セキュリティ設定を構成する
StorageGRID software

NetApp
December 03, 2025

目次

セキュリティ設定を構成する

TLSおよびSSHポリシーを管理する

TLS および SSH ポリシーは、クライアント アプリケーションとの安全な TLS 接続と内部StorageGRIDサービスへの安全な SSH 接続を確立するために使用されるプロトコルと暗号を決定します。

セキュリティ ポリシーは、TLS と SSH が移動中のデータを暗号化する方法を制御します。一般に、システムが Common Criteria に準拠している必要がある場合、または他の暗号を使用する必要がない限り、最新の互換性 (デフォルト) ポリシーを使用します。

> 一部のStorageGRIDサービスは、これらのポリシーの暗号を使用するように更新されていません。

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" 。
- あなたは"ルートアクセス権限"。

セキュリティポリシーを選択する

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。

   TLS および **SSH** ポリシー タブには、使用可能なポリシーが表示されます。現在アクティブなポリシーは、ポリシー タイルに緑色のチェック マークで表示されます。

2. タイルを確認して、利用可能なポリシーについて学習します。

ポリシー	説明
最新の互換性（デフォルト）	強力な暗号化が必要な場合や特別な要件がない限り、デフォルトのポリシーを使用します。このポリシーは、ほとんどの TLS および SSH クライアントと互換性があります。

ポリシー	説明
レガシー互換性	古いクライアントに追加の互換性オプションが必要な場合は、このポリシーを使用します。このポリシーの追加オプションにより、モダン互換性ポリシーよりも安全性が低くなる可能性があります。
コモンクライテリア	Common Criteria 認証が必要な場合は、このポリシーを使用します。
FIPS厳格	Common Criteria 認定が必要であり、ロード バランサ エンドポイント、Tenant Manager、および Grid Manager への外部クライアント接続にNetApp暗号化セキュリティ モジュール 3.0.8 を使用する必要がある場合は、このポリシーを使用します。このポリシーを使用するとパフォーマンスが低下する可能性があります。 注意: このポリシーを選択した後は、すべてのノードが"ローリング方式で再起動"NetApp暗号化セキュリティ モジュールをアクティブ化します。再起動を開始および監視するには、[メンテナンス] > [ローリング再起動] を使用します。
カスタム	独自の暗号を適用する必要がある場合は、カスタム ポリシーを作成します。

3. 各ポリシーの暗号、プロトコル、アルゴリズムの詳細を表示するには、[詳細を表示] を選択します。
4. 現在のポリシーを変更するには、[ポリシーの使用] を選択します。

   ポリシー タイルの 現在のポリシー の横に緑色のチェック マークが表示されます。

カスタムセキュリティポリシーを作成する

独自の暗号を適用する必要がある場合は、カスタム ポリシーを作成できます。

手順

1. 作成するカスタム ポリシーに最も類似したポリシーのタイルから、[詳細の表示] を選択します。
2. *クリップボードにコピー*を選択し、*キャンセル*を選択します。

3. カスタム ポリシー タイルから、構成して使用 を選択します。
4. コピーした JSON を貼り付けて、必要な変更を加えます。
5. *ポリシーを使用する*を選択します。

   カスタム ポリシー タイルの 現在のポリシー の横に緑色のチェック マークが表示されます。

6. 必要に応じて、[構成の編集] を選択して、新しいカスタム ポリシーにさらに変更を加えます。

一時的にデフォルトのセキュリティポリシーに戻す

カスタムセキュリティポリシーを設定した場合、設定されたTLSポリシーが"構成されたサーバー証明書"。

一時的にデフォルトのセキュリティ ポリシーに戻すことができます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。

2. 次のコマンドを実行します。

   ```
   restore-default-cipher-configurations
   ```

3. Web ブラウザから、同じ管理ノード上のグリッド マネージャーにアクセスします。
4. 以下の手順に従ってくださいセキュリティポリシーを選択するポリシーを再度構成します。

ネットワークとオブジェクトのセキュリティを構成する

ネットワークとオブジェクトのセキュリティを設定して、保存されたオブジェクトを暗号化したり、特定の S3 リクエストを防止したり、ストレージノードへのクライアント接続で HTTPS ではなく HTTP を使用できるようにしたりできます。

保存されたオブジェクトの暗号化

保存されたオブジェクトの暗号化により、S3 を介して取り込まれるすべてのオブジェクト データの暗号化が可能になります。デフォルトでは、保存されたオブジェクトは暗号化されませんが、AES‐128 または AES‐256 暗号化アルゴリズムを使用してオブジェクトを暗号化することを選択できます。この設定を有効にすると、新しく取り込まれたすべてのオブジェクトが暗号化されますが、既存の保存されたオブジェクトは変更されません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままになりますが、新しく取り込まれたオブジェクトは暗号化されません。

保存されたオブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化によって暗号化されていない S3 オブジェクトにのみ適用されます。

StorageGRID暗号化方式の詳細については、以下を参照してください。"StorageGRIDの暗号化方式を確認する" 。

クライアントの変更を防止する

クライアントの変更を禁止するのはシステム全体の設定です。 クライアントの変更を禁止する オプションを選択すると、次の要求は拒否されます。

S3 REST API

- DeleteBucketリクエスト
- 既存のオブジェクトのデータ、ユーザー定義のメタデータ、または S3 オブジェクトのタグ付けを変更するリクエスト

ストレージノード接続に**HTTP**を有効にする

デフォルトでは、クライアント アプリケーションは、ストレージ ノードへの直接接続に HTTPS ネットワーク プロトコルを使用します。オプションで、非本番グリッドをテストする場合など、これらの接続に対して HTTP を有効にすることもできます。

S3 クライアントがストレージ ノードに直接 HTTP 接続を行う必要がある場合にのみ、ストレージ ノード接続に HTTP を使用します。 HTTPS接続のみを使用するクライアントや、ロードバランササービスに接続するクライアントの場合は、このオプションを使用する必要はありません（"各ロードバランサのエンドポイントを構成する" HTTP または HTTPS のいずれかを使用します。

見る"概要: クライアント接続の IP アドレスとポート"HTTP または HTTPS を使用してストレージ ノードに接続するときに S3 クライアントが使用するポートを確認します。

オプションを選択

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" 。
- ルートアクセス権限があります。

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。
2. *ネットワークとオブジェクト*タブを選択します。
3. 保存されたオブジェクトの暗号化については、保存されたオブジェクトを暗号化しない場合は なし (デフォルト) 設定を使用し、保存されたオブジェクトを暗号化するには **AES-128** または **AES-256** を選択します。
4. S3 クライアントが特定のリクエストを行わないようにする場合は、オプションで クライアントの変更を禁止する を選択します。

   この設定を変更した場合、新しい設定が適用されるまで約 1 分かかります。構成された値は、パフォーマンスとスケーリングのためにキャッシュされます。

5. クライアントがストレージ ノードに直接接続し、HTTP 接続を使用する場合は、オプションで [ストレージ ノード接続に **HTTP** を有効にする] を選択します。

   実稼働グリッドで HTTP を有効にする場合は、リクエストが暗号化されずに送信されるため注意してください。

6. *保存*を選択します。

インターフェースのセキュリティ設定を変更する

インターフェース セキュリティ設定では、指定された時間を超えてユーザーが非アクティブだった場合にユーザーをログアウトするかどうか、および API エラー応答にスタック トレースを含めるかどうかを制御できます。

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"ルートアクセス権限"。

タスク概要

セキュリティ設定 ページには、ブラウザの非アクティブ タイムアウト と 管理 **API** スタック トレース の設定が含まれています。

ブラウザの非アクティブタイムアウト

ユーザーがサインアウトするまでに、ユーザーのブラウザが非アクティブになっていられる時間を示します。デフォルトは15分です。

ブラウザの非アクティブ タイムアウトは、次の要素によっても制御されます。

- システム セキュリティのために組み込まれた、個別の構成不可能なStorageGRIDタイマー。各ユーザーの認証トークンは、ユーザーがサインインしてから 16 時間後に期限切れになります。ユーザーの認証の有効期限が切れると、ブラウザの非アクティブ タイムアウトが無効になっている場合やブラウザ

のタイムアウト値に達していない場合でも、そのユーザーは自動的にサインアウトされます。トークンを更新するには、ユーザーは再度サインインする必要があります。

- StorageGRIDでシングル サインオン (SSO) が有効になっていることを前提とした、ID プロバイダーのタイムアウト設定。

  SSO が有効になっていて、ユーザーのブラウザがタイムアウトした場合、ユーザーは SSO 資格情報を再入力してStorageGRID に再度アクセスする必要があります。見る"シングルサインオンを構成する" 。

管理**API**スタックトレース

Grid Manager および Tenant Manager API エラー応答でスタック トレースが返されるかどうかを制御します。

このオプションはデフォルトで無効になっていますが、テスト環境ではこの機能を有効にする必要がある場合があります。一般に、API エラーが発生したときに内部ソフトウェアの詳細が公開されないように、運用環境ではスタック トレースを無効のままにしておく必要があります。

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。
2. *インターフェース*タブを選択します。
3. ブラウザの非アクティブタイムアウトの設定を変更するには:
   a. アコーディオンを展開します。
   b. タイムアウト期間を変更するには、60 秒から 7 日間の値を指定します。デフォルトのタイムアウトは 15 分です。
   c. この機能を無効にするには、チェックボックスをオフにします。
   d. *保存*を選択します。

      新しい設定は、現在サインインしているユーザーには影響しません。新しいタイムアウト設定を有効にするには、ユーザーは再度サインインするか、ブラウザを更新する必要があります。

4. 管理 API スタック トレースの設定を変更するには:
   a. アコーディオンを展開します。
   b. チェックボックスを選択すると、Grid Manager および Tenant Manager API エラー応答でスタック トレースが返されます。

      

      API エラーが発生したときに内部ソフトウェアの詳細が公開されないように、運用環境ではスタック トレースを無効のままにしておきます。

   c. *保存*を選択します。

著作権に関する情報

商標に関する情報