SSH	サービスラップトップ	すべてのノード	コンソールの手順を実行するには、 SSH アクセスまたはコンソールアクセスが必要です。必要に応じて、ポート 22 の代わりに 2022 を使用できます。
25	TCP	SMTP	管理ノード	E メールサーバ	アラートおよび E メールベースの AutoSupport に使用されます。Email Servers ページを使用して、デフォルトのポート設定である 25 を上書きできます。
53	TCP / UDP	DNS	すべてのノード	DNS サーバ	DNSに使用されます。
67	UDP	DHCP	すべてのノード	DHCP サービス	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的に設定されたグリッドに対しては実行されません。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
68	UDP	DHCP	DHCP サービス	すべてのノード	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的 IP アドレスを使用するグリッドに対しては実行されません。
80	TCP	HTTP	ブラウザ	管理ノード	ポート 80 は、管理ノードのユーザインターフェイス用のポート 443 にリダイレクトされます。
80	TCP	HTTP	ブラウザ	アプライアンス	ポート 80 は、 StorageGRID アプライアンスインストーラ用のポート 8443 にリダイレクトされます。
80	TCP	HTTP	ADC を採用するストレージノード	AWS	AWS または HTTP を使用する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のメッセージに使用します。エンドポイントの作成時に、テナントのデフォルトの HTTP ポート設定である 80 よりも優先される。
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クラウドストレージプール要求。クラウドストレージプールを設定するときに、グリッド管理者がデフォルトの HTTP ポート設定である 80 を上書きできます。
111	TCP / UDP	rpcbind	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（ portmap ）で使用します。 • 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。
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、クロックの時間と外部 NTP の時間ソースとの同期も行います。
137	UDP	NETBIOS	SMB クライアント	管理ノード	NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。 • 注：このポートは、 SMB 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。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
138	UDP	NETBIOS	SMB クライアント	管理ノード	NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。 • 注：このポートは、 SMB 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。
139	TCP	SMB	SMB クライアント	管理ノード	NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。 • 注：このポートは、 SMB 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。
161	TCP / UDP	SNMP	SNMP クライアント	すべてのノード	SNMP ポーリングに使用します。すべてのノードは基本情報を提供し、管理ノードはアラートデータとアラームデータも提供します。設定時のデフォルトの UDP ポートは 161 です。 • 注：このポートは必須です。 SNMP が設定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 を使用する場合は、代替ポートを設定できます。 • 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。
162	TCP / UDP	SNMP 通知	すべてのノード	通知の送信先	アウトバウンド SNMP 通知およびトラップのデフォルトの UDP ポートは 162 です。 • 注：このポートは、 SNMP が有効で通知の送信先が設定されている場合にのみ必要です。SNMP を使用する場合は、代替ポートを設定できます。 • 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。
389	TCP / UDP	LDAP	ADC を採用するストレージノード	Active Directory / LDAP	アイデンティティフェデレーション用の Active Directory または LDAP サーバに接続するために使用します。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
443	TCP	HTTPS	ブラウザ	管理ノード	Grid Manager と Tenant Manager にアクセスするために Web ブラウザと管理 API クライアントで使用します。 注：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ユーザ（ユーザを含む）は、ユーザのIPアドレスが特権アドレスリストに追加されていないかぎりGrid Managerにアクセスできなくなります。を参照してください "ファイアウォールコントロールを設定します" 特権IPアドレスを設定します。
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で使用します。
443	TCP	HTTPS	アーカイブノード	Amazon S3	アーカイブノードから Amazon S3 にアクセスするために使用します。
443	TCP	HTTPS	ADC を採用するストレージノード	AWS	AWS または HTTPS を使用する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のメッセージに使用します。エンドポイントの作成時に、テナントがデフォルトの HTTP ポート設定である 443 を上書きできる。
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クラウドストレージプール要求。クラウドストレージプールの設定時に、グリッド管理者がデフォルトの HTTPS ポート設定である 443 を上書きできます。
445	TCP	SMB	SMB クライアント	管理ノード	SMB ベースの監査エクスポートで使用します。 • 注：このポートは、 SMB 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。
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します（`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。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
2022	TCP	SSH	サービスラップトップ	すべてのノード	コンソールの手順を実行するには、 SSH アクセスまたはコンソールアクセスが必要です。必要に応じて、 2022 の代わりにポート 22 を使用できます。
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 ）で使用します。 • 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。
5353	UDP	mDNS	すべてのノード	すべてのノード	フルグリッドIPの変更、およびインストール、拡張、リカバリ時のプライマリ管理ノードの検出に使用するマルチキャストDNS（mDNS）サービスを提供します。
5696	TCP	KMIP	アプライアンス	KMS	ノードの暗号化用に設定されたアプライアンスから Key Management Server （ KMS ）へのキー管理 Interoperability Protocol （ KMIP ）の外部トラフィック（ StorageGRID アプライアンスインストーラの KMS 構成のページで別のポートを指定している場合を除く）。
8022	TCP	SSH	サービスラップトップ	すべてのノード	ポート 8022 で SSH を使用すると、サポートとトラブルシューティング用に、アプライアンスと仮想ノードプラットフォーム上のベースのオペレーティングシステムへのアクセスが許可されます。このポートは Linux ベース（ベアメタル）ノードには使用されず、グリッドノード間または通常運用時にアクセス可能である必要はありません。
8443	TCP	HTTPS	ブラウザ	管理ノード	任意。Grid Manager にアクセスするために Web ブラウザと管理 API クライアントで使用されます。を使用して、 Grid Manager と Tenant Manager の通信を分離できます。 注：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ユーザ（ユーザを含む）は、ユーザのIPアドレスが特権アドレスリストに追加されていないかぎりGrid Managerにアクセスできなくなります。を参照してください "ファイアウォールコントロールを設定します" 特権IPアドレスを設定します。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
9022	TCP	SSH	サービスラップトップ	アプライアンス	サポートとトラブルシューティングのために、構成前モードでの 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、グリッドノード間で、または通常運用時にアクセス可能である必要はありません。
9091	TCP	HTTPS	外部の Grafana サービス	管理ノード	外部の Grafana サービスが StorageGRID Prometheus サービスへのセキュアなアクセスに使用します。 • 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。
ポート 1	TCP	HTTPS	ブラウザ	管理ノード	任意。Tenant Manager にアクセスするために Web ブラウザと管理 API クライアントで使用します。を使用して、 Grid Manager と Tenant Manager の通信を分離できます。
18082 年	TCP	HTTPS	S3 クライアント	ストレージノード	ストレージノードへの S3 クライアントトラフィック（ HTTPS ）。
18083 年	TCP	HTTPS	Swift クライアント	ストレージノード	ストレージノードへの Swift クライアントトラフィック（ HTTPS ）。
18084 年	TCP	HTTP	S3 クライアント	ストレージノード	ストレージノードへの S3 クライアントトラフィック（ HTTP ）。
18085 年になります	TCP	HTTP	Swift クライアント	ストレージノード	ストレージノードへの Swift クライアントトラフィック（ HTTP ）。
23000-23999	TCP	HTTPS	グリッド間レプリケーションのソースグリッド上のすべてのノード	グリッド間レプリケーション用のデスティネーション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が同じポートを使用します。

著作権に関する情報

商標に関する情報