



ネットワークポートのリファレンス StorageGRID 11.7

NetApp
April 12, 2024

目次

ネットワークポートのリファレンス	1
内部でのグリッドノードの通信	1
外部との通信	5

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。
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。

ポート	tcp または udp です	移動元	終了：	詳細
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。
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。

ポート	tcp または udp です	移動元	終了：	詳細
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。
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。

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。

ポート	tcp または udp です	プロトコル	移動元	終了：	詳細
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。
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タラ用のポート 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。 <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
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。
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。 <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	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。
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。 <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	<p>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。</p> <p>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。</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。 • 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。
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）。

ポート	tcp または udp です	プロトコル	移動元	終了：	詳細
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。
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）。

ポート	tcp または udp です	プロトコル	移動元	終了：	詳細
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

Copyright © 2024 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。