ファイアウォールを制御する
StorageGRID software

NetApp
December 03, 2025

目次

ファイアウォールを制御する

外部ファイアウォールでアクセスを制御する

外部ファイアウォールで特定のポートを開いたり閉じたりすることができます。

外部ファイアウォールで特定のポートを開いたり閉じたりすることで、 StorageGRID管理ノード上のユーザー インターフェイスと API へのアクセスを制御できます。たとえば、他の方法を使用してシステム アクセスを制御するだけでなく、ファイアウォールでテナントが Grid Manager に接続できないようにすることもできます。

StorageGRID内部ファイアウォールを設定する場合は、"内部ファイアウォールを構成する" 。

ポート	説明	ポートが開いている場合...
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザおよび管理 API クライアントは、グリッド マネージャ、グリッド管理 API、テナント マネージャ、およびテナント管理 API にアクセスできます。 注: ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限されたグリッド マネージャー ポート	• Web ブラウザおよび管理 API クライアントは、HTTPS を使用して Grid Manager および Grid Management API にアクセスできます。 • Web ブラウザおよび管理 API クライアントは、テナント マネージャまたはテナント管理 API にアクセスできません。 • 内部コンテンツのリクエストは拒否されます。
9443	管理ノード上の制限されたテナント マネージャー ポート	• Web ブラウザと管理 API クライアントは、HTTPS を使用してテナント マネージャとテナント管理 API にアクセスできます。 • Web ブラウザおよび管理 API クライアントは、グリッド マネージャーまたはグリッド管理 API にアクセスできません。 • 内部コンテンツのリクエストは拒否されます。

シングル サインオン (SSO) は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザーをシングル サインオンで認証する場合は、デフォルトの HTTPS ポート (443) を使用する必要があります。

関連情報

- "グリッドマネージャーにSign in"
- "テナントアカウントを作成する"

- "外部コミュニケーション"

内部ファイアウォール制御を管理する

StorageGRID には各ノードに内部ファイアウォールが含まれており、ノードへのネットワーク アクセスを制御できるため、グリッドのセキュリティが強化されます。ファイアウォールを使用して、特定のグリッド展開に必要なポートを除くすべてのポートでのネットワーク アクセスを防止します。ファイアウォール制御ページで行った構成の変更は、各ノードに展開されます。

ファイアウォール制御ページの 3 つのタブを使用して、グリッドに必要なアクセスをカスタマイズします。

- 特権アドレス リスト: このタブを使用して、閉じたポートへの選択したアクセスを許可します。 「外部アクセスの管理」タブを使用して、閉じられたポートにアクセスできる IP アドレスまたはサブネットを CIDR 表記で追加できます。
- 外部アクセスの管理: このタブを使用して、デフォルトで開いているポートを閉じたり、以前に閉じたポートを再度開いたりします。
- 信頼されていないクライアント ネットワーク: このタブを使用して、ノードがクライアント ネットワークからの受信トラフィックを信頼するかどうかを指定します。

  このタブの設定は、「外部アクセスの管理」タブの設定を上書きします。

  - 信頼できないクライアント ネットワークを持つノードは、そのノードに設定されているロード バランサ エンドポイント ポート (グローバル、ノード インターフェイス、およびノード タイプにバインドされたエンドポイント) 上の接続のみを受け入れます。
  - ロード バランサのエンドポイント ポートは、[外部ネットワークの管理] タブの設定に関係なく、信頼されていないクライアント ネットワーク上で唯一開いているポートです。
  - 信頼されている場合、[外部アクセスの管理] タブで開かれているすべてのポートと、クライアント ネットワークで開かれているすべてのロード バランサー エンドポイントにアクセスできるようになります。

> あるタブで行った設定は、別のタブで行うアクセスの変更に影響を与える可能性があります。すべてのタブの設定を必ず確認し、ネットワークが期待どおりに動作することを確認してください。

内部ファイアウォール制御を構成するには、"ファイアウォール制御を構成する" 。

外部ファイアウォールとネットワークセキュリティの詳細については、以下を参照してください。"外部ファイアウォールでアクセスを制御する" 。

特権アドレスリストと外部アクセスの管理タブ

特権アドレス リスト タブでは、閉じられているグリッド ポートへのアクセスが許可される 1 つ以上の IP アドレスを登録できます。 [外部アクセスの管理] タブでは、選択した外部ポートまたは開いているすべての外部ポートへの外部アクセスを閉じることができます (外部ポートは、デフォルトで非グリッド ノードからアクセスできるポートです)。多くの場合、これら 2 つのタブを一緒に使用して、グリッドに許可する必要があるネットワーク アクセスを正確にカスタマイズできます。

特権 IP アドレスには、デフォルトでは内部グリッド ポートへのアクセス権がありません。

例**1:** メンテナンスタスクにジャンプホストを使用する

ネットワーク管理にジャンプ ホスト (セキュリティが強化されたホスト) を使用するとします。次の一般的な手順を使用できます。

1. 特権アドレス リスト タブを使用して、ジャンプ ホストの IP アドレスを追加します。
2. すべてのポートをブロックするには、「外部アクセスの管理」タブを使用します。

ポート 443 および 8443 をブロックする前に、特権 IP アドレスを追加します。ブロックされたポートに現在接続しているユーザー (あなたを含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。

設定を保存すると、グリッド内の管理ノード上のすべての外部ポートが、ジャンプ ホストを除くすべてのホストに対してブロックされます。その後、ジャンプ ホストを使用して、グリッド上でメンテナンス タスクをより安全に実行できるようになります。

例**2:** 機密ポートをロックダウンする

機密ポートとそのポート上のサービス (たとえば、ポート 22 上の SSH) をロックダウンするとします。次の一般的な手順を使用できます。

1. 特権アドレス リスト タブを使用して、サービスへのアクセスが必要なホストにのみアクセスを許可します。
2. すべてのポートをブロックするには、「外部アクセスの管理」タブを使用します。

Grid Manager および Tenant Manager にアクセスするために割り当てられたポートへのアクセスをブロックする前に、特権 IP アドレスを追加します (プリセット ポートは 443 と 8443)。ブロックされたポートに現在接続しているユーザー (あなたを含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。

設定を保存すると、特権アドレス リスト上のホストでポート 22 と SSH サービスが利用できるようになります。他のすべてのホストは、リクエストがどのインターフェースから送信されたかに関係なく、サービスへのアクセスを拒否されます。

例**3:** 使用されていないサービスへのアクセスを無効にする

ネットワーク レベルでは、使用しない予定の一部のサービスを無効にすることができます。たとえば、HTTP S3 クライアント トラフィックをブロックするには、[外部アクセスの管理] タブのトグルを使用してポート 18084 をブロックします。

信頼できないクライアントネットワークタブ

クライアント ネットワークを使用している場合は、明示的に構成されたエンドポイントでのみ受信クライアント トラフィックを受け入れることで、 StorageGRID を敵対的な攻撃から保護することができます。

デフォルトでは、各グリッド ノード上のクライアント ネットワークは信頼済みです。つまり、デフォルトでは、 StorageGRIDはすべてのグリッドノードへの受信接続を信頼します。"利用可能な外部ポート" 。

各ノードのクライアント ネットワークを信頼できないものとして指定することで、 StorageGRIDシステムに対する敵対的な攻撃の脅威を軽減できます。ノードのクライアント ネットワークが信頼されていない場合、ノードはロード バランサのエンドポイントとして明示的に構成されたポート上の受信接続のみを受け入れます。見る"ロードバランサのエンドポイントを構成する"そして"ファイアウォール制御を構成する"。

例**1:** ゲートウェイノードは**HTTPS S3**リクエストのみを受け入れる

ゲートウェイ ノードで、HTTPS S3 リクエストを除くクライアント ネットワーク上のすべての受信トラフィックを拒否するとします。次のような一般的な手順を実行します。

1. から"ロード バランサ エンドポイント"ページで、ポート 443 で HTTPS 経由の S3 のロード バランサー エンドポイントを構成します。
2. ファイアウォール制御ページで、「信頼できない」を選択して、ゲートウェイ ノード上のクライアント ネットワークが信頼できないことを指定します。

設定を保存すると、ポート 443 の HTTPS S3 要求と ICMP エコー (ping) 要求を除き、ゲートウェイ ノードのクライアント ネットワーク上のすべての受信トラフィックがドロップされます。

例**2:** ストレージノードが**S3**プラットフォームサービスリクエストを送信する

ストレージ ノードからの送信 S3 プラットフォーム サービス トラフィックを有効にしたいが、クライアント ネットワーク上のそのストレージ ノードへの受信接続を禁止したいとします。次のような一般的な手順を実行します。

- ファイアウォール制御ページの「信頼できないクライアント ネットワーク」タブで、ストレージ ノード上のクライアント ネットワークが信頼できないことを示します。

構成を保存すると、ストレージ ノードはクライアント ネットワーク上の着信トラフィックを受け入れなくなりますが、構成されたプラットフォーム サービスの宛先への送信要求は引き続き許可されます。

例**3:** グリッドマネージャへのアクセスをサブネットに制限する

特定のサブネット上でのみ Grid Manager アクセスを許可するとします。次の手順を実行します。

1. 管理ノードのクライアント ネットワークをサブネットに接続します。
2. 「信頼できないクライアント ネットワーク」タブを使用して、クライアント ネットワークを信頼できないものとして構成します。
3. 管理インターフェイス ロード バランサ エンドポイントを作成するときは、ポートを入力し、ポートがアクセスする管理インターフェイスを選択します。
4. 信頼できないクライアントネットワークに対して*はい*を選択します。
5. [外部アクセスの管理] タブを使用して、すべての外部ポート (そのサブネットの外部のホストに特権 IP アドレスが設定されているかどうかに関係なく) をブロックします。

設定を保存すると、指定したサブネット上のホストのみがグリッド マネージャーにアクセスできるようになります。その他のホストはすべてブロックされます。

内部ファイアウォールを構成する

StorageGRIDファイアウォールを設定して、 StorageGRIDノード上の特定のポートへの

ネットワーク アクセスを制御できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。
- 下記の情報を確認しました"ファイアウォール制御を管理する"そして"ネットワークガイドライン"。
- 管理ノードまたはゲートウェイ ノードが明示的に構成されたエンドポイントでのみ受信トラフィックを受け入れるようにする場合は、ロード バランサのエンドポイントを定義しておきます。

> クライアント ネットワークの設定を変更する場合、ロード バランサのエンドポイントが構成されていないと、既存のクライアント接続が失敗する可能性があります。

タスク概要

StorageGRID には各ノードに内部ファイアウォールが含まれており、グリッドのノード上の一部のポートを開いたり閉じたりすることができます。ファイアウォール コントロール タブを使用して、グリッド ネットワーク、管理ネットワーク、およびクライアント ネットワークでデフォルトで開いているポートを開いたり閉じたりすることができます。閉じられているグリッド ポートにアクセスできる特権 IP アドレスのリストを作成することもできます。クライアント ネットワークを使用している場合は、ノードがクライアント ネットワークからの受信トラフィックを信頼するかどうかを指定し、クライアント ネットワーク上の特定のポートのアクセスを構成できます。

グリッド外部の IP アドレスに開くポートの数を絶対に必要なものだけに制限すると、グリッドのセキュリティが強化されます。 3 つのファイアウォール制御タブのそれぞれの設定を使用して、必要なポートのみが開かれていることを確認します。

ファイアウォール制御の使用に関する詳細（例を含む）については、以下を参照してください。"ファイアウォール制御を管理する" 。

外部ファイアウォールとネットワークセキュリティの詳細については、以下を参照してください。"外部ファイアウォールでアクセスを制御する" 。

ファイアウォール制御へのアクセス

手順

1. 構成 > セキュリティ > *ファイアウォール制御*を選択します。

   このページの3つのタブについては、"ファイアウォール制御を管理する" 。

2. ファイアウォール コントロールを構成するには、任意のタブを選択します。

   これらのタブは任意の順序で使用できます。 1 つのタブで設定した内容によって他のタブで実行できる内容が制限されることはありませんが、1 つのタブで行った設定変更によって、他のタブで設定されたポートの動作が変わる場合があります。

特権アドレスリスト

[特権アドレス リスト] タブを使用して、デフォルトで閉じられているポート、または [外部アクセスの管理] タブの設定によって閉じられているポートへのホスト アクセスを許可します。

特権 IP アドレスとサブネットには、デフォルトでは内部グリッド アクセスがありません。また、[特権アドレス一覧] タブで開かれたロード バランサーのエンドポイントと追加のポートには、[外部アクセスの管理] タブでブロックされていてもアクセスできます。

[特権アドレス リスト] タブの設定は、[信頼されていないクライアント ネットワーク] タブの設定を上書きできません。

手順

1. [特権アドレス リスト] タブで、閉じたポートへのアクセスを許可するアドレスまたは IP サブネットを入力します。
2. 必要に応じて、別の **IP** アドレスまたはサブネットを **CIDR** 表記で追加 を選択して、特権クライアントを追加します。

   特権リストに追加するアドレスはできる限り少なくします。

3. 必要に応じて、「特権 IP アドレスにStorageGRID内部ポートへのアクセスを許可する」を選択します。見る"StorageGRID内部ポート" 。

   このオプションは、内部サービスに対する一部の保護を削除します。可能であれば無効のままにしておきます。

4. *保存*を選択します。

外部アクセスを管理する

[外部アクセスの管理] タブでポートが閉じられている場合、IP アドレスを特権アドレス リストに追加しない限り、グリッド以外の IP アドレスからポートにアクセスすることはできません。閉じることができるのはデフォルトで開いているポートのみであり、開くことができるのは閉じたポートのみです。

[外部アクセスの管理] タブの設定は、[信頼されていないクライアント ネットワーク] タブの設定を上書きできません。たとえば、ノードが信頼されていない場合、ポート SSH/22 は [外部アクセスの管理] タブで開いている場合でも、クライアント ネットワーク上でブロックされます。 [信頼されていないクライアント ネットワーク] タブの設定は、クライアント ネットワーク上の閉じたポート (443、8443、9443 など) を上書きします。

手順

1. *外部アクセスの管理*を選択します。タブには、グリッド内のノードのすべての外部ポート (デフォルトでは非グリッド ノードからアクセス可能なポート) を含むテーブルが表示されます。
2. 次のオプションを使用して、開くポートと閉じるポートを構成します。
   - 各ポートの横にあるトグルを使用して、選択したポートを開いたり閉じたりします。
   - 表にリストされているすべてのポートを開くには、「表示されているすべてのポートを開く」を選択します。
   - 表にリストされているすべてのポートを閉じるには、「表示されているすべてのポートを閉じる」を選択します。

Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。

利用可能なすべてのポートが表示されていることを確認するには、表の右側にあるスクロール バーを使用します。検索フィールドにポート番号を入力して、任意の外部ポートの設定を検索します。ポート番号の一部を入力できます。たとえば、「**2**」と入力すると、名前の一部に文字列「2」が含まれるすべてのポートが表示されます。

3. *保存*を選択

信頼できないクライアントネットワーク

ノードのクライアント ネットワークが信頼されていない場合、ノードは、ロード バランサのエンドポイントとして構成されたポートと、オプションでこのタブで選択した追加のポート上の受信トラフィックのみを受け入れます。このタブを使用して、拡張で追加された新しいノードのデフォルト設定を指定することもできます。

ロード バランサのエンドポイントが構成されていない場合、既存のクライアント接続が失敗する可能性があります。

信頼されていないクライアント ネットワーク タブで行った構成の変更は、外部アクセスの管理 タブの設定を上書きします。

手順

1. *信頼されていないクライアントネットワーク*を選択します。
2. [新しいノードのデフォルトの設定] セクションでは、拡張手順でグリッドに新しいノードが追加されたときのデフォルト設定を指定します。
   - 信頼済み (デフォルト): 拡張でノードが追加されると、そのクライアント ネットワークは信頼されます。
   - 信頼されていない: 拡張でノードが追加されると、そのクライアント ネットワークは信頼されなくなります。

     必要に応じて、このタブに戻って特定の新しいノードの設定を変更できます。

     この設定は、 StorageGRIDシステム内の既存のノードには影響しません。
3. 明示的に構成されたロード バランサ エンドポイントまたは追加の選択されたポートでのみクライアント接続を許可するノードを選択するには、次のオプションを使用します。
   - *表示されているノードを信頼しない*を選択すると、テーブルに表示されているすべてのノードが信頼できないクライアント ネットワーク リストに追加されます。
   - *表示されているノードを信頼する*を選択すると、テーブルに表示されているすべてのノードが信頼されていないクライアント ネットワーク リストから削除されます。
   - 各ノードの横にあるトグルを使用して、選択したノードのクライアント ネットワークを信頼済みまたは信頼なしに設定します。

たとえば、「表示されているノードを信頼しない」を選択して、すべてのノードを信頼できないクライアント ネットワーク リストに追加し、個々のノードの横にあるトグルを使用して、その単一のノードを信頼できるクライアント ネットワーク リストに追加することができます。

利用可能なすべてのノードが表示されていることを確認するには、テーブルの右側にあるスクロール バーを使用します。検索フィールドにノード名を入力して、任意のノードの設定を検索します。名前の一部を入力できます。たとえば、**GW** と入力すると、名前の一部に文字列「GW」が含まれるすべてのノードが表示されます。

4. *保存*を選択します。

新しいファイアウォール設定はすぐに適用され、強制されます。ロード バランサのエンドポイントが構成されていない場合、既存のクライアント接続が失敗する可能性があります。

著作権に関する情報

商標に関する情報