



ネットワークのガイドライン StorageGRID

NetApp
October 03, 2025

目次

| | |
|---------------------------------------|----|
| ネットワークのガイドライン | 1 |
| StorageGRID ネットワークの概要 | 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 | 5 |
| ネットワーク要件 | 12 |
| 一般的なネットワーク要件 | 12 |
| 管理ノードとゲートウェイノードの接続 | 13 |
| ネットワークアドレス変換（NAT）の使用 | 13 |
| ネットワーク固有の要件 | 14 |
| ネットワークゲートウェイおよびルータ | 14 |
| サブネット | 14 |
| Grid ネットワーク | 14 |
| 管理ネットワーク | 15 |
| クライアントネットワーク | 15 |
| 環境固有のネットワークに関する考慮事項 | 15 |
| Linux の導入 | 16 |
| Docker環境向けのホストネットワーク構成 | 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用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 | 19 |
| ノードの初期導入 | 19 |
| プライマリ管理ノードへの自動ノード登録 | 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します | 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のリファレンス | 21 |
| 内部でのグリッドノードの通信 | 21 |
| 外部との通信 | 25 |

ネットワークのガイドライン

StorageGRID アーキテクチャとネットワークトポロジについて説明します。ネットワークの設定とプロビジョニングの要件を理解します。

- ["StorageGRID ネットワークの概要"](#)
- ["ネットワークの要件とガイドライン"](#)
- ["環境固有のネットワークに関する考慮事項"](#)
- ["ネットワークのインストールとプロビジョニング"](#)
- ["インストール後のガイドライン"](#)
- ["ネットワークポートのリファレンス"](#)

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する必要があります。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。

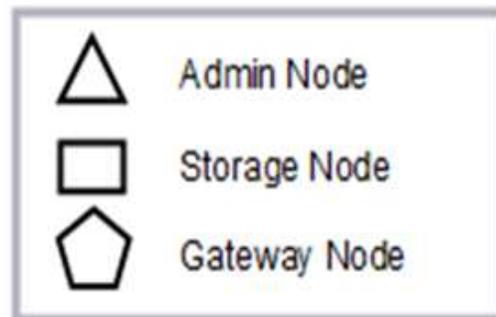
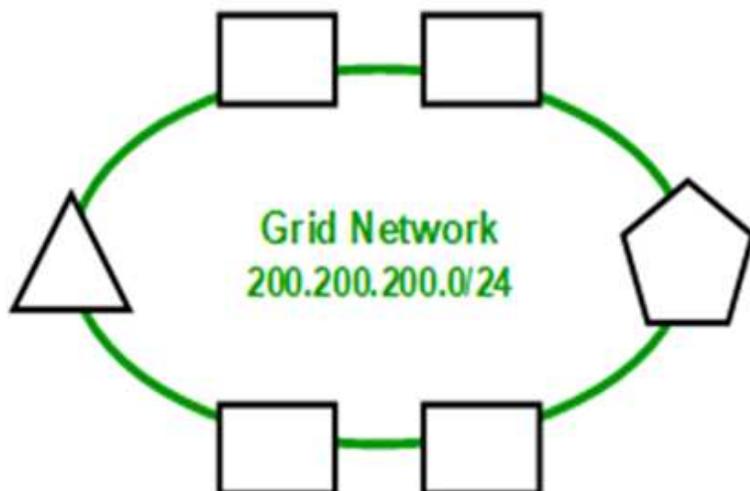
インストール時に、グリッドネットワークのインターフェイスでは、GNSL に含まれるすべてのサブネットに静的ルートが適用され、設定されている場合はノードのデフォルトルートがグリッドネットワークゲートウェイに設定されます。クライアントネットワークがなく、グリッドネットワークゲートウェイがノードのデフォルトルートである場合、GNSL は必要ありません。グリッド内の他のすべてのノードへのホストルートも生成されます。

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。

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。

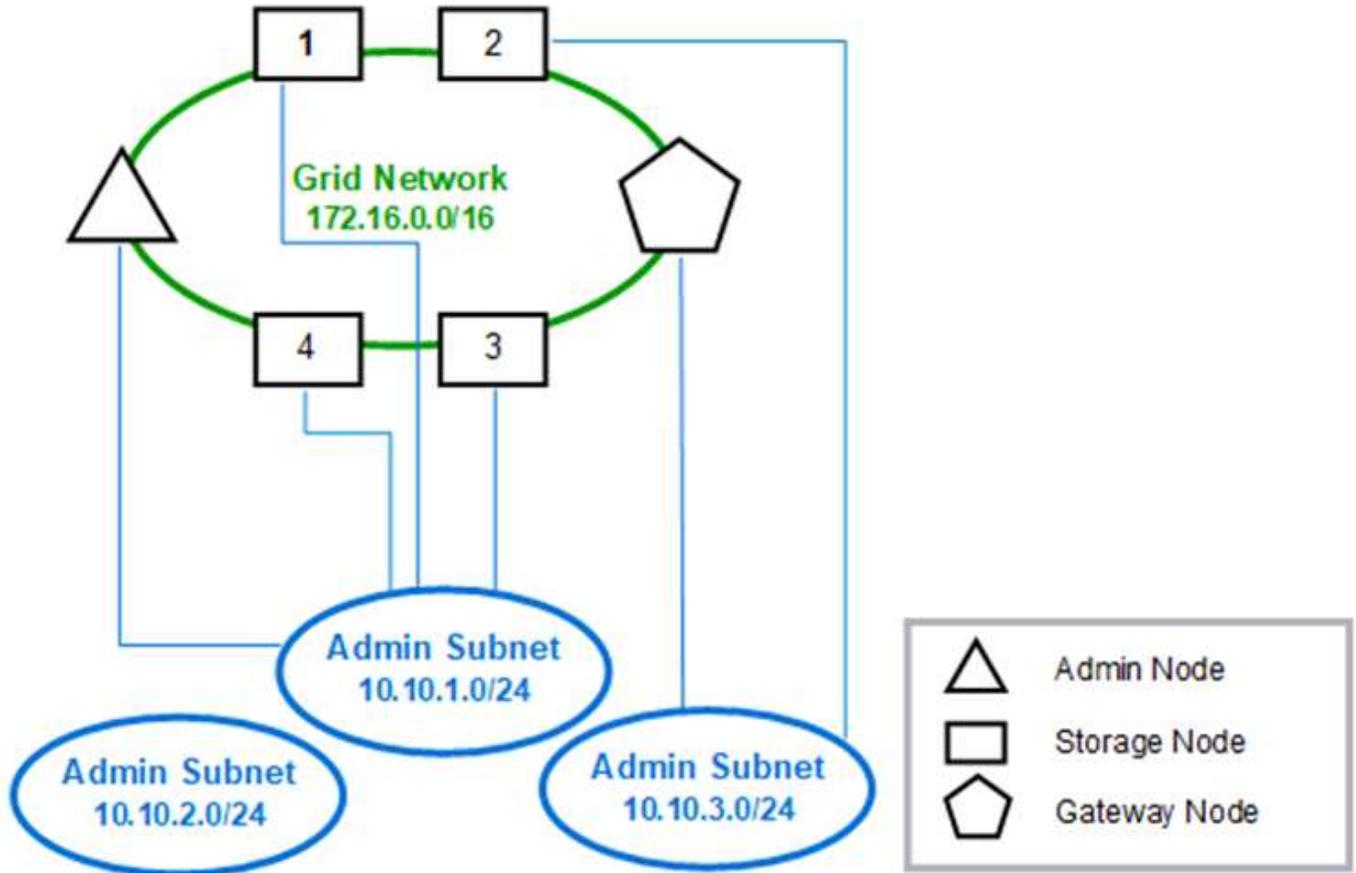
管理ネットワークを設定するときは、各グリッドノードの eth1 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。

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。

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。

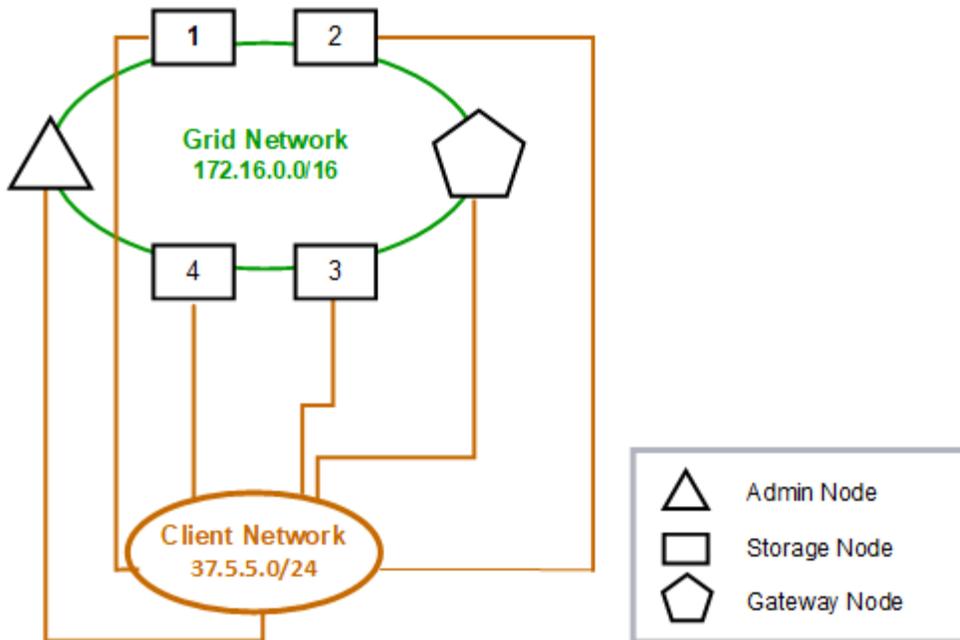
クライアントネットワークを構成するときは、構成済みノードの eth2 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。各ノードのクライアントネットワークは、他のノードのクライアントネットワークとは独立している可能性があります。

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

| 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 |

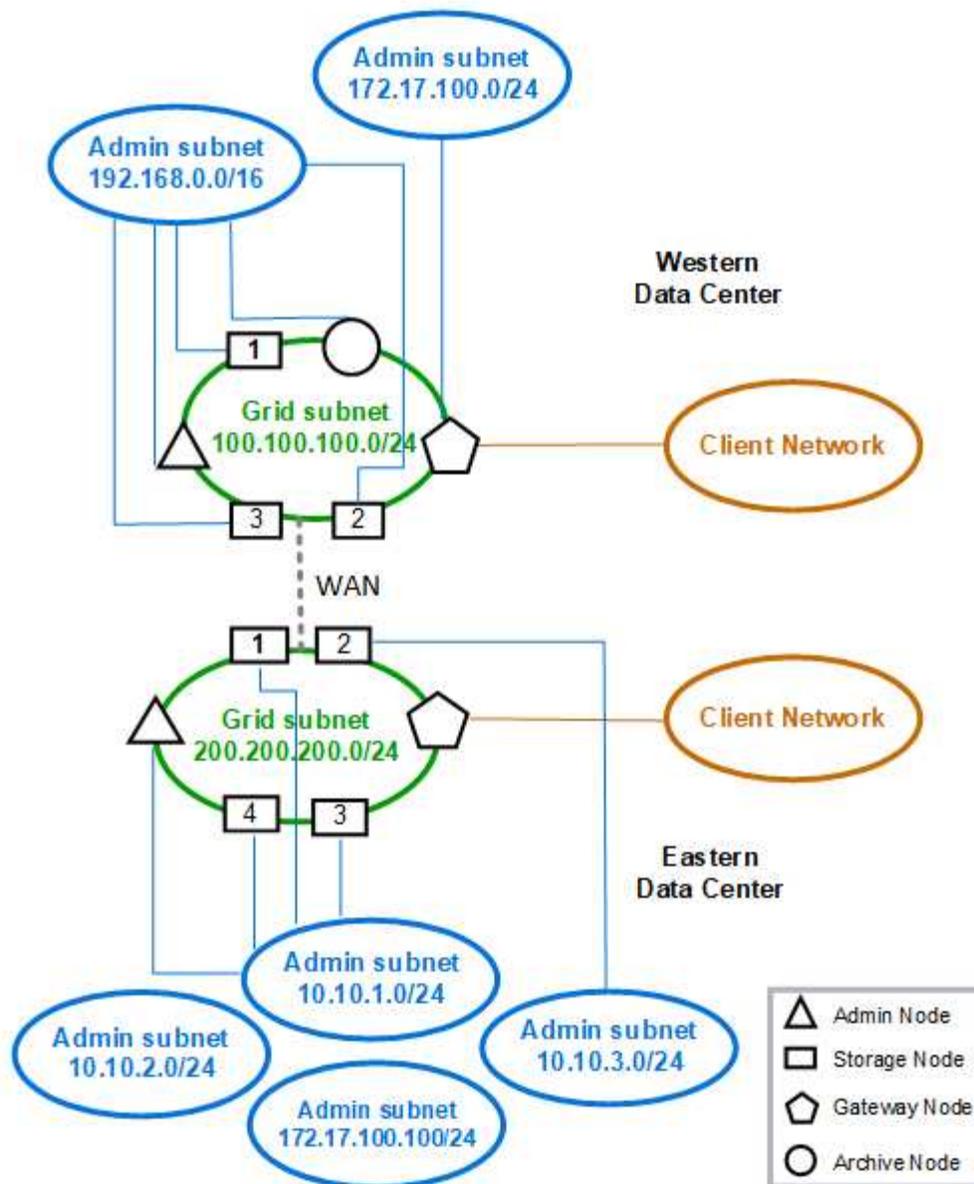
3つのネットワークすべてのトポロジ

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eithersupport.netapp.comまたはお客様が設定したプロキシへのアウトバウンドTCP接続。
- * 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。

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 サーバや DNS サーバと StorageGRID が通信できない場合は、DNS サーバと NTP サーバの IP アドレスが指定されていれば、すべてのネットワーク（グリッド、管理、クライアント）で自動的に接続が試行されます。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せんが、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かった場合は、設定手順でグリッドノードを承認する際にこれらのネットワークを設定できます。また、リカバリとメンテナンスの手順に従ってIP変更ツールを使用すると、インストールの完了後にこれらのネットワークを設定することもできます。

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。StorageGRID の管理手順のハイアベイラビリティグループに関する情報を参照してください。

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のみサポートされます。

関連情報

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 255.255.255.0（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。
- 管理ネットワークのサブネットは、グリッドネットワークのサブネット、クライアントネットワークのサブネット、または GNSL のサブネットと重複することはできません。
- AESL 内のサブネットを GNSL 内のどのサブネットとも重複させることはできません。
- クライアントネットワークのサブネットは、グリッドネットワークのサブネット、管理ネットワークのサブネット、GNSL のサブネット、または AESL に含まれるすべて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する必要があります。
- 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。

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としては、管理接続、AutoSupport、KMS、NTP、DNS、LDAP などの重要なサーバへの接続が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提供されない場合があります。



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。StorageGRID の管理手順のロードバランシングと信頼されていないクライアントネットワークの管理に関する情報を参照してください。

関連情報

["StorageGRID の管理"](#)

環境固有のネットワークに関する考慮事項

使用する導入プラットフォームによっては、StorageGRID ネットワーク設計に関する追加の考慮事項が生じることがあります。

グリッドノードは次のように導入できます。

- VMware vSphere Web Clientで仮想マシンとして導入される、ソフトウェアベースのグリッドノード

- Linuxホスト上のDockerコンテナ内に導入された、ソフトウェアベースのグリッドノード
- アプライアンスベースのノード

グリッドノードに関する追加情報 の場合は、[_グリッド入門_](#)を参照してください。

関連情報

["グリッド入門"](#)

Linux の導入

効率性、信頼性、セキュリティを確保するため、StorageGRID システムはDockerコンテナの集合としてLinux上で動作します。StorageGRID システムではDocker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名前空間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。

Red Hat Enterprise Linux/CentOSまたはUbuntu / Debianの環境でのインストール手順を参照してください。

関連情報

["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"](#)

Docker環境向けのホストネットワーク構成

Dockerコンテナ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。

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別に推奨される最小帯域幅を示します。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 |
| 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 | 1 Gbps | 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: $10 + 1 = 11\text{Gbps}$)
- 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: $10 + 10 = 20\text{Gbps}$)
- 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 $11+20+10=41\text{ Gbps}$ 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 クラスター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

する準備として推奨される方法については、使用しているLinuxプラットフォームのインストール手順のホストネットワークの設定に関する情報を参照してください。

関連情報

["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"](#)

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。この例では、信頼されていないクライアントネットワーク機能を使用して、インバウンド接続を制限できます。

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。

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。

非透過型プロキシサーバを使用する場合は、プロキシの設定で、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する必要があります。プロキシの設定方法については、StorageGRID の管理を参照してください。

信頼されていないクライアントネットワークの詳細については、StorageGRID の管理手順を参照してください。プラットフォームサービスの詳細については、テナントアカウントの使用手順を参照してください。クラウドストレージプールの詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

["ネットワークポートのリファレンス"](#)

["グリッド入門"](#)

["StorageGRID の管理"](#)

["テナントアカウントを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

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。

アプライアンスのインストールとメンテナンスの手順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。

関連情報

["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"](#)

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。リカバリとメンテナンスの手順のネットワークメンテナンスの手順に関する情報を参照してください。

関連情報

■

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。設定時に 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。リカバリとメンテナンスの手順のIPアドレスの設定に関する情報を参照してください。
- 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。ネットワークの変更内容によっては、接続の再確立が必要になる場合があります。

関連情報

["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"](#)

""

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。

内部でのグリッドノードの通信と外部との通信に表示される詳細を使用して、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"
- "外部との通信"

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、ポート 22、80、123、443 を除き、グリッドネットワーク上の特定のポートへの受信接続のみを許可します（外部通信に関する情報を参照）。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を向上させることができます。

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、ハイアベイラビリティ (HA) グループが設定されている場合だけです。

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と導入設定パラメータの詳細については、Linuxプラットフォームのインストール手順を参照してください。

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と導入設定パラメータの詳細については、VMwareのインストール手順を参照してください。

アプライアンスストレージ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。アプライアンスのポート再マッピングの詳細については、ストレージアプライアンスのインストール手順を参照してください。

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する必要があります。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。 |
| 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。 |
| 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。 |
| 5353 | UDP | すべてのノード | すべてのノード | 必要に応じて、フルグリッドの IP 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します。 |
| 7001 | TCP | ストレージノード | ストレージノード | Cassandra TLS ノード間クラスタ通信。 |
| 7443 | TCP | すべてのノード | 管理ノード | 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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"](#)

["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"](#)

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。

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、ロードバランサエンドポイントを使用してユーザ定義のポートへのアクセスを許可できます。信頼されていないクライアントネットワーク機能を使用すると、ロードバランサエンドポイントポートにのみアクセスを許可できません。



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、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、ご使用のプラットフォームのインストール手順を参照してください。

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、ロードバランサエンドポイント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。詳細については、ロードバランサエンドポイントの設定手順を参照してください。

| 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 | ドメインネームシステムに使用します。 |
| 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。 |
| 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。 |

| ポート | tcp または udp です | プロトコル | 移動元 | 終了: | 詳細 |
|-----|----------------|---------|-------------------|--------|--|
| 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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 | <p>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。</p> <ul style="list-style-type: none"> 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 | <p>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。</p> <ul style="list-style-type: none"> 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 | <p>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。</p> <ul style="list-style-type: none"> 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。 |

| ポート | tcp または udp です | プロトコル | 移動元 | 終了: | 詳細 |
|-----|----------------|---------|-------------------|-------------------------|--|
| 162 | TCP / UDP | SNMP 通知 | すべてのノード | 通知の送信先 | <p>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。</p> <ul style="list-style-type: none"> 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。 |
| 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。 |
| 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。 |

| 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 | 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。 <ul style="list-style-type: none"> 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)。 <ul style="list-style-type: none"> 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。 |
| 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。 <ul style="list-style-type: none"> 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 |
|----------|----------------|-------|----------------|-----------|---|
| 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 | サービスラック 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。 |
| 「 8082 」 | TCP | HTTPS | S3 クライアント | ゲートウェイノード | ゲートウェイノードへの S3 関連の外部トラフィック (HTTPS)。 |
| 8083 | TCP | HTTPS | Swift クライアント | ゲートウェイノード | ゲートウェイノードへの Swift 関連の外部トラフィック (HTTPS)。 |
| 8084 | TCP | HTTP | S3 クライアント | ゲートウェイノード | ゲートウェイノードへの S3 関連の外部トラフィック (HTTP)。 |
| 8085 | TCP | HTTP | Swift クライアント | ゲートウェイノード | ゲートウェイノードへの Swift 関連の外部トラフィック (HTTP)。 |
| 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。 |

| 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。 <ul style="list-style-type: none"> 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関連 の外部トラフィック (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関 連の外部トラフィック (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関連 の外部トラフィック (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関 連の外部トラフィック (HTTP)。 |

関連情報

["内部でのグリッドノードの通信"](#)

"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"

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。