信頼されていないクライアントネットワークの管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

信頼されていないクライアントネットワークの管理

クライアントネットワークを使用している場合は、明示的に設定された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。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRID は、使用可能なすべての外部ポートでの各グリッドノードへのインバウンド接続をデフォルトで信頼します（ネットワークガイドラインの外部通信に関する情報を参照）。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある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エンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。

例 1 ：ゲートウェイノードが HTTPS S3 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. Load Balancer Endpoints ページで、ポート 443 で S3 over HTTPS のロードバランサエンドポイントを設定します。
2. Untrusted Client Networks ページで、ゲートウェイ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ことを指定します。

設定を保存すると、ポート 443 での 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インバウンドトラフィックが破棄されます。

例 2 ：ストレージノードが S3 プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンド S3 プラットフォームサービストラフィックは有効にするが、クライアントネットワークでそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- Untrusted Client Networks ページで、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されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、 Amazon Web Services へのアウトバウンド要求は引き続き許可します。

関連情報

"ネットワークガイドライン"

"ロードバランサエンドポイントの設定"

ノードのクライアントネットワークの指定は信頼されていません

クライアントネットワークを使用している場合は、各ノードのクライアントネットワークが信頼されているかどうかを指定できます。拡張で追加し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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

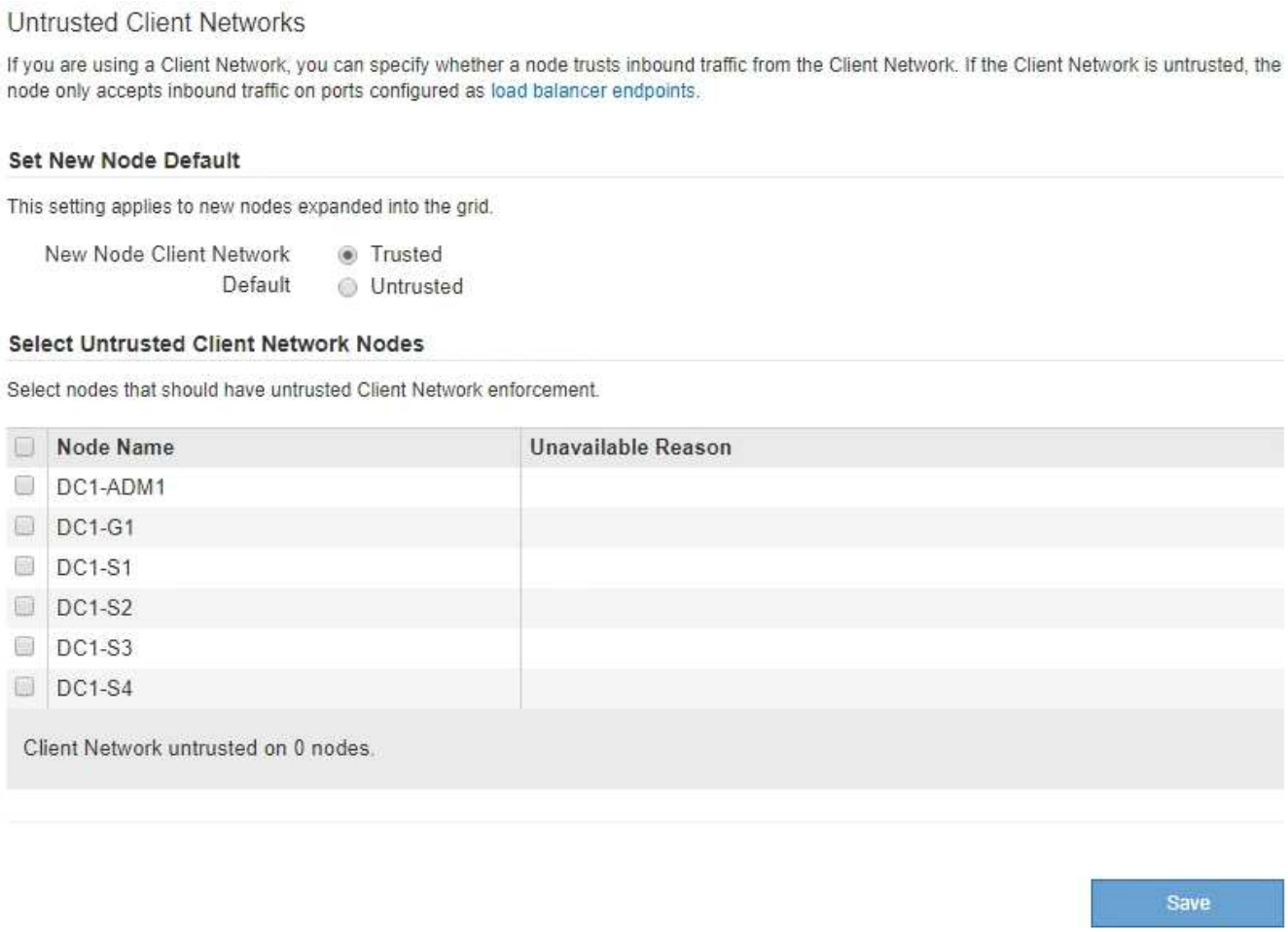
> ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

手順

1. 「* Configuration * Network Settings * Untrusted Client Network *」を選択します。

   [Untrusted Client Networks]ページが表示されます。

   このページには、StorageGRID システム内のすべてのノードが表示されます。ノードのクライアントネットワークが信頼されている必要がある場合は、 Unavailable Reason 列にエントリが表示されます。



2. Set New Node Default * セクションで、拡張手順 で新しいノードをグリッドに追加するときのデフォルト設定を指定します。

   - * Trusted * ：拡張でノードが追加されるときに、そのクライアントネットワークが信頼されます。
   - * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。必要に応じて、このページに戻って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. Select Untrusted Client Network Nodes * セクションで、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クライアント接続を許可するノードを選択します。

   タイトルのチェックボックスをオンまたはオフにすると、すべてのノードを選択または選択解除できます。

4. [保存（ Save ）] をクリックします。

   新しいファイアウォールルールがすぐに追加され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

関連情報

"ロードバランサエンドポイントの設定"

著作権に関する情報

商標に関する情報