StorageGRID ネットワークの概要

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID ネットワークの概要

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、_グリッド入門_の説明に従ってStorageGRID アーキテクチャについて理解しておいてください。

StorageGRID を導入して設定する前に、ネットワークインフラを設定する必要があります。通信は、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の間で発生する必要があります。

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
  - Domain Name System （ DNS ；ドメインネームシステム）
  - 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。

使用する3つのStorageGRID ネットワークのうち、どのネットワークをどのように設定するかを決定したら、適切な手順に従ってStorageGRID ノードを設置して設定できます。

関連情報

"グリッド入門"

"StorageGRID の管理"

"リリースノート"

"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"

"SG100 SG1000サービスアプライアンス"

"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"

"SG5600 ストレージアプライアンス"

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）
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）

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。

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。

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（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アドレスを追加する機能です。詳細については、 StorageGRID の管理手順を参照してください。

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に関する次の要件および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としては、Grid Managerユーザインターフェイスへのアクセス、NTP、DNS、外部キー管理（KMS）、Lightweight Directory Access Protocol（LDAP）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用のSecure Shell Protocol（SSH）アクセスがあります。

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。

管理ネットワークに関する次の要件および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存在する必要はなく、ノードが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。信頼されていないクライアントネットワーク機能とロードバランササービスの詳細については、StorageGRID の管理手順を参照してください。

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。

関連情報

"ネットワークの要件とガイドライン"

"StorageGRID の管理"

"SG100 SG1000サービスアプライアンス"

"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"

"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"

ネットワークトポロジの例

単一サイト環境またはマルチサイト環境のネットワークトポロジを設計する際に、必要なグリッドネットワークに加え、管理ネットワークとクライアントネットワークのインターフェイスを設定するかどうかを選択できます。

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。内部ポートと外部ポートの詳細については、ネットワークポートリファレンスを参照してください。

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して指定する場合は、インバウンドトラフィックを受け入れるようにロードバランサエンドポイントを設定します。信頼されていないクライアントネットワークとロードバランサエンドポイントの設定については、StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

"ネットワークポートのリファレンス"

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。

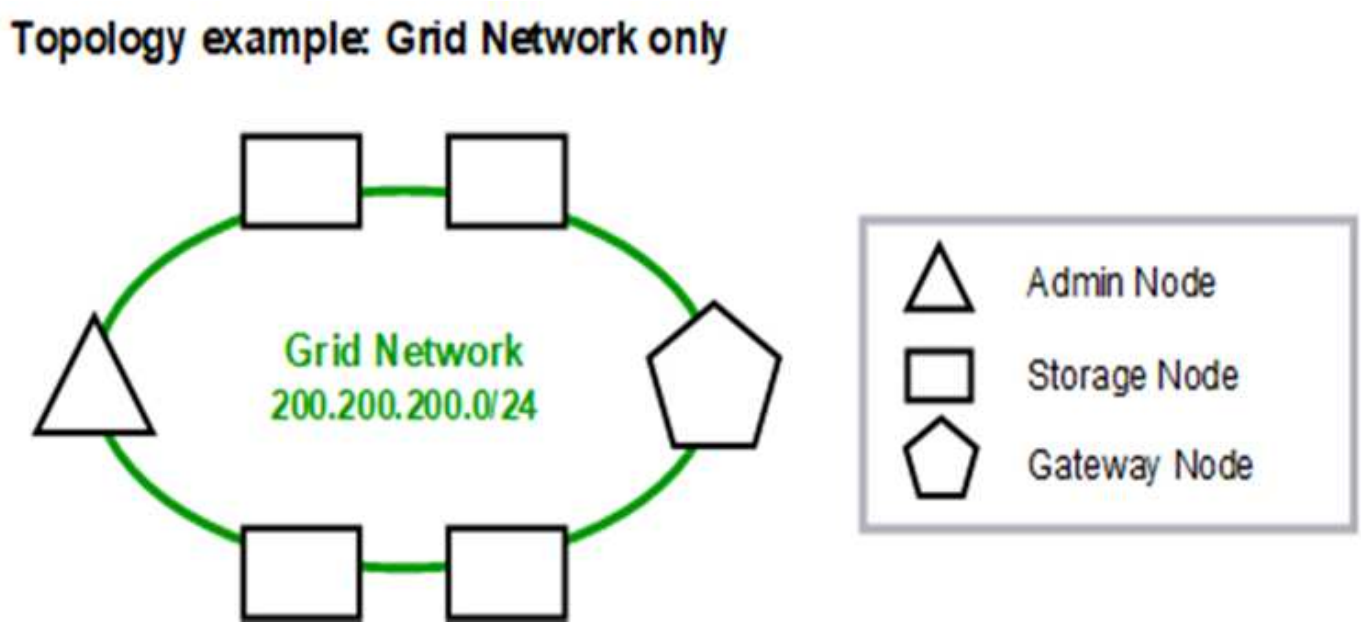
グリッドネットワークを設定するときは、各グリッドノードの eth0 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。

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、外部からは使用できない単一サイトの配置、概念実証またはテスト用の配置、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。



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

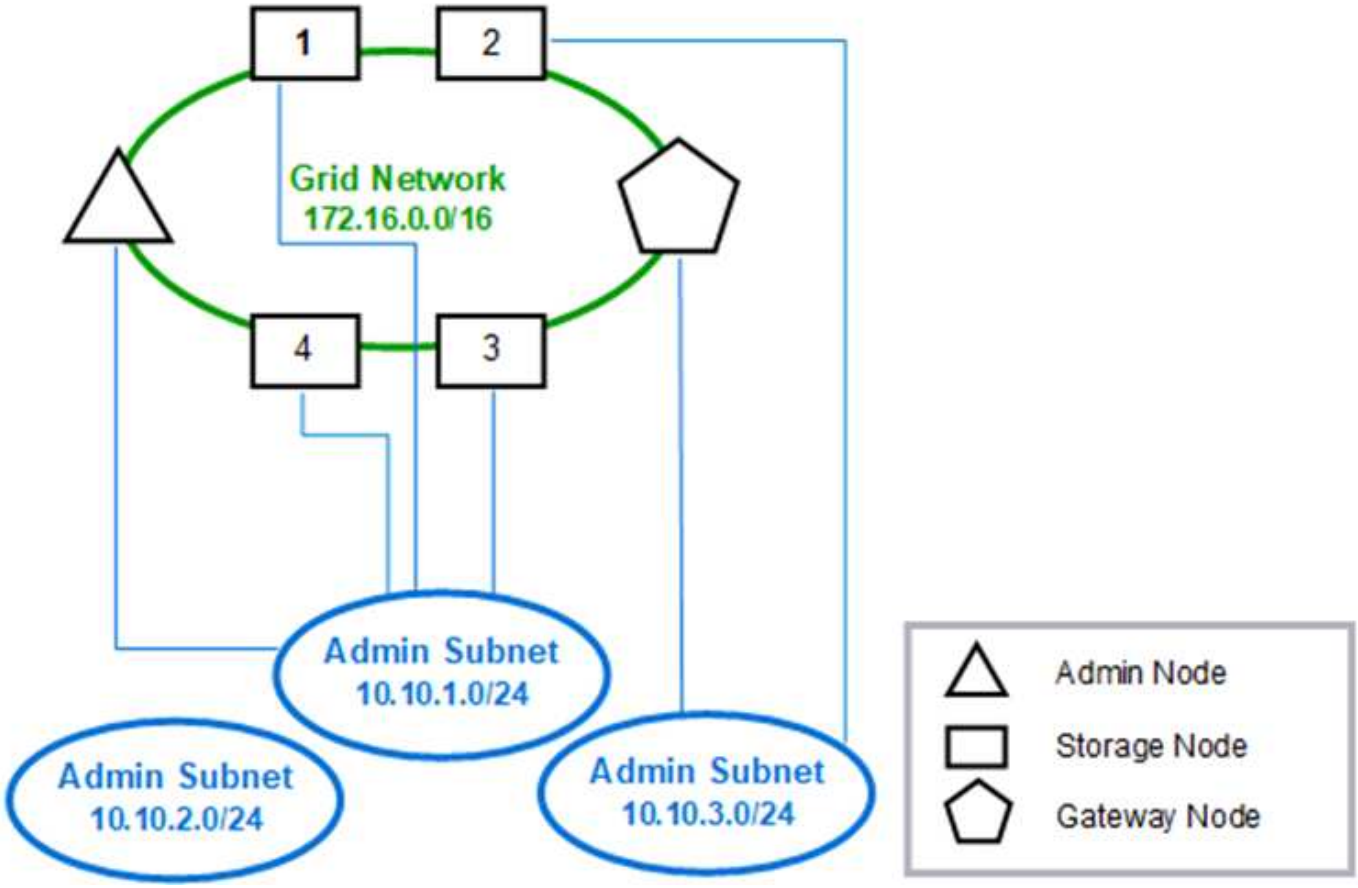
管理ネットワークの使用はオプションです。管理ネットワークとグリッドネットワークを使用する方法の 1 つは、ノードごとにルーティング可能なグリッドネットワークと境界で保護された管理ネットワークを設定することです。

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。

Topology example: Grid and Admin Networks



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。

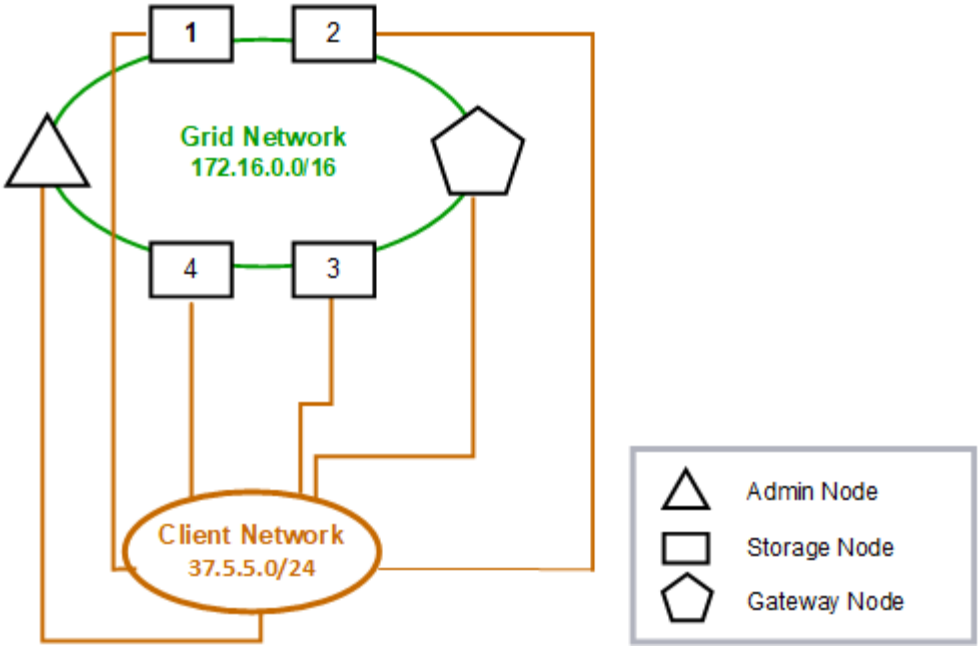
クライアントネットワークを構成するときは、構成済みノードの eth2 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。各ノードのクライアントネットワークは、他のノードのクライアントネットワークとは独立している可能性があります。

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。

Topology example: Grid and Client Networks



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 Generoted

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

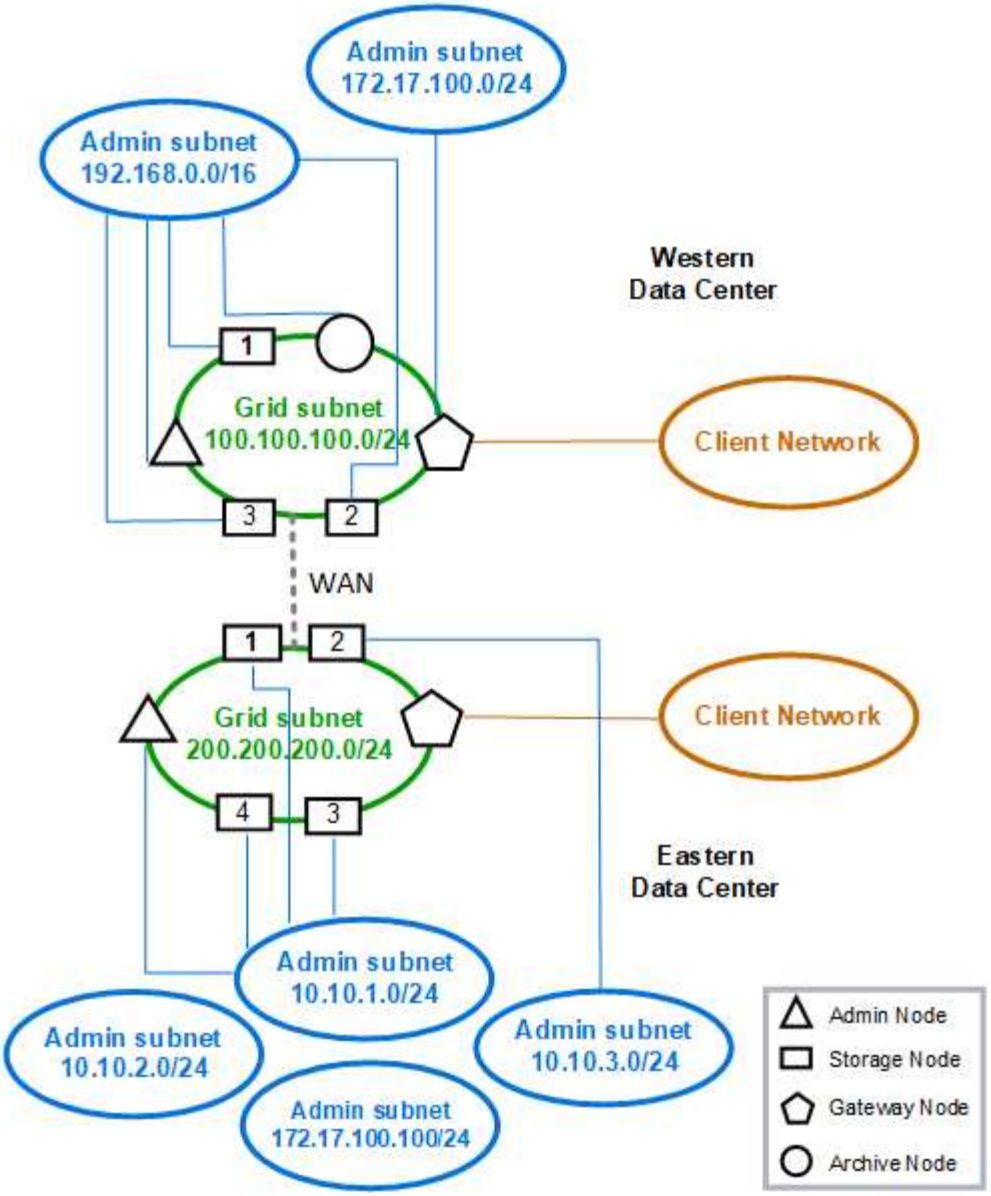
3 つのネットワークすべてのトポロジ

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



著作権に関する情報

商標に関する情報