セキュリティを管理する
StorageGRID software

NetApp
December 03, 2025

目次

セキュリティを管理する

セキュリティを管理する

Grid Manager からさまざまなセキュリティ設定を構成して、 StorageGRIDシステムのセキュリティを強化できます。

暗号化を管理する

StorageGRID は、データを暗号化するためのいくつかのオプションを提供します。あなたがすべき"利用可能な暗号化方式を確認する"どれがデータ保護要件を満たしているかを判断します。

証明書の管理

あなたはできる"サーバー証明書の設定と管理"HTTP 接続に使用され、またはサーバーに対してクライアントまたはユーザーの ID を認証するために使用されるクライアント証明書です。

キー管理サーバーを構成する

使用して"鍵管理サーバー"アプライアンスがデータセンターから削除された場合でも、 StorageGRIDデータを保護できます。アプライアンス ボリュームが暗号化された後は、ノードが KMS と通信できない限り、アプライアンス上のデータにアクセスできなくなります。

> 暗号化キー管理を使用するには、アプライアンスをグリッドに追加する前に、インストール中に各アプライアンスの ノード暗号化 設定を有効にする必要があります。

プロキシ設定を管理する

S3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している場合は、"ストレージプロキシサーバー"ストレージノードと外部 S3 エンドポイント間。 HTTPSまたはHTTPを使用してAutoSupportパッケージを送信する場合は、"管理プロキシサーバー"管理ノードとテクニカル サポート間。

ファイアウォールを制御する

システムのセキュリティを強化するために、特定のポートを開いたり閉じたりすることで、 StorageGRID管理ノードへのアクセスを制御できます。"外部ファイアウォール" 。各ノードのネットワークアクセスを制御するには、"内部ファイアウォール" 。展開に必要なポートを除くすべてのポートへのアクセスを禁止できます。

StorageGRIDの暗号化方式を確認する

StorageGRID は、データを暗号化するためのいくつかのオプションを提供します。利用可能な方法を確認して、どの方法がデータ保護要件を満たすかを判断する必要があります。

この表は、 StorageGRIDで使用できる暗号化方法の概要を示しています。

暗号化オプション	仕組み	適用対象
グリッド マネージャーのキー管理サーバー (KMS)	あなた"キー管理サーバーを構成する"StorageGRIDサイトと "アプライアンスのノード暗号化を有効にする"。次に、アプライアンス ノードは KMS に接続してキー暗号化キー (KEK) を要求します。このキーは、各ボリューム上のデータ暗号化キー (DEK) を暗号化および復号化します。	インストール中に ノード暗号化 が有効になっているアプライアンス ノード。アプライアンス上のすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。 注: KMS を使用した暗号化キーの管理は、ストレージ ノードとサービス アプライアンスでのみサポートされます。
StorageGRIDアプライアンスインストーラのドライブ暗号化ページ	アプライアンスにハードウェア暗号化をサポートするドライブが含まれている場合は、インストール中にドライブのパスフレーズを設定できます。ドライブ パスフレーズを設定すると、パスフレーズを知らない限り、システムから削除されたドライブから有効なデータを回復することは不可能になります。インストールを開始する前に、ハードウェアの構成 > ドライブ暗号化 に移動して、ノード内のすべてのStorageGRID管理の自己暗号化ドライブに適用されるドライブ パスフレーズを設定します。	自己暗号化ドライブを搭載したアプライアンス。保護されたドライブ上のすべてのデータは、物理的な紛失やデータセンターからの削除から保護されます。 ドライブ暗号化は、 SANtricity管理ドライブには適用されません。自己暗号化ドライブとSANtricityコントローラを備えたストレージ アプライアンスがある場合は、SANtricityでドライブ セキュリティを有効にすることができます。
SANtricity System Manager のドライブセキュリティ	StorageGRIDアプライアンスでドライブセキュリティ機能が有効になっている場合は、 "SANtricity System Manager"セキュリティ キーを作成および管理します。保護されたドライブ上のデータにアクセスするには、キーが必要です。	フルディスク暗号化 (FDE) ドライブまたは自己暗号化ドライブを備えたストレージアプライアンス。保護されたドライブ上のすべてのデータは、物理的な紛失やデータセンターからの削除から保護されます。一部のストレージ アプライアンスまたはサービス アプライアンスでは使用できません。
保存されたオブジェクトの暗号化	有効にすると、"保存されたオブジェクトの暗号化"グリッド マネージャーのオプション。有効にすると、バケット レベルまたはオブジェクト レベルで暗号化されていない新しいオブジェクトは、取り込み時に暗号化されます。	新しく取り込まれた S3 オブジェクト データ。 既存の保存オブジェクトは暗号化されません。オブジェクトのメタデータやその他の機密データは暗号化されません。

暗号化オプション	仕組み	適用対象
S3バケットの暗号化	バケットの暗号化を有効にするには、PutBucketEncryption リクエストを発行します。オブジェクト レベルで暗号化されていない新しいオブジェクトは、取り込み中に暗号化されます。	新しく取り込まれた S3 オブジェクト データのみ。 バケットに暗号化を指定する必要があります。既存のバケット オブジェクトは暗号化されません。オブジェクトのメタデータやその他の機密データは暗号化されません。 "バケットの操作"
S3 オブジェクトのサーバー側暗号化 (SSE)	オブジェクトを保存するためにS3 リクエストを発行し、 `x-amz-server-side-encryption`リクエスト ヘッダー。	新しく取り込まれた S3 オブジェクト データのみ。 オブジェクトに暗号化を指定する必要があります。オブジェクトのメタデータやその他の機密データは暗号化されません。 StorageGRID がキーを管理します。 "サーバー側の暗号化を使用する"
顧客提供キーを使用した S3 オブジェクトのサーバー側暗号化 (SSE-C)	オブジェクトを保存するための S3 リクエストを発行し、3 つのリクエスト ヘッダーを含めます。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	新しく取り込まれた S3 オブジェクト データのみ。 オブジェクトに暗号化を指定する必要があります。オブジェクトのメタデータやその他の機密データは暗号化されません。 キーはStorageGRIDの外部で管理されます。 "サーバー側の暗号化を使用する"

暗号化オプション	仕組み	適用対象
外部ボリュームまたはデータストアの暗号化	導入プラットフォームでサポートされている場合は、 StorageGRID外部の暗号化方法を使用してボリューム全体またはデータストアを暗号化します。	すべてのボリュームまたはデータストアが暗号化されていると仮定した場合、すべてのオブジェクトデータ、メタデータ、およびシステム構成データ。 外部暗号化方式により、暗号化アルゴリズムとキーをより厳密に制御できます。記載されている他の方法と組み合わせることができます。
StorageGRID外部のオブジェクト暗号化	オブジェクト データとメタデータをStorageGRIDに取り込む前に暗号化するには、 StorageGRID外部の暗号化方式を使用します。	オブジェクト データとメタデータのみ (システム構成データは暗号化されません)。 外部暗号化方式により、暗号化アルゴリズムとキーをより厳密に制御できます。記載されている他の方法と組み合わせることができます。 "Amazon Simple Storage Service - ユーザーガイド: クライアント側暗号化を使用したデータの保護"

複数の暗号化方式を使用する

要件に応じて、一度に複数の暗号化方法を使用できます。例えば：

- KMS を使用してアプライアンス ノードを保護し、 SANtricity System Manager のドライブ セキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMS を使用してアプライアンス ノード上のデータを保護し、保存されたオブジェクトの暗号化オプションを使用して、取り込まれたすべてのオブジェクトを暗号化することもできます。

オブジェクトのごく一部にのみ暗号化が必要な場合は、代わりにバケットまたは個々のオブジェクト レベルで暗号化を制御することを検討してください。複数レベルの暗号化を有効にすると、パフォーマンスコストが追加されます。

証明書の管理

セキュリティ証明書を管理する

セキュリティ証明書は、 StorageGRIDコンポーネント間およびStorageGRIDコンポーネントと外部システム間の安全で信頼できる接続を作成するために使用される小さなデータ ファイルです。

StorageGRID は2 種類のセキュリティ証明書を使用します。

- HTTPS 接続を使用する場合は、サーバー証明書 が必要です。サーバー証明書は、クライアントとサーバー間の安全な接続を確立し、クライアントに対してサーバーの ID を認証し、データの安全な通信パスを提供するために使用されます。サーバーとクライアントはそれぞれ証明書のコピーを持ちます。
- クライアント証明書 は、クライアントまたはユーザーの ID をサーバーに対して認証し、パスワードのみを使用する場合よりも安全な認証を提供します。クライアント証明書はデータを暗号化しません。

クライアントが HTTPS を使用してサーバーに接続すると、サーバーは公開キーを含むサーバー証明書で応答します。クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、クライアントは同じ公開鍵を使用してサーバーとのセッションを開始します。

StorageGRID は、一部の接続 (ロード バランサ エンドポイントなど) のサーバーとして機能し、他の接続 (CloudMirror レプリケーション サービスなど) のクライアントとして機能します。

デフォルトのグリッド**CA**証明書

StorageGRID には、システムのインストール中に内部グリッド CA 証明書を生成する組み込みの証明機関 (CA) が含まれています。デフォルトでは、グリッド CA 証明書が、内部StorageGRIDトラフィックのセキュリティ保護に使用されます。外部証明機関 (CA) は、組織の情報セキュリティ ポリシーに完全に準拠したカスタム証明書を発行できます。グリッド CA 証明書は非実稼働環境でも使用できますが、実稼働環境では、外部証明機関によって署名されたカスタム証明書を使用するのがベスト プラクティスです。証明書のない安全でない接続もサポートされていますが、推奨されません。

- カスタム CA 証明書では内部証明書は削除されませんが、カスタム証明書はサーバー接続の検証用に指定する必要があります。
- すべてのカスタム証明書は、"サーバー証明書のシステム強化ガイドライン" 。
- StorageGRID は、CA からの証明書を 1 つのファイルにバンドルすること (CA 証明書バンドルと呼ばれる) をサポートしています。

> StorageGRID には、すべてのグリッドで同じオペレーティング システム CA 証明書も含まれています。運用環境では、オペレーティング システムの CA 証明書の代わりに、外部証明機関によって署名されたカスタム証明書を指定してください。

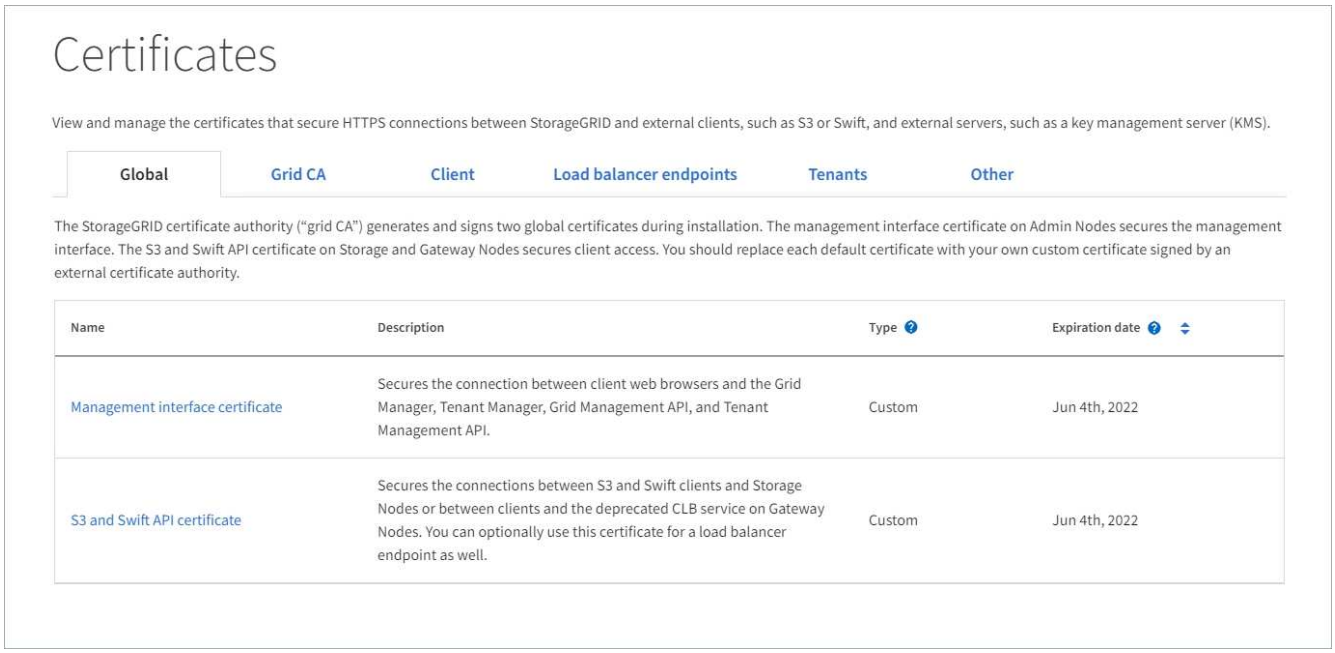
サーバー証明書とクライアント証明書の種類のバリエーションは、いくつかの方法で実装されます。システムを構成する前に、特定のStorageGRID構成に必要なすべての証明書を準備しておく必要があります。

セキュリティ証明書にアクセスする

すべてのStorageGRID証明書に関する情報と、各証明書の構成ワークフローへのリンクに 1 か所でアクセスできます。

手順

1. Grid Manager から、構成 > セキュリティ > 証明書 を選択します。



2. 各証明書カテゴリに関する情報や証明書設定にアクセスするには、「証明書」ページのタブを選択します。タブにアクセスするには、"適切な許可" 。

   - グローバル: Web ブラウザおよび外部 API クライアントからのStorageGRIDアクセスを保護します。
   - グリッド **CA**: 内部StorageGRIDトラフィックを保護します。
   - クライアント: 外部クライアントとStorageGRID Prometheus データベース間の接続を保護します。
   - ロード バランサ エンドポイント: S3 クライアントとStorageGRIDロード バランサ間の接続を保護します。
   - テナント: ID フェデレーション サーバーへの接続、またはプラットフォーム サービス エンドポイントから S3 ストレージ リソースへの接続を保護します。
   - その他: 特定の証明書を必要とするStorageGRID接続を保護します。

   各タブについては、追加の証明書の詳細へのリンクとともに以下で説明します。

グローバル

グローバル証明書は、Web ブラウザおよび外部 S3 API クライアントからのStorageGRIDアクセスを保護します。インストール中に、 StorageGRID証明機関によって最初に 2 つのグローバル証明書が生成されます。実稼働環境でのベストプラクティスは、外部証明機関によって署名されたカスタム証明書を使用することです。

- [管理インターフェース証明書]: StorageGRID管理インターフェイスへのクライアント Web ブラウザ接続を保護します。
- S3 API証明書: S3 クライアント アプリケーションがオブジェクト データのアップロードとダウンロードに使用するストレージ ノード、管理ノード、ゲートウェイ ノードへのクライアント API 接続を保護します。

インストールされているグローバル証明書に関する情報は次のとおりです。

- 名前: 証明書を管理するためのリンクを含む証明書の名前。
- 説明
- タイプ: カスタムまたはデフォルト。 + グリッドのセキュリティを強化するには、常にカスタム証明書を使用する必要があります。
- 有効期限: デフォルトの証明書を使用している場合、有効期限は表示されません。

次の操作を実行できます。

- グリッドのセキュリティを強化するために、デフォルトの証明書を外部証明機関によって署名されたカスタム証明書に置き換えます。
  - "デフォルトのStorageGRID生成管理インターフェース証明書を置き換えます"Grid Manager および Tenant Manager の接続に使用されます。
  - "S3 API証明書を置き換える"ストレージ ノードとロード バランサ エンドポイント (オプション) の接続に使用されます。
- "デフォルトの管理インターフェース証明書を復元する" 。
- "デフォルトのS3 API証明書を復元する" 。
- "スクリプトを使用して新しい自己署名管理インターフェース証明書を生成する" 。
- コピーまたはダウンロード"管理インターフェース証明書"または"S3 API証明書"。

グリッド**CA**

そのグリッド CA 証明書は、 StorageGRID のインストール中にStorageGRID証明機関によって生成され、すべての内部StorageGRIDトラフィックを保護します。

証明書情報には、証明書の有効期限と証明書の内容が含まれます。

あなたはできる"グリッドCA証明書をコピーまたはダウンロードする"ただし、変更することはできません。

クライアント

クライアント証明書外部証明機関によって生成された証明書は、外部監視ツールとStorageGRID Prometheus データベース間の接続を保護します。

証明書テーブルには、構成されたクライアント証明書ごとに行があり、証明書の有効期限とともに、証明書が Prometheus データベース アクセスに使用できるかどうかが示されます。

次の操作を実行できます。

- "新しいクライアント証明書をアップロードまたは生成します。"
- 証明書名を選択すると、証明書の詳細が表示され、次の操作を実行できます。
  - "クライアント証明書の名前を変更します。"
  - "Prometheus のアクセス権限を設定します。"
  - "クライアント証明書をアップロードして置き換えます。"
  - "クライアント証明書をコピーまたはダウンロードします。"
  - "クライアント証明書を削除します。"
- アクション*を選択してすぐに"編集"、"添付する" 、 または"削除"クライアント証明書。 *アクション > 削除 を使用して、最大 10 個のクライアント証明書を選択して一度に削除できます。

ロード バランサ エンドポイント

ロードバランサのエンドポイント証明書ゲートウェイ ノードおよび管理ノード上の S3 クライアントとStorageGRIDロード バランサ サービス間の接続を保護します。

ロード バランサー エンドポイント テーブルには、構成されたロード バランサー エンドポイントごとに 1 行あり、エンドポイントにグローバル S3 API 証明書が使用されているか、カスタム ロード バランサー エンドポイント証明書が使用されているかを示します。各証明書の有効期限も表示されます。

> エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

次の操作を実行できます。

- "ロードバランサのエンドポイントを表示する"（証明書の詳細を含む）
- "FabricPoolのロード バランサ エンドポイント証明書を指定します。"
- "グローバルS3 API証明書を使用する"新しいロードバランサのエンドポイント証明書を生成する代わりに。

テナント

テナントはIDフェデレーションサーバー証明書またはプラットフォームサービスエンドポイント証明書StorageGRIDとの接続を保護します。

テナント テーブルにはテナントごとに 1 行あり、各テナントに独自の ID ソースまたはプラットフォーム サービスを使用する権限があるかどうかを示します。

次の操作を実行できます。

- "テナント名を選択してテナント マネージャーにサインインします"
- "テナントIDフェデレーションの詳細を表示するには、テナント名を選択してください"
- "テナント名を選択して、テナント プラットフォーム サービスの詳細を表示します。"

- "エンドポイントの作成時にプラットフォーム サービス エンドポイント証明書を指定します"

その他

StorageGRID は特定の目的のために他のセキュリティ証明書を使用します。これらの証明書は機能名別にリストされています。その他のセキュリティ証明書には次のものがあります:

- クラウド ストレージ プールの証明書
- 電子メールアラート通知証明書
- 外部 syslog サーバー証明書
- グリッドフェデレーション接続証明書
- アイデンティティフェデレーション証明書
- キー管理サーバー（KMS）証明書
- シングルサインオン証明書

情報は、関数が使用する証明書の種類と、該当する場合はサーバーおよびクライアント証明書の有効期限を示します。関数名を選択するとブラウザタブが開き、証明書の詳細を表示および編集できます。

他の証明書の情報を閲覧したりアクセスしたりするには、"適切な許可" 。

次の操作を実行できます。

- "S3、C2S S3、またはAzureのクラウドストレージプール証明書を指定します"
- "アラートメール通知用の証明書を指定する"
- "外部Syslogサーバーの証明書を使用する"
- "グリッドフェデレーション接続証明書のローテーション"
- "ID フェデレーション証明書の表示と編集"
- "キー管理サーバー（KMS）のサーバー証明書とクライアント証明書をアップロードする"
- "証明書利用者信頼の SSO 証明書を手動で指定する"

セキュリティ証明書の詳細

各タイプのセキュリティ証明書については、実装手順へのリンクとともに以下で説明します。

管理インターフェース証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	クライアント Web ブラウザとStorageGRID管理インターフェイス間の接続を認証し、ユーザーがセキュリティ警告なしで Grid Manager および Tenant Manager にアクセスできるようにします。 この証明書は、グリッド管理 API およびテナント管理 API 接続も認証します。 インストール中に作成されたデフォルトの証明書を使用することも、カスタム証明書をアップロードすることもできます。	構成 > セキュリティ > *証明書*で、*グローバル*タブを選択し、*管理インターフェース証明書*を選択します。	"管理インターフェース証明書を構成する"

S3 API証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	ストレージ ノードおよびロード バランサ エンドポイントへの安全な S3 クライアント接続を認証します (オプション)。	構成 > セキュリティ > 証明書、*グローバル*タブを選択し、*S3 API証明書*を選択します。	"S3 API証明書を設定する"

グリッド **CA** 証明書

参照デフォルトのグリッドCA証明書の説明。

管理者クライアント証明書

証明書の種類	説明	ナビゲーション位置	詳細
クライアント	各クライアントにインストールされ、StorageGRID が外部クライアント アクセスを認証できるようになります。 • 承認された外部クライアントがStorageGRID Prometheus データベースにアクセスできるようにします。 • 外部ツールを使用してStorageGRIDを安全に監視できます。	構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。	"クライアント証明書を構成する"

ロードバランサのエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	ゲートウェイ ノードおよび管理ノード上の S3 クライアントとStorageGRIDロード バランサ サービス間の接続を認証します。ロード バランサー エンドポイントを構成するときに、ロード バランサー証明書をアップロードまたは生成できます。クライアント アプリケーションは、StorageGRIDに接続してオブジェクト データを保存および取得するときに、ロード バランサ証明書を使用します。 グローバルのカスタムバージョンを使用することもできますS3 API証明書 ロード バランサ サービスへの接続を認証するための証明書。グローバル証明書を使用してロード バランサー接続を認証する場合は、ロード バランサーのエンドポイントごとに個別の証明書をアップロードまたは生成する必要はありません。 注: ロード バランサの認証に使用される証明書は、通常のStorageGRID操作中に最もよく使用される証明書です。	構成 > ネットワーク > ロードバランサエンドポイント	• "ロードバランサのエンドポイントを構成する" • "FabricPoolのロードバランサエンドポイントを作成する"

クラウド ストレージ プールのエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDクラウド ストレージ プールから S3 Glacier や Microsoft Azure Blob ストレージなどの外部ストレージの場所への接続を認証します。クラウド プロバイダーの種類ごとに異なる証明書が必要です。	**ILM** > ストレージプール	"クラウドストレージプールを作成する"

電子メールアラート通知証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	アラート通知に使用される SMTP 電子メール サーバーとStorageGRID間の接続を認証します。 • SMTP サーバーとの通信にトランスポート層セキュリティ (TLS) が必要な場合は、電子メール サーバーの CA 証明書を指定する必要があります。 • SMTP 電子メール サーバーが認証にクライアント証明書を必要とする場合にのみ、クライアント証明書を指定します。	アラート > メール設定	"アラートのメール通知を設定する"

外部 **syslog** サーバー証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDにイベントを記録する外部 syslog サーバー間の TLS または RELP/TLS 接続を認証します。 注: 外部 syslog サーバへの TCP、RELP/TCP、および UDP 接続には、外部 syslog サーバ証明書は必要ありません。	構成 > 監視 > 監査および**Syslog**サーバー	"外部のSyslogサーバーを使用する"

グリッドフェデレーション接続証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	現在のStorageGRIDシステムとグリッド フェデレーション接続内の別のグリッド間で送信される情報を認証および暗号化します。	構成 > システム > グリッドフェデレーション	• "グリッドフェデレーション接続を作成する" • "接続証明書をローテーションする"

アイデンティティフェデレーション証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDと Active Directory、OpenLDAP、Oracle Directory Server などの外部 ID プロバイダー間の接続を認証します。管理者グループとユーザーを外部システムで管理できるようにする ID フェデレーションに使用されます。	構成 > アクセス制御 > アイデンティティ連携	"アイデンティティフェデレーションを使用する"

キー管理サーバー（**KMS**）証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	StorageGRIDと、StorageGRIDアプライアンス ノードに暗号化キーを提供する外部キー管理サーバー (KMS) 間の接続を認証します。	構成 > セキュリティ > キー管理サーバー	"キー管理サーバー（KMS）を追加する"

プラットフォーム サービス エンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDプラットフォーム サービスから S3 ストレージ リソースへの接続を認証します。	テナント マネージャー > ストレージ **(S3)** > プラットフォーム サービス エンドポイント	"プラットフォーム サービス エンドポイントを作成する" "プラットフォーム サービス エンドポイントを編集する"

シングルサインオン（**SSO**）証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	Active Directory フェデレーション サービス (AD FS) などの ID フェデレーション サービスと、シングル サインオン (SSO) 要求に使用されるStorageGRID間の接続を認証します。	設定 > アクセス制御 > シングルサインオン	"シングルサインオンを構成する"

証明書の例

例**1:** ロードバランササービス

この例では、 StorageGRID がサーバーとして機能します。

1. ロード バランサのエンドポイントを構成し、 StorageGRIDでサーバー証明書をアップロードまたは生成します。
2. ロードバランサーエンドポイントへの S3 クライアント接続を構成し、同じ証明書をクライアントにアップロードします。
3. クライアントがデータを保存または取得する場合、HTTPS を使用してロード バランサー エンドポイントに接続します。
4. StorageGRID は、公開キーを含むサーバー証明書と、秘密キーに基づく署名で応答します。
5. クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントはオブジェクト データをStorageGRIDに送信します。

例**2:** 外部キー管理サーバー **(KMS)**

この例では、 StorageGRID がクライアントとして機能します。

1. 外部のキー管理サーバ ソフトウェアを使用して、 StorageGRID をKMS クライアントとして構成し、CA 署名付きサーバ証明書、公開クライアント証明書、およびクライアント証明書の秘密キーを取得します。
2. Grid Manager を使用して、KMS サーバーを構成し、サーバー証明書とクライアント証明書およびクライアント秘密キーをアップロードします。
3. StorageGRIDノードは暗号化キーを必要とする場合、証明書のデータと秘密キーに基づく署名を含む要求を KMS サーバーに送信します。
4. KMS サーバーは証明書の署名を検証し、 StorageGRID を信頼できると判断します。
5. KMS サーバーは検証された接続を使用して応答します。

サポートされているサーバー証明書の種類

StorageGRIDシステムは、RSA または ECDSA (楕円曲線デジタル署名アルゴリズム) で暗号化されたカスタム証明書をサポートします。

セキュリティ ポリシーの暗号タイプは、サーバー証明書タイプと一致する必要があります。たとえば、RSA 暗号には RSA 証明書が必要であり、ECDSA 暗号には ECDSA 証明書が必要です。見る"セキュリティ証明書を管理する" 。サーバー証明書と互換性のないカスタムセキュリティポリシーを構成する場合は、"一時的にデフォルトのセキュリティポリシーに戻す" 。

StorageGRIDがクライアント接続を保護する方法の詳細については、以下を参照してください。"S3 クライアントのセキュリティ" 。

管理インターフェース証明書を構成する

デフォルトの管理インターフェイス証明書を単一のカスタム証明書に置き換えて、ユーザーがセキュリティ警告に遭遇することなく Grid Manager および Tenant Manager にアクセスできるようにすることができます。デフォルトの管理インターフェイス証明書に戻したり、新しい証明書を生成したりすることもできます。

タスク概要

デフォルトでは、すべての管理ノードにグリッド CA によって署名された証明書が発行されます。これらの CA 署名付き証明書は、単一の共通カスタム管理インターフェイス証明書と対応する秘密キーに置き換えることができます。

すべての管理ノードに単一のカスタム管理インターフェイス証明書が使用されるため、クライアントが Grid Manager および Tenant Manager に接続するときにホスト名を検証する必要がある場合は、証明書をワイルドカードまたはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードと一致するようにカスタム証明書を定義します。

サーバー上で構成を完了する必要があります。また、使用しているルート証明機関 (CA) によっては、ユーザーが Grid Manager および Tenant Manager にアクセスするために使用する Web ブラウザーに Grid CA 証明書をインストールする必要もあります。

失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、管理インターフェイスのサーバー証明書の有効期限*アラートがトリガーされます。必要に応じて、**[*CONFIGURATION]** > [**Security**] > [**Certificates**] を選択し、[Global] タブで管理インターフェイス証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスしている場合、次のいずれかが発生すると、ブラウザにバイパス オプションのない証明書エラーが表示されます。

- カスタム管理インターフェース証明書の有効期限が切れます。
- あなたカスタム管理インターフェース証明書からデフォルトのサーバー証明書に戻す。

カスタム管理インターフェース証明書を追加する

カスタム管理インターフェイス証明書を追加するには、独自の証明書を提供するか、グリッド マネージャーを使用して証明書を生成します。

手順

1. 構成 > セキュリティ > *証明書*を選択します。

2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *カスタム証明書を使用する*を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードします。

a. *証明書のアップロード*を選択します。

b. 必要なサーバー証明書ファイルをアップロードします。

- サーバー証明書: カスタム サーバー証明書ファイル (PEM エンコード)。
- 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(`.key`）。

> EC 秘密鍵は 224 ビット以上である必要があります。 RSA 秘密鍵は 2048 ビット以上である必要があります。

- **CA** バンドル: 各中間発行証明機関 (CA) からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。

c. *証明書の詳細*を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。

- 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA** バンドルのダウンロード を選択します。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」または「**CA** バンドル **PEM** のコピー」を選択します。

d. *保存*を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、または Tenant Manager API への以降のすべての新しい接続に使用されます。

証明書を生成する

サーバー証明書ファイルを生成します。

> 実稼働環境でのベスト プラクティスは、外部証明機関によって署名されたカスタム管理インターフェイス証明書を使用することです。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める 1 つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。

フィールド	説明
IP	証明書に含める 1 つ以上の IP アドレス。
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名 (DN)。 このフィールドに値が入力されない場合、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

d. 生成された証明書のメタデータを表示するには、「証明書の詳細」を選択します。

   - 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

     証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

e. *保存*を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、または Tenant Manager API への以降のすべての新しい接続に使用されます。

5. ページを更新して、Web ブラウザが更新されていることを確認します。

> 新しい証明書をアップロードまたは生成した後、関連する証明書の有効期限アラートがクリアされるまで最大 1 日かかります。

6. カスタム管理インターフェイス証明書を追加すると、管理インターフェイス証明書ページに、使用中の証明書の詳細な証明書情報が表示されます。 + 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトの管理インターフェース証明書を復元する

Grid Manager および Tenant Manager 接続にデフォルトの管理インターフェイス証明書を使用するように戻すことができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *デフォルトの証明書を使用する*を選択します。

   デフォルトの管理インターフェイス証明書を復元すると、構成したカスタム サーバー証明書ファイルが削除され、システムから回復できなくなります。以降のすべての新しいクライアント接続には、デフォルトの管理インターフェイス証明書が使用されます。

4. ページを更新して、Web ブラウザが更新されていることを確認します。

スクリプトを使用して新しい自己署名管理インターフェース証明書を生成する

厳密なホスト名検証が必要な場合は、スクリプトを使用して管理インターフェイス証明書を生成できます。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。

タスク概要

実稼働環境でのベストプラクティスは、外部の証明機関によって署名された証明書を使用することです。

手順

1. 各管理ノードの完全修飾ドメイン名 (FQDN) を取得します。
2. プライマリ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@primary_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 `#`。
3. 新しい自己署名証明書を使用してStorageGRIDを構成します。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - のために `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例えば、 `*.ui.storagegrid.example.com` *ワイルドカードを使用して `admin1.ui.storagegrid.example.com`そして `admin2.ui.storagegrid.example.com`。
   - セット `--type`に `management`Grid Manager および Tenant Manager で使用される管理インターフェイス証明書を構成します。

◦ デフォルトでは、生成された証明書の有効期間は 1 年間 (365 日間) で、有効期限が切れる前に再作成する必要があります。使用することができます `--days`デフォルトの有効期間を上書きする引数。

> ⓘ 証明書の有効期間は、 `make-certificate`実行されます。管理クライアントがStorageGRIDと同じタイム ソースに同期されていることを確認する必要があります。そうでない場合、クライアントは証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

結果の出力には、管理 API クライアントに必要な公開証明書が含まれます。

4. 証明書を選択してコピーします。

   選択範囲に BEGIN タグと END タグを含めます。

5. コマンド シェルからログアウトします。 `$ exit`
6. 証明書が構成されたことを確認します。
   a. グリッド マネージャーにアクセスします。
   b. 構成 > セキュリティ > *証明書*を選択します。
   c. *グローバル*タブで、*管理インターフェース証明書*を選択します。
7. コピーした公開証明書を使用するように管理クライアントを構成します。 BEGIN タグと END タグを含めます。

管理インターフェース証明書をダウンロードまたはコピーします

管理インターフェイスの証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *サーバー*または*CAバンドル*タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは**CA**バンドルをダウンロードする

証明書またはCAバンドルをダウンロードする `.pem`ファイル。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. *証明書のダウンロード*または*CAバンドルのダウンロード*を選択します。

   CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つのファイルとしてダウンロードされます。

b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー を選択します。

   CA バンドルをコピーする場合、CA バンドルのセカンダリ タブ内のすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキスト エディターに貼り付けます。

c. 拡張子をつけてテキストファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

S3 API証明書を設定する

ストレージ ノードまたはロード バランサー エンドポイントへの S3 クライアント接続に使用されるサーバー証明書を置き換えたり復元したりできます。交換用のカスタム サーバー証明書は、組織に固有のものです。

このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る "StorageGRID 11.8: S3およびSwift API証明書の設定"。

タスク概要

デフォルトでは、すべてのストレージ ノードにグリッド CA によって署名された X.509 サーバー証明書が発行されます。これらの CA 署名付き証明書は、単一の共通カスタム サーバー証明書と対応する秘密キーに置き換えることができます。

すべてのストレージ ノードに単一のカスタム サーバー証明書が使用されるため、クライアントがストレージ エンドポイントに接続するときにホスト名を検証する必要がある場合は、証明書をワイルドカードまたはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージ ノードに一致するようにカスタム証明書を定義します。

サーバーでの設定が完了したら、使用しているルート証明機関 (CA) に応じて、システムにアクセスするために使用する S3 API クライアントに Grid CA 証明書をインストールする必要もあります。

> 失敗したサーバー証明書によって操作が中断されないように、ルート サーバー証明書の有効期限が切れそうになると、**S3 API** のグローバル サーバー証明書の有効期限切れ アラートがトリガーされます。必要に応じて、[設定] > [セキュリティ] > [証明書] を選択し、[グローバル] タブで S3 API 証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

カスタム S3 API 証明書をアップロードまたは生成できます。

カスタム**S3 API**証明書を追加する

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *カスタム証明書を使用する*を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードします。

a. *証明書のアップロード*を選択します。

b. 必要なサーバー証明書ファイルをアップロードします。

   - サーバー証明書: カスタム サーバー証明書ファイル (PEM エンコード)。
   - 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(`.key`）。

   > EC 秘密鍵は 224 ビット以上である必要があります。 RSA 秘密鍵は 2048 ビット以上である必要があります。

   - **CA** バンドル: 各中間発行証明機関からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。

c. 証明書の詳細を選択すると、アップロードされた各カスタム S3 API 証明書のメタデータと PEM が表示されます。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。

   - 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA** バンドルのダウンロード を選択します。

     証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」または「**CA** バンドル **PEM** のコピー」を選択します。

d. *保存*を選択します。

   カスタム サーバー証明書は、後続の新しい S3 クライアント接続に使用されます。

証明書を生成する

サーバー証明書ファイルを生成します。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める 1 つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める 1 つ以上の IP アドレス。

フィールド	説明
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名 (DN)。 このフィールドに値が入力されない場合、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

d. 証明書の詳細 を選択すると、生成されたカスタム S3 API 証明書のメタデータと PEM が表示されます。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

e. *保存*を選択します。

カスタム サーバー証明書は、後続の新しい S3 クライアント接続に使用されます。

5. タブを選択すると、デフォルトのStorageGRIDサーバー証明書、アップロードされた CA 署名付き証明書、または生成されたカスタム証明書のメタデータが表示されます。

> ⓘ 新しい証明書をアップロードまたは生成した後、関連する証明書の有効期限アラートがクリアされるまで最大 1 日かかります。

6. ページを更新して、Web ブラウザが更新されていることを確認します。

7. カスタム S3 API 証明書を追加すると、S3 API 証明書ページに、使用中のカスタム S3 API 証明書の詳細な証明書情報が表示されます。 + 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトの**S3 API**証明書を復元する

ストレージノードへの S3 クライアント接続にデフォルトの S3 API 証明書を使用するように戻すことができます。ただし、ロードバランサーエンドポイントにはデフォルトの S3 API 証明書は使用できません。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *デフォルトの証明書を使用する*を選択します。

   グローバル S3 API 証明書のデフォルト バージョンを復元すると、設定したカスタム サーバー証明書ファイルが削除され、システムから復元できなくなります。デフォルトの S3 API 証明書は、ストレージ ノードへの後続の新しい S3 クライアント接続に使用されます。

4. **OK** を選択して警告を確認し、デフォルトの S3 API 証明書を復元します。

   ルートアクセス権限があり、カスタム S3 API 証明書がロードバランサーのエンドポイント接続に使用されていた場合、デフォルトの S3 API 証明書を使用してアクセスできなくなるロードバランサーのエンドポイントのリストが表示されます。へ移動"ロードバランサのエンドポイントを構成する"影響を受けるエンドポイントを編集または削除します。

5. ページを更新して、Web ブラウザが更新されていることを確認します。

S3 API証明書をダウンロードまたはコピーします

S3 API 証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *サーバー*または*CAバンドル*タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは**CA**バンドルをダウンロードする

証明書またはCAバンドルをダウンロードする `.pem`ファイル。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. *証明書のダウンロード*または*CAバンドルのダウンロード*を選択します。

   CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つのファイルとしてダウンロードされます。

b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー を選択します。

   CA バンドルをコピーする場合、CA バンドルのセカンダリ タブ内のすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキスト エディターに貼り付けます。

c. 拡張子をつけてテキストファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

- "S3 REST APIを使用する"
- "S3エンドポイントのドメイン名を設定する"

グリッド**CA**証明書をコピーする

StorageGRID は、内部証明機関 (CA) を使用して内部トラフィックを保護します。独自の証明書をアップロードした場合、この証明書は変更されません。

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" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

カスタム サーバー証明書が構成されている場合、クライアント アプリケーションはカスタム サーバー証明書を使用してサーバーを検証する必要があります。 StorageGRIDシステムから CA 証明書をコピーしないでください。

手順

1. 構成 > セキュリティ > 証明書 を選択し、グリッド **CA** タブを選択します。
2. 証明書 **PEM** セクションで、証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `.pem`ファイル。

a. *証明書のダウンロード*を選択します。
b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

例： `storagegrid_certificate.pem`

証明書**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。

a. *証明書PEMのコピー*を選択します。
b. コピーした証明書をテキスト エディターに貼り付けます。
c. 拡張子をつけてテキストファイルを保存する `.pem`。

例： `storagegrid_certificate.pem`

FabricPoolのStorageGRID証明書を構成する

FabricPoolを使用するONTAPクライアントなど、厳密なホスト名検証を実行し、厳密なホスト名検証の無効化をサポートしていない S3 クライアントの場合は、ロードバランサのエンドポイントを設定するときにサーバ証明書を生成またはアップロードできます。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- 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" 。

タスク概要

ロード バランサー エンドポイントを作成するときに、自己署名サーバー証明書を生成するか、既知の証明機関 (CA) によって署名された証明書をアップロードすることができます。運用環境では、既知の CA によって署名された証明書を使用する必要があります。 CA によって署名された証明書は、中断することなくローテーションできます。また、中間者攻撃に対する保護が強化されるため、安全性も高まります。

次の手順は、 FabricPoolを使用する S3 クライアントの一般的なガイドラインを示しています。詳しい情報と手順については、"FabricPool用にStorageGRIDを構成する" 。

手順

1. 必要に応じて、 FabricPoolが使用する高可用性 (HA) グループを構成します。
2. FabricPoolが使用する S3 ロード バランサ エンドポイントを作成します。

   HTTPS ロード バランサ エンドポイントを作成すると、サーバー証明書、証明書の秘密キー、およびオプションの CA バンドルをアップロードするように求められます。

3. StorageGRID をONTAPのクラウド層として接続します。

   アップロードした CA 証明書で使用されるロード バランサーのエンドポイント ポートと完全修飾ドメイン名を指定します。次に、CA 証明書を提供します。

   中間 CA がStorageGRID証明書を発行した場合は、中間 CA 証明書を提供する必要があります。 StorageGRID証明書がルート CA によって直接発行された場合は、ルート CA 証明書を提供する必要があります。

クライアント証明書を構成する

クライアント証明書により、承認された外部クライアントがStorageGRID Prometheusデータベースにアクセスできるようになり、外部ツールがStorageGRID を安全に監視できるようになります。

外部監視ツールを使用してStorageGRIDにアクセスする必要がある場合は、Grid Manager を使用してクライアント証明書をアップロードまたは生成し、証明書情報を外部ツールにコピーする必要があります。

見る"セキュリティ証明書を管理する"そして"カスタムサーバー証明書を構成する"。

失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、*証明書ページで構成されたクライアント証明書の有効期限*アラートがトリガーされます。必要に応じて、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブでクライアント証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

特別に構成されたアプライアンスノード上のデータを保護するためにキー管理サーバー（KMS）を使用している場合は、"KMSクライアント証明書のアップロード" 。

開始する前に

- ルートアクセス権限があります。
- 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" 。
- クライアント証明書を構成するには:
  - 管理ノードの IP アドレスまたはドメイン名があります。
  - StorageGRID管理インターフェイス証明書を設定している場合は、管理インターフェイス証明書を設定するために使用した CA、クライアント証明書、および秘密キーがあります。
  - 独自の証明書をアップロードするには、証明書の秘密キーがローカル コンピューター上で利用可能である必要があります。
  - 秘密鍵は作成時に保存または記録されている必要があります。元の秘密鍵がない場合は、新しい秘密鍵を作成する必要があります。

- クライアント証明書を編集するには:
  - 管理ノードの IP アドレスまたはドメイン名があります。
  - 独自の証明書または新しい証明書をアップロードするには、秘密キー、クライアント証明書、および CA (使用されている場合) がローカル コンピューター上で使用可能です。

クライアント証明書を追加する

クライアント証明書を追加するには、次のいずれかの手順を使用します。

- [管理インターフェース証明書はすでに構成されています]
- CA発行のクライアント証明書
- [グリッドマネージャーから生成された証明書]

管理インターフェース証明書はすでに構成されています

顧客提供の CA、クライアント証明書、および秘密キーを使用して管理インターフェイス証明書がすでに構成されている場合は、この手順を使用してクライアント証明書を追加します。

手順

1. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. *追加*を選択します。
3. 証明書名を入力します。
4. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
5. *続行*を選択します。
6. *証明書の添付*手順では、管理インターフェース証明書をアップロードします。
   a. *証明書のアップロード*を選択します。
   b. *参照*を選択し、管理インターフェース証明書ファイルを選択します。(`.pem`）。
      - 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
   c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

      新しい証明書が [クライアント] タブに表示されます。
7. 外部監視ツールを構成するGrafana など。

CA発行のクライアント証明書

管理インターフェース証明書が設定されておらず、CA 発行のクライアント証明書と秘密キーを使用する Prometheus のクライアント証明書を追加する予定の場合は、この手順を使用して管理者クライアント証明書を追加します。

手順

1. 以下の手順を実行します"管理インターフェース証明書を構成する"。

2. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
3. *追加*を選択します。
4. 証明書名を入力します。
5. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
6. *続行*を選択します。
7. *証明書の添付*手順では、クライアント証明書、秘密キー、および CA バンドル ファイルをアップロードします。
   a. *証明書のアップロード*を選択します。
   b. *参照*を選択し、クライアント証明書、秘密鍵、CAバンドルファイルを選択します。(`.pem`）。
      - 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
   c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

      新しい証明書が [クライアント] タブに表示されます。
8. 外部監視ツールを構成するGrafana など。

グリッドマネージャーから生成された証明書

管理インターフェース証明書が構成されておらず、Grid Manager の証明書生成機能を使用する Prometheus のクライアント証明書を追加する予定の場合は、この手順を使用して管理者クライアント証明書を追加します。

手順

1. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. *追加*を選択します。
3. 証明書名を入力します。
4. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
5. *続行*を選択します。
6. *証明書の添付*手順では、*証明書の生成*を選択します。
7. 証明書情報を指定します。
   - **Subject** (オプション): 証明書所有者の X.509 サブジェクトまたは識別名 (DN)。
   - 有効日数: 生成された証明書が有効な日数 (生成された時点から計算)。
   - キー使用拡張機能の追加: 選択した場合 (デフォルト、推奨)、生成された証明書にキー使用拡張機能と拡張キー使用拡張機能が追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

8. *生成*を選択します。
9. 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。

ダイアログを閉じると、証明書の秘密キーを表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

例： `storagegrid_certificate.pem`

- 証明書の秘密キーをコピーして他の場所に貼り付けるには、「秘密キーのコピー」を選択します。
- 秘密鍵をファイルとして保存するには、「秘密鍵のダウンロード」を選択します。

  秘密鍵ファイル名とダウンロード場所を指定します。

10. 作成 を選択して、証明書をグリッド マネージャーに保存します。

    新しい証明書が [クライアント] タブに表示されます。

11. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[グローバル] タブを選択します。
12. *管理インターフェイス証明書*を選択します。
13. *カスタム証明書を使用する*を選択します。
14. certificate.pemとprivate_key.pemファイルをアップロードします。クライアント証明書の詳細ステップ。CA バンドルをアップロードする必要はありません。
    a. *証明書のアップロード*を選択し、*続行*を選択します。
    b. 各証明書ファイルをアップロードする(`.pem`）。
    c. 保存 を選択して、証明書をグリッド マネージャーに保存します。

       新しい証明書が管理インターフェイスの証明書ページに表示されます。

15. 外部監視ツールを構成するGrafana など。

外部監視ツールを設定する

手順

1. Grafana などの外部監視ツールで次の設定を構成します。
   a. 名前: 接続の名前を入力します。

      StorageGRIDこの情報は必要ありませんが、接続をテストするには名前を指定する必要があります。

b. **URL**: 管理ノードのドメイン名または IP アドレスを入力します。 HTTPS とポート 9091 を指定します。

   例： `https://admin-node.example.com:9091`

c. **TLS** クライアント認証 と **CA** 証明書 を有効にします。

d. TLS/SSL認証の詳細の下に、以下の内容をコピーして貼り付けます:

   - 管理インターフェース CA 証明書を **CA Cert** へ
   - **Client Cert** へのクライアント証明書
   - クライアントキーの秘密鍵

e. **ServerName**: 管理ノードのドメイン名を入力します。

   ServerName は、管理インターフェイス証明書に表示されるドメイン名と一致する必要があります。

2. StorageGRIDまたはローカル ファイルからコピーした証明書と秘密キーを保存してテストします。

   外部監視ツールを使用して、 StorageGRIDから Prometheus メトリックにアクセスできるようになりました。

   指標の詳細については、"StorageGRIDの監視手順" 。

クライアント証明書を編集する

管理者クライアント証明書を編集して名前を変更したり、Prometheus アクセスを有効または無効にしたり、現在の証明書の有効期限が切れたときに新しい証明書をアップロードしたりできます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

   証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すでに切れている場合は、テーブルにメッセージが表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. *編集*を選択し、*名前と権限の編集*を選択します。
4. 証明書名を入力します。
5. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
6. *続行*を選択して、グリッド マネージャーに証明書を保存します。

   更新された証明書が [クライアント] タブに表示されます。

新しいクライアント証明書を添付する

現在の証明書の有効期限が切れた場合は、新しい証明書をアップロードできます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

   証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すでに切れている場合は、テーブルにメッセージが表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. *編集*を選択し、編集オプションを選択します。

証明書をアップロード

証明書のテキストをコピーして他の場所に貼り付けます。

a. *証明書のアップロード*を選択し、*続行*を選択します。

b. クライアント証明書名をアップロードする(`.pem`）。

   証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。

   - 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

     証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

   更新された証明書が [クライアント] タブに表示されます。

証明書を生成する

他の場所に貼り付けるための証明書テキストを生成します。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

   - **Subject** (オプション): 証明書所有者の X.509 サブジェクトまたは識別名 (DN)。
   - 有効日数: 生成された証明書が有効な日数 (生成された時点から計算)。
   - キー使用拡張機能の追加: 選択した場合 (デフォルト、推奨)、生成された証明書にキー使用拡張機能と拡張キー使用拡張機能が追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

     証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

d. 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。

   ダイアログを閉じると、証明書の秘密キーを表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

   - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

  証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の秘密キーをコピーして他の場所に貼り付けるには、「秘密キーのコピー」を選択します。
- 秘密鍵をファイルとして保存するには、「秘密鍵のダウンロード」を選択します。

  秘密鍵ファイル名とダウンロード場所を指定します。

e. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

クライアント証明書をダウンロードまたはコピーする

他の場所で使用するためにクライアント証明書をダウンロードまたはコピーすることができます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. コピーまたはダウンロードする証明書を選択します。
3. 証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `.pem`ファイル。

a. *証明書のダウンロード*を選択します。
b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

証明書のコピー

証明書のテキストをコピーして他の場所に貼り付けます。

a. *証明書PEMのコピー*を選択します。
b. コピーした証明書をテキスト エディターに貼り付けます。
c. 拡張子をつけてテキストファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

クライアント証明書を削除する

管理者クライアント証明書が不要になった場合は、削除できます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. 削除する証明書を選択します。
3. *削除*を選択して確認します。

> 最大 10 個の証明書を削除するには、[クライアント] タブで削除する各証明書を選択し、[アクション] > [削除] を選択します。

証明書が削除された後、その証明書を使用していたクライアントは、 StorageGRID Prometheus データベースにアクセスするために新しいクライアント証明書を指定する必要があります。

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。
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。

キー管理サーバーを構成する

キー管理サーバー **(KMS)** とは何ですか**?**

キー管理サーバー (KMS) は、キー管理相互運用性プロトコル (KMIP) を使用して、関連付けられたStorageGRIDサイトのStorageGRIDアプライアンス ノードに暗号化キーを提供する外部のサードパーティ システムです。

StorageGRID は特定のキー管理サーバーのみをサポートします。サポートされている製品とバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

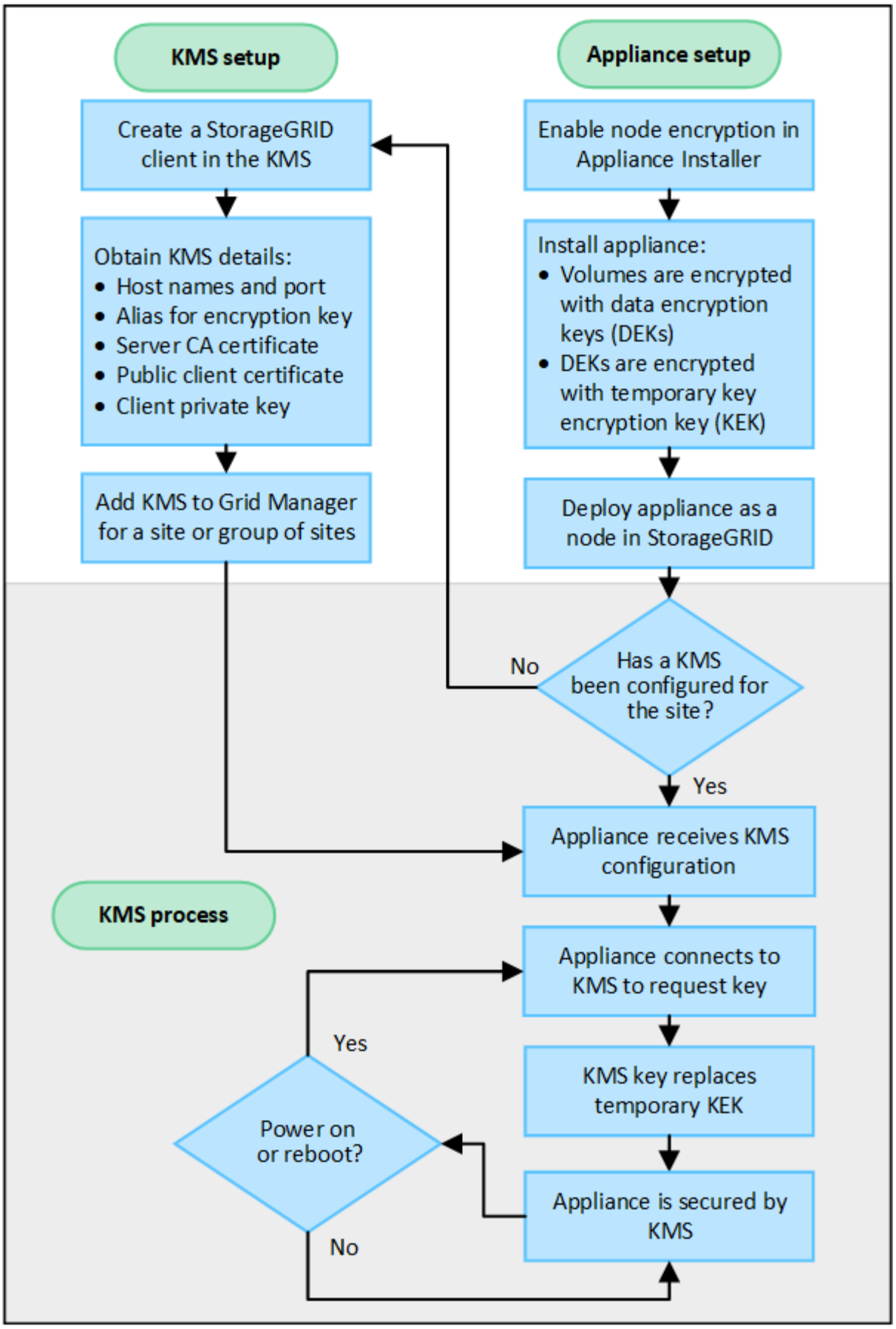
インストール中に ノード暗号化 設定が有効になっているStorageGRIDアプライアンス ノードのノード暗号化キーを管理するには、1 つ以上のキー管理サーバーを使用できます。これらのアプライアンス ノードでキー管理サーバーを使用すると、アプライアンスがデータ センターから削除された場合でもデータを保護できます。アプライアンス ボリュームが暗号化された後は、ノードが KMS と通信できない限り、アプライアンス上のデータにアクセスできなくなります。

> StorageGRID は、アプライアンス ノードの暗号化と復号化に使用される外部キーを作成または管理しません。 StorageGRIDデータを保護するために外部のキー管理サーバを使用する予定の場合は、そのサーバの設定方法と暗号化キーの管理方法を理解している必要があります。キー管理タスクの実行は、これらの手順の範囲外です。ヘルプが必要な場合は、キー管理サーバーのドキュメントを参照するか、テクニカル サポートにお問い合わせください。

KMSとアプライアンスの構成

キー管理サーバー (KMS) を使用してアプライアンス ノード上のStorageGRIDデータを保護する前に、1 つ以上の KMS サーバーを設定し、アプライアンス ノードのノード暗号化を有効にするという 2 つの構成タスクを完了する必要があります。これら 2 つの構成タスクが完了すると、キー管理プロセスが自動的に実行されます。

このフローチャートは、KMS を使用してアプライアンス ノード上のStorageGRIDデータを保護するための大まかな手順を示しています。



フローチャートでは、KMS セットアップとアプライアンス セットアップが並行して行われていることを示し

ています。ただし、要件に応じて、新しいアプライアンス ノードのノード暗号化を有効にする前または後に、キー管理サーバーをセットアップできます。

キー管理サーバー（KMS）をセットアップする

キー管理サーバーの設定には、次の大まかな手順が含まれます。

手順	参照
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスターにStorageGRIDのクライアントを追加します。	"StorageGRIDをKMSのクライアントとして設定する"
KMS 上のStorageGRIDクライアントに必要な情報を取得します。	"StorageGRIDをKMSのクライアントとして設定する"
KMS を Grid Manager に追加し、単一のサイトまたはデフォルトのサイト グループに割り当て、必要な証明書をアップロードして、KMS 構成を保存します。	"キー管理サーバー（KMS）を追加する"

アプライアンスのセットアップ

KMS を使用するためにアプライアンス ノードを設定するには、次の大まかな手順が含まれます。

1. アプライアンスのインストールのハードウェア構成段階で、 StorageGRIDアプライアンス インストーラを使用して、アプライアンスの ノード暗号化 設定を有効にします。

   > アプライアンスをグリッドに追加された後は、*ノード暗号化*設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用することはできません。

2. StorageGRIDアプライアンス インストーラを実行します。インストール中に、次のようにランダム データ暗号化キー (DEK) が各アプライアンス ボリュームに割り当てられます。
   - DEK は各ボリューム上のデータを暗号化するために使用されます。これらのキーは、アプライアンス OS の Linux Unified Key Setup (LUKS) ディスク暗号化を使用して生成され、変更できません。
   - 個々の DEK は、マスター キー暗号化キー (KEK) によって暗号化されます。初期 KEK は、アプライアンスが KMS に接続できるようになるまで DEK を暗号化する一時的なキーです。
3. アプライアンス ノードをStorageGRIDに追加します。

見る "ノード暗号化を有効にする"詳細については。

キー管理暗号化プロセス（自動的に実行）

キー管理暗号化には、自動的に実行される次の高レベルの手順が含まれます。

1. ノード暗号化が有効になっているアプライアンスをグリッドにインストールすると、 StorageGRID は新しいノードを含むサイトに KMS 構成が存在するかどうかを判断します。

- サイトに KMS がすでに構成されている場合、アプライアンスは KMS 構成を受け取ります。
- サイトに KMS がまだ構成されていない場合は、サイトに KMS が構成され、アプライアンスが KMS 構成を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化され続けます。

2. アプライアンスは KMS 構成を使用して KMS に接続し、暗号化キーを要求します。
3. KMS はアプライアンスに暗号化キーを送信します。 KMS からの新しいキーは一時的な KEK に置き換えられ、アプライアンス ボリュームの DEK の暗号化と復号化に使用されるようになりました。

> 暗号化されたアプライアンス ノードが構成された KMS に接続する前に存在するすべてのデータは、一時キーで暗号化されます。ただし、一時キーが KMS 暗号化キーに置き換えられるまで、アプライアンス ボリュームはデータ センターからの削除から保護されているとは見なされません。

4. アプライアンスの電源がオンになったり再起動したりすると、KMS に再接続してキーを要求します。揮発性メモリに保存されるキーは、電源喪失や再起動により失われます。

鍵管理サーバーの使用に関する考慮事項と要件

外部キー管理サーバー (KMS) を構成する前に、考慮事項と要件を理解しておく必要があります。

サポートされている **KMIP** のバージョンは何ですか**?**

StorageGRID はKMIP バージョン 1.4 をサポートしています。

"鍵管理相互運用性プロトコル仕様バージョン1.4"

ネットワークに関する考慮事項は何ですか**?**

ネットワーク ファイアウォール設定では、各アプライアンス ノードがキー管理相互運用性プロトコル (KMIP) 通信に使用されるポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

ノード暗号化を使用する各アプライアンス ノードが、サイト用に構成した KMS または KMS クラスターへのネットワーク アクセス権を持っていることを確認する必要があります。

どのバージョンの **TLS** がサポートされていますか**?**

アプライアンス ノードと構成された KMS 間の通信には、安全な TLS 接続が使用されます。 StorageGRID は、KMSまたはKMSクラスタへのKMIP接続を行う際に、KMSがサポートするものと、"TLSおよびSSHポリシー"使用しているもの。

StorageGRID は、接続時に KMS とプロトコルと暗号 (TLS 1.2) または暗号スイート (TLS 1.3) をネゴシエートします。利用可能なプロトコルバージョンと暗号/暗号スイートを確認するには、 `tlsOutbound`グリッドのアクティブな TLS および SSH ポリシーのセクション (*[構成] > [セキュリティ] [セキュリティ設定])。

どのアプライアンスがサポートされていますか**?**

キー管理サーバー (KMS) を使用して、グリッド内の ノード暗号化 設定が有効になっている任意のStorageGRIDアプライアンスの暗号化キーを管理できます。この設定は、 StorageGRIDアプライアンス インストーラを使用したアプライアンスのインストールのハードウェア構成段階でのみ有効にできます。

アプライアンスをグリッドに追加された後はノード暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用することはできません。

構成された KMS は、 StorageGRIDアプライアンスおよびアプライアンス ノードに使用できます。

構成された KMS は、次のようなソフトウェア ベース (アプライアンス以外) のノードには使用できません。

- 仮想マシン (VM) として展開されたノード
- Linuxホスト上のコンテナエンジン内にデプロイされたノード

これらの他のプラットフォームに展開されたノードは、データストアまたはディスク レベルでStorageGRIDの外部の暗号化を使用できます。

キー管理サーバーはいつ構成すればよいですか?

新規インストールの場合、通常、テナントを作成する前に、グリッド マネージャーで 1 つ以上のキー管理サーバーを設定する必要があります。この順序により、オブジェクト データがノードに保存される前にノードが保護されることが保証されます。

アプライアンス ノードをインストールする前または後に、グリッド マネージャーでキー管理サーバーを構成できます。

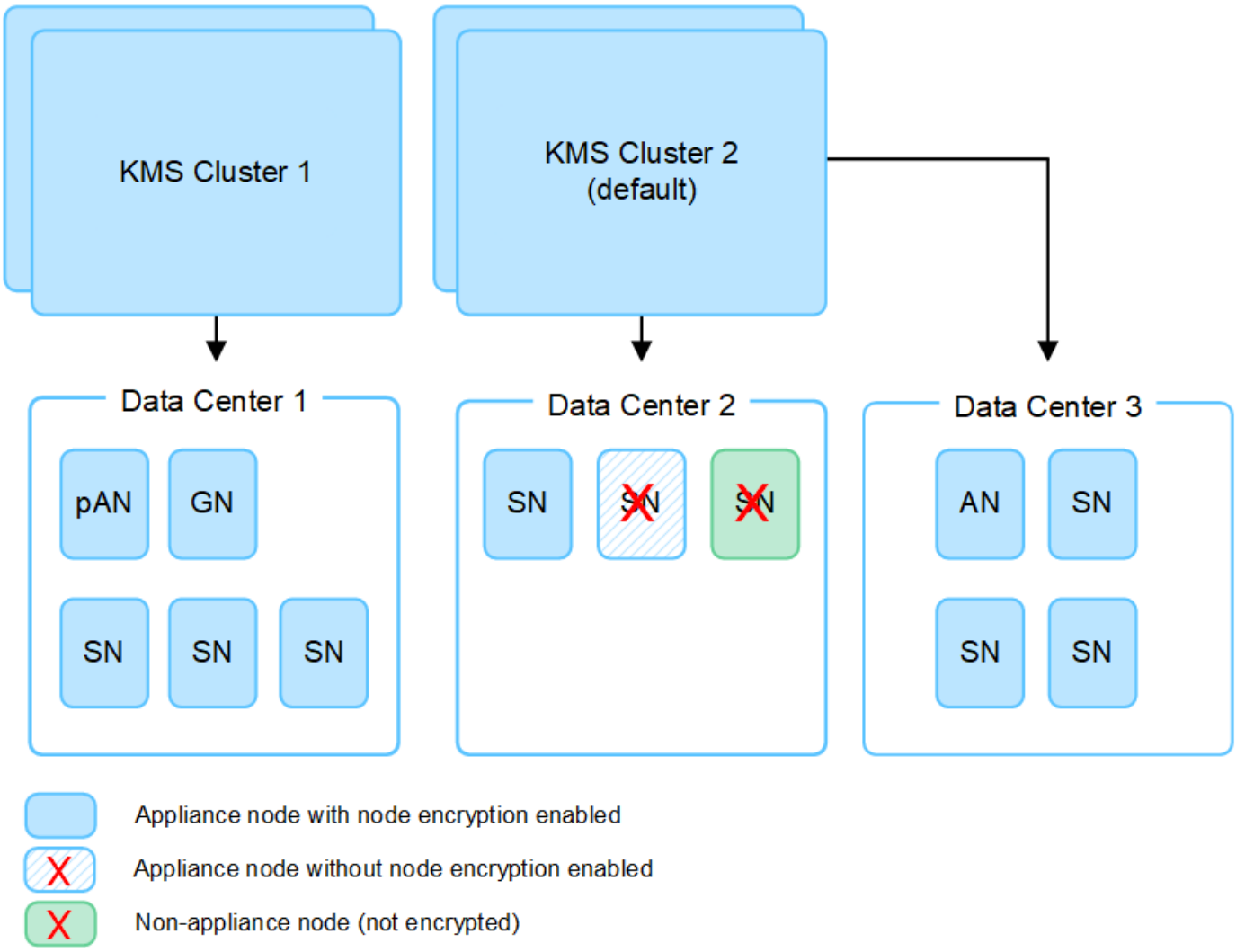
キー管理サーバーは何台必要ですか?

StorageGRIDシステム内のアプライアンス ノードに暗号化キーを提供するように、1 つ以上の外部キー管理サーバーを設定できます。各 KMS は、単一のサイトまたはサイト グループのStorageGRIDアプライアンス ノードに単一の暗号化キーを提供します。

StorageGRID はKMS クラスターの使用をサポートしています。各 KMS クラスターには、構成設定と暗号化キーを共有する複数の複製されたキー管理サーバーが含まれています。高可用性構成のフェイルオーバー機能が向上するため、キー管理に KMS クラスターを使用することをお勧めします。

たとえば、 StorageGRIDシステムに 3 つのデータ センター サイトがあるとします。 1 つの KMS クラスターを構成してデータ センター 1 のすべてのアプライアンス ノードにキーを提供し、2 つ目の KMS クラスターを構成して他のすべてのサイトのすべてのアプライアンス ノードにキーを提供するといったことが可能です。 2 番目の KMS クラスターを追加すると、データセンター 2 とデータセンター 3 のデフォルトの KMS を構成できます。

アプライアンス以外のノードや、インストール時に ノード暗号化 設定が有効になっていなかったアプライアンス ノードでは、KMS を使用できないことに注意してください。



キーをローテーションすると何が起こりますか**?**

セキュリティのベストプラクティスとして、定期的に"暗号化キーをローテーションする"構成された各 KMS によって使用されます。

新しいキー バージョンが利用可能になると、次のようになります。

- これは、KMS に関連付けられたサイトまたはサイト内の暗号化されたアプライアンス ノードに自動的に配布されます。配布は、キーがローテーションされてから 1 時間以内に行われる必要があります。
- 新しいキー バージョンが配布されたときに暗号化されたアプライアンス ノードがオフラインの場合、ノードは再起動するとすぐに新しいキーを受け取ります。
- 何らかの理由で新しいキー バージョンを使用してアプライアンス ボリュームを暗号化できない場合は、アプライアンス ノードに対して **KMS** 暗号化キーのローテーションに失敗しました というアラートがトリガーされます。このアラートを解決するには、テクニカル サポートに問い合わせる必要がある場合があります。

アプライアンス ノードを暗号化した後に再利用できますか**?**

暗号化されたアプライアンスを別のStorageGRIDシステムにインストールする必要がある場合は、まずグリッド ノードを廃止して、オブジェクト データを別のノードに移動する必要があります。その後、 StorageGRID

アプライアンスインストーラを使用して "KMS構成をクリアする"。 KMS 構成をクリアすると、ノード暗号化設定が無効になり、アプライアンス ノードとStorageGRIDサイトの KMS 構成間の関連付けが削除されます。

KMS 暗号化キーにアクセスできないと、アプライアンスに残っているデータにはアクセスできなくなり、永久にロックされます。

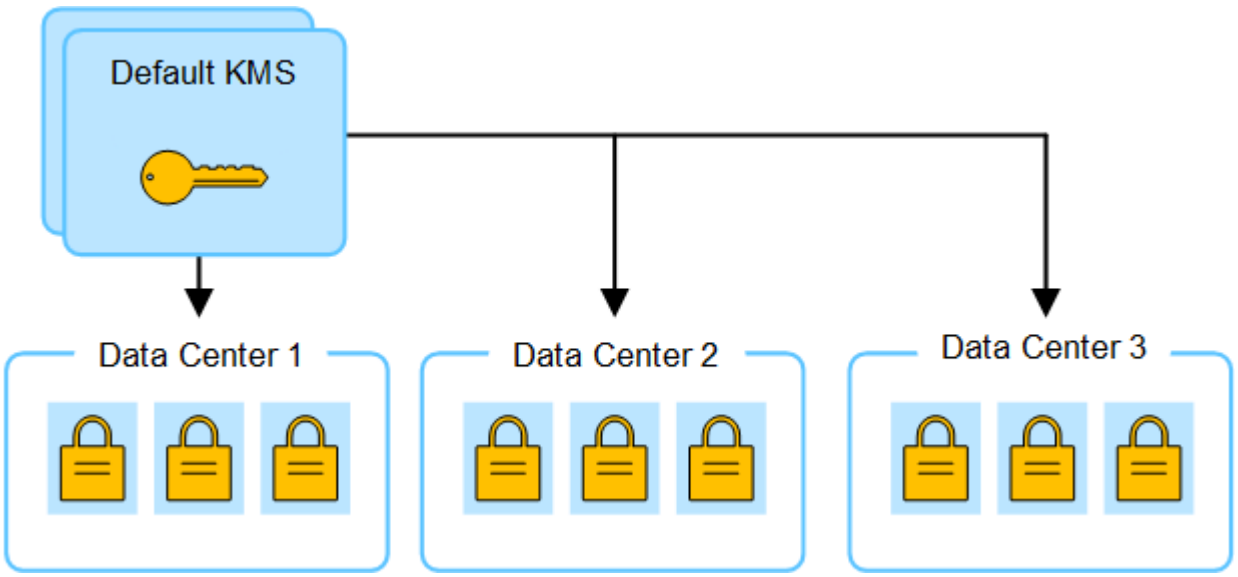
サイトの**KMS**を変更する際の考慮事項

各キー管理サーバー (KMS) または KMS クラスターは、単一のサイトまたはサイト グループにあるすべてのアプライアンス ノードに暗号化キーを提供します。サイトに使用する KMS を変更する必要がある場合は、暗号化キーをある KMS から別の KMS にコピーする必要がある場合があります。

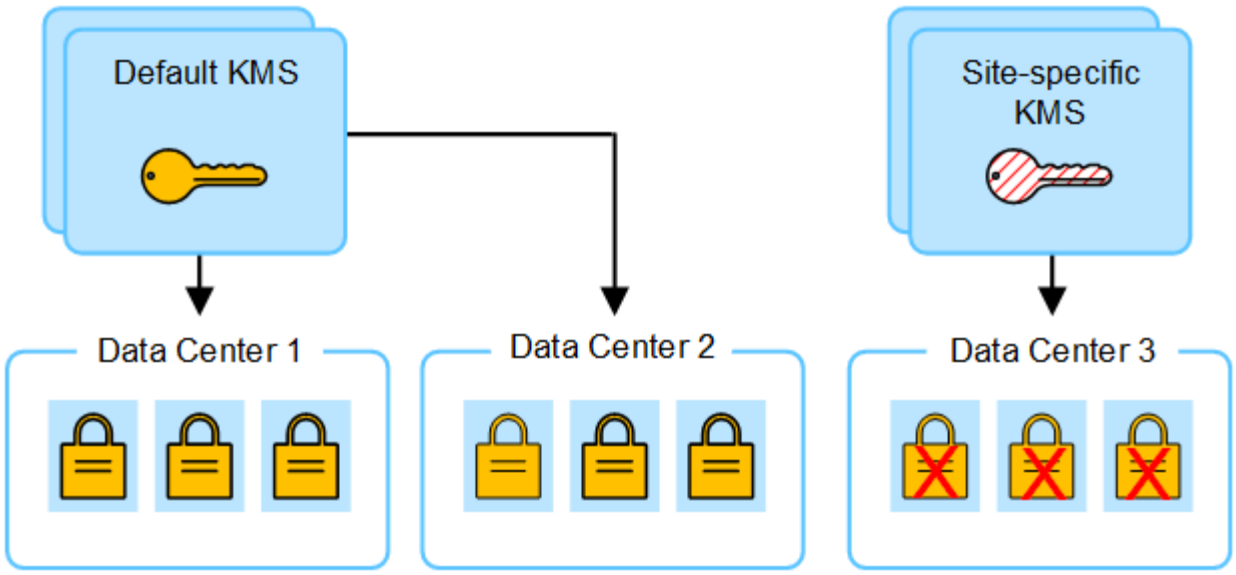
サイトに使用されている KMS を変更する場合は、そのサイトにある以前に暗号化されたアプライアンス ノードを、新しい KMS に保存されているキーを使用して復号化できることを確認する必要があります。場合によっては、現在のバージョンの暗号化キーを元の KMS から新しい KMS にコピーする必要があります。サイトの暗号化されたアプライアンス ノードを復号化するには、KMS に正しいキーがあることを確認する必要があります。

例えば：

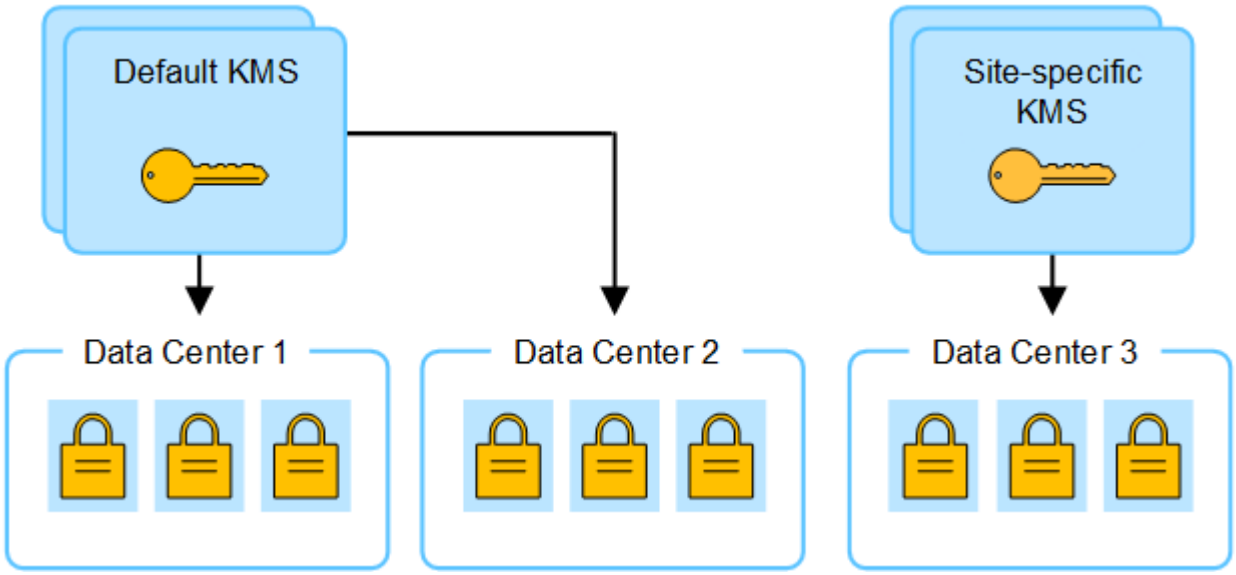
1. 最初に、専用の KMS がないすべてのサイトに適用されるデフォルトの KMS を構成します。
2. KMS が保存されると、*ノード暗号化*設定が有効になっているすべてのアプライアンス ノードが KMS に接続し、暗号化キーを要求します。このキーは、すべてのサイトのアプライアンス ノードを暗号化するために使用されます。これらのアプライアンスを復号化する場合にも、同じキーを使用する必要があります。



3. 1 つのサイト (図のデータ センター 3) にサイト固有の KMS を追加することにしました。ただし、アプライアンス ノードはすでに暗号化されているため、サイト固有の KMS の構成を保存しようとすると検証エラーが発生します。このエラーは、サイト固有の KMS にそのサイトのノードを復号化するための正しいキーがないため発生します。



4. この問題を解決するには、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーします。 (技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーは新しいキーの以前のバージョンになります。サイト固有の KMS には、データセンター 3 のアプライアンス ノードを復号化するための正しいキーが含まれるようになったため、 StorageGRIDに保存できるようになりました。



サイトで使用する **KMS** を変更するユースケース

次の表は、サイトの KMS を変更する最も一般的なケースに必要な手順をまとめたものです。

サイトの **KMS** を変更するユースケース	必要な手順
1 つ以上のサイト固有の KMS エントリがあり、そのうちの 1 つをデフォルトの KMS として使用します。	サイト固有の KMS を編集します。 キーの管理対象 フィールドで、別の **KMS** によって管理されていないサイト **(**デフォルトの **KMS)** を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。これは、専用の KMS を持たないすべてのサイトに適用されます。 "キー管理サーバー（KMS）を編集する"
デフォルトの KMS があり、拡張で新しいサイトを追加します。新しいサイトではデフォルトの KMS を使用しません。	1. 新しいサイトのアプライアンス ノードがすでにデフォルトの KMS によって暗号化されている場合は、KMS ソフトウェアを使用して、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーします。 2. グリッド マネージャーを使用して、新しい KMS を追加し、サイトを選択します。 "キー管理サーバー（KMS）を追加する"
サイトの KMS で別のサーバーを使用する必要がある。	1. サイトのアプライアンス ノードが既存の KMS によって既に暗号化されている場合は、KMS ソフトウェアを使用して、暗号化キーの現在のバージョンを既存の KMS から新しい KMS にコピーします。 2. グリッド マネージャーを使用して、既存の KMS 構成を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバー（KMS）を追加する"

StorageGRIDをKMSのクライアントとして設定する

KMS をStorageGRIDに追加するには、まず各外部キー管理サーバーまたは KMS クラスターのクライアントとしてStorageGRID を構成する必要があります。

これらの手順は、Thales CipherTrust Manager および Hashicorp Vault に適用されます。サポートされている製品とバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

手順

1. KMS ソフトウェアから、使用する予定の KMS または KMS クラスターごとにStorageGRIDクライアントを作成します。

   各 KMS は、単一のサイトまたはサイト グループにあるStorageGRIDアプライアンス ノードの単一の暗号化キーを管理します。

2. 次の 2 つの方法のいずれかを使用してキーを作成します。

   - KMS 製品のキー管理ページを使用します。各 KMS または KMS クラスターに対して AES 暗号化キーを作成します。

暗号化キーは 2,048 ビット以上で、エクスポート可能である必要があります。

- StorageGRIDにキーを作成させます。テストして保存するとプロンプトが表示されます"クライアント証明書のアップロード"。

3. 各 KMS または KMS クラスターについて次の情報を記録します。

   KMS をStorageGRIDに追加するときに、次の情報が必要になります。

   - 各サーバーのホスト名または IP アドレス。
   - KMS で使用される KMIP ポート。
   - KMS 内の暗号化キーのキーエイリアス。

4. 各 KMS または KMS クラスターごとに、証明機関 (CA) によって署名されたサーバー証明書、または証明書チェーンの順序で連結された各 PEM エンコードされた CA 証明書ファイルを含む証明書バンドルを取得します。

   サーバー証明書により、外部 KMS はStorageGRIDに対して自身を認証できるようになります。

   - 証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。
   - 各サーバー証明書のサブジェクト別名 (SAN) フィールドには、 StorageGRIDが接続する完全修飾ドメイン名 (FQDN) または IP アドレスが含まれている必要があります。

     StorageGRIDで KMS を構成する場合は、ホスト名 フィールドに同じ FQDN または IP アドレスを入力する必要があります。

   - サーバー証明書は、通常ポート 5696 を使用する KMS の KMIP インターフェイスで使用される証明書と一致する必要があります。

5. 外部 KMS によってStorageGRIDに発行された公開クライアント証明書と、クライアント証明書の秘密キーを取得します。

   クライアント証明書により、 StorageGRID はKMS に対して自身を認証できるようになります。

キー管理サーバー（**KMS**）を追加する

各 KMS または KMS クラスターを追加するには、 StorageGRIDキー管理サーバ ウィザードを使用します。

開始する前に

- あなたは、"キー管理サーバーの使用に関する考慮事項と要件" 。
- あなたが持っている"StorageGRIDをKMSのクライアントとして構成しました"各 KMS または KMS クラスターの必要な情報が得られます。
- 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"。

タスク概要

可能であれば、別の KMS によって管理されていないすべてのサイトに適用されるデフォルトの KMS を構成

する前に、サイト固有のキー管理サーバーを構成します。最初にデフォルトの KMS を作成すると、グリッド内のすべてのノード暗号化アプライアンスがデフォルトの KMS によって暗号化されます。後でサイト固有の KMS を作成する場合、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要があります。見る"サイトのKMSを変更する際の考慮事項"詳細については。

ステップ**1: KMS**の詳細

キー管理サーバーの追加ウィザードの手順 1 (KMS の詳細) では、KMS または KMS クラスターの詳細を指定します。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   構成の詳細タブが選択された状態で、キー管理サーバー ページが表示されます。

2. *作成*を選択します。

   キー管理サーバーの追加ウィザードのステップ 1 (KMS の詳細) が表示されます。

3. KMS と、その KMS で構成したStorageGRIDクライアントについて、次の情報を入力します。

フィールド	説明
KMS name	この KMS を識別するのに役立つ説明的な名前。 1 ～ 64 文字にする必要があります。
キー名	KMS 内のStorageGRIDクライアントの正確なキーエイリアス。 1 ～255 文字にする必要があります。 注: KMS 製品を使用してキーを作成していない場合は、StorageGRIDでキーを作成するように求められます。
キーを管理します	この KMS に関連付けられるStorageGRIDサイト。可能であれば、別の KMS によって管理されていないすべてのサイトに適用されるデフォルトの KMS を構成する前に、サイト固有のキー管理サーバーを構成する必要があります。 • この KMS が特定のサイトのアプライアンス ノードの暗号化キーを管理する場合は、サイトを選択します。 • 専用の KMS を持たないサイトと、その後の拡張で追加するサイトに適用されるデフォルトの KMS を構成するには、[別の KMS によって管理されていないサイト (デフォルトの KMS)] を選択します。 注意: 以前にデフォルトの KMS によって暗号化されたサイトを選択し、元の暗号化キーの現在のバージョンを新しい KMS に提供しなかった場合、KMS 構成を保存するときに検証エラーが発生します。

フィールド	説明
ポート	KMS サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注: サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスが含まれている必要があります。そうしないと、 StorageGRID はKMS または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。
5. *続行*を選択します。

ステップ**2:** サーバー証明書をアップロードする

キー管理サーバーの追加ウィザードの手順 2 (サーバー証明書のアップロード) では、KMS のサーバー証明書 (または証明書バンドル) をアップロードします。サーバー証明書により、外部 KMS はStorageGRIDに対して自身を認証できるようになります。

手順

1. ステップ **2 (**サーバー証明書のアップロード**)** から、保存されたサーバー証明書または証明書バンドルの場所を参照します。
2. 証明書ファイルをアップロードします。

   サーバー証明書のメタデータが表示されます。

   証明書バンドルをアップロードした場合、各証明書のメタデータがそれぞれのタブに表示されます。

3. *続行*を選択します。

ステップ**3:** クライアント証明書をアップロードする

キー管理サーバーの追加ウィザードの手順 3 (クライアント証明書のアップロード) では、クライアント証明書とクライアント証明書の秘密キーをアップロードします。クライアント証明書により、 StorageGRID はKMS に対して自身を認証できるようになります。

手順

1. ステップ **3 (**クライアント証明書のアップロード**)** から、クライアント証明書の場所を参照します。
2. クライアント証明書ファイルをアップロードします。

   クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密キーの場所を参照します。
4. 秘密鍵ファイルをアップロードします。

5. *テストして保存*を選択します。

   キーが存在しない場合は、 StorageGRIDにキーを作成するように要求されます。

   キー管理サーバーとアプライアンス ノード間の接続がテストされます。すべての接続が有効で、正しいキーが KMS に見つかった場合、新しいキー管理サーバーが [キー管理サーバー] ページのテーブルに追加されます。

   > KMS を追加するとすぐに、[キー管理サーバー] ページの証明書のステータスが [不明] と表示されます。 StorageGRID が各証明書の実際のステータスを取得するには、最大 30 分かかる場合があります。現在のステータスを確認するには、Web ブラウザを更新する必要があります。

6. テストして保存 を選択したときにエラー メッセージが表示される場合は、メッセージの詳細を確認して **OK** を選択します。

   たとえば、接続テストが失敗した場合、「422: 処理できないエンティティ」というエラーが表示されることがあります。

7. 外部接続をテストせずに現在の構成を保存する必要がある場合は、「強制保存」を選択します。

   > *強制保存*を選択すると、KMS 構成は保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成に問題がある場合は、影響を受けるサイトでノード暗号化が有効になっているアプライアンス ノードを再起動できない可能性があります。問題が解決されるまで、データにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、構成を強制的に保存する場合は [**OK**] を選択します。

   KMS 構成は保存されますが、KMS への接続はテストされません。

KMSを管理する

キー管理サーバー (KMS) の管理には、詳細の表示または編集、証明書の管理、暗号化されたノードの表示、不要になった KMS の削除が含まれます。

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" 。
- あなたは"必要なアクセス許可"。

KMSの詳細を表示

StorageGRIDシステム内の各キー管理サーバー (KMS) に関する情報 (キーの詳細、サーバーおよびクライアント証明書の現在のステータスなど) を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示され、次の情報が表示されます。

- [構成の詳細] タブには、構成されているキー管理サーバーの一覧が表示されます。
- 「暗号化されたノード」タブには、ノード暗号化が有効になっているノードが一覧表示されます。

2. 特定の KMS の詳細を表示し、その KMS に対して操作を実行するには、KMS の名前を選択します。 KMS の詳細ページには、次の情報が表示されます。

フィールド	説明
キーを管理します	KMS に関連付けられたStorageGRIDサイト。 このフィールドには、特定のStorageGRIDサイトの名前、または 別の **KMS** によって管理されていないサイト **(**デフォルトの **KMS)** が表示されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 つのキー管理サーバーのクラスターがある場合は、両方のサーバーの完全修飾ドメイン名または IP アドレスがリストされます。クラスター内に 3 台以上のキー管理サーバーが存在する場合、最初の KMS の完全修飾ドメイン名または IP アドレスが、クラスター内の追加のキー管理サーバーの数とともに一覧表示されます。 例えば： `10.10.10.10 and 10.10.10.11`または `10.10.10.10 and 2 others`。 クラスター内のすべてのホスト名を表示するには、KMS を選択し、[編集] または [アクション] > [編集] を選択します。

3. KMS 詳細ページでタブを選択すると、次の情報が表示されます。

タブ	フィールド	説明
主な詳細	キー名	KMS 内のStorageGRIDクライアントのキー エイリアス。
キーUID	キーの最新バージョンの一意の識別子。	最終更新日
キーの最新バージョンの日時。	サーバ証明書	メタデータ
証明書のメタデータ (シリアル番号、有効期限、時刻、証明書 PEM など)。	証明書PEM	証明書の PEM (プライバシー強化メール) ファイルの内容。
クライアント証明書	メタデータ	証明書のメタデータ (シリアル番号、有効期限、時刻、証明書 PEM など)。

4. 組織のセキュリティ慣行で必要な頻度で、「キーのローテーション」を選択するか、KMS ソフトウェアを使用して新しいバージョンのキーを作成します。

   キーのローテーションが成功すると、キー UID と最終変更日フィールドが更新されます。

> KMS ソフトウェアを使用して暗号化キーをローテーションする場合は、最後に使用したキーのバージョンから同じキーの新しいバージョンにローテーションします。まったく異なるキーに回転しないでください。
>
> KMS のキー名 (エイリアス) を変更してキーをローテーションしないでください。StorageGRID、以前に使用したすべてのキー バージョン (および将来のバージョン) が同じキー エイリアスを使用して KMS からアクセスできる必要があります。構成された KMS のキー エイリアスを変更すると、 StorageGRID はデータを復号化できなくなる可能性があります。

証明書の管理

サーバーまたはクライアント証明書に関する問題があれば速やかに対処してください。可能であれば、証明書の有効期限が切れる前に交換してください。

> データ アクセスを維持するには、証明書の問題をできるだけ早く解決する必要があります。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。
2. 表で、各 KMS の証明書の有効期限の値を確認します。
3. いずれかの KMS の証明書の有効期限が不明な場合は、最大 30 分待ってから Web ブラウザを更新してください。
4. 証明書の有効期限列に証明書の有効期限が切れているか、有効期限が近づいていることが示されている場合は、KMS を選択して KMS の詳細ページに移動します。
   a. *サーバー証明書*を選択し、「有効期限」フィールドの値を確認します。
   b. 証明書を置き換えるには、[証明書の編集] を選択して新しい証明書をアップロードします。
   c. これらのサブステップを繰り返し、サーバー証明書の代わりに*クライアント証明書*を選択します。
5. **KMS CA** 証明書の有効期限、**KMS** クライアント証明書の有効期限、および **KMS** サーバー証明書の有効期限 アラートがトリガーされた場合は、各アラートの説明をメモし、推奨されるアクションを実行してください。

   StorageGRID が証明書の有効期限の更新を取得するには、最大 30 分かかる場合があります。現在の値を表示するには、Web ブラウザを更新してください。

> サーバー証明書のステータスが不明 というステータスが表示される場合は、KMS でクライアント証明書を必要とせずにサーバー証明書を取得できることを確認してください。

暗号化されたノードを表示する

*ノード暗号化*設定が有効になっているStorageGRIDシステム内のアプライアンス ノードに関する情報を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示されます。 [構成の詳細] タブには、構成されているキー管理サーバーが表示されます。

2. ページの上部から、[暗号化されたノード] タブを選択します。

   [暗号化されたノード] タブには、 StorageGRIDシステム内の ノード暗号化 設定が有効になっているアプライアンス ノードが一覧表示されます。

3. 各アプライアンス ノードの表の情報を確認します。

列	説明
ノード名	アプライアンス ノードの名前。
ノード タイプ	ノードのタイプ: ストレージ、管理、またはゲートウェイ。
サイト	ノードがインストールされているStorageGRIDサイトの名前。
KMS name	ノードに使用される KMS の説明的な名前。 KMS がリストされていない場合は、[構成の詳細] タブを選択して KMS を追加します。 "キー管理サーバー（KMS）を追加する"
キーUID	アプライアンス ノード上のデータの暗号化と復号化に使用される暗号化キーの一意の ID。キー UID 全体を表示するには、テキストを選択します。 ダッシュ (--) は、アプライアンス ノードと KMS 間の接続の問題が原因で、キー UID が不明であることを示します。
ステータス	KMS とアプライアンス ノード間の接続の状態。ノードが接続されている場合、タイムスタンプは 30 分ごとに更新されます。 KMS 構成の変更後、接続ステータスが更新されるまでに数分かかる場合があります。 **注:** 新しい値を表示するには、Web ブラウザを更新してください。

4. ステータス列に KMS の問題が示されている場合は、すぐに問題に対処してください。

   通常の KMS 操作中は、ステータスは **KMS** に接続済み になります。ノードがグリッドから切断されている場合、ノードの接続状態 (管理上ダウンまたは不明) が表示されます。

   その他のステータス メッセージは、同じ名前のStorageGRIDアラートに対応しています。

   - KMS構成の読み込みに失敗しました
   - KMS接続エラー

- KMS暗号化キー名が見つかりません
- KMS暗号化キーのローテーションに失敗しました
- KMS キーがアプライアンス ボリュームの暗号化に失敗しました
- KMSが設定されていません

これらのアラートに対して推奨されるアクションを実行します。

データが完全に保護されるようにするには、問題があればすぐに対処する必要があります。

KMSの編集

たとえば、証明書の有効期限が近づいている場合など、キー管理サーバーの構成を編集する必要がある場合があります。

開始する前に

- KMS用に選択したサイトを更新する予定の場合は、"サイトのKMSを変更する際の考慮事項" 。
- 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"。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示され、構成されているすべてのキー管理サーバーが表示されます。

2. 編集する KMS を選択し、[アクション] > [編集] を選択します。

   表内の KMS 名を選択し、KMS 詳細ページで 編集 を選択して、KMS を編集することもできます。

3. 必要に応じて、キー管理サーバーの編集ウィザードの*ステップ 1 (KMS の詳細)* で詳細を更新します。

フィールド	説明
KMS name	この KMS を識別するのに役立つ説明的な名前。 1 ～ 64 文字にする必要があります。
キー名	KMS 内のStorageGRIDクライアントの正確なキーエイリアス。 1～255 文字にする必要があります。 キー名を編集する必要があるのは、まれなケースのみです。たとえば、KMS でエイリアスの名前が変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされた場合は、キー名を編集する必要があります。

フィールド	説明
キーを管理します	サイト固有の KMS を編集していて、デフォルトの KMS がまだない場合は、オプションで 別の **KMS** によって管理されていないサイト **(**デフォルトの **KMS)** を選択します。これを選択すると、サイト固有の KMS がデフォルトの KMS に変換され、専用の KMS を持たないすべてのサイトと、拡張で追加されたすべてのサイトに適用されます。 注意**:** サイト固有の KMS を編集している場合は、別のサイトを選択することはできません。デフォルトの KMS を編集している場合は、特定のサイトを選択することはできません。
ポート	KMS サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注**:** サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスが含まれている必要があります。そうしないと、StorageGRID はKMS または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。
5. *続行*を選択します。

   キー管理サーバーの編集ウィザードのステップ 2 (サーバー証明書のアップロード) が表示されます。

6. サーバー証明書を置き換える必要がある場合は、[参照] を選択して新しいファイルをアップロードします。
7. *続行*を選択します。

   キー管理サーバーの編集ウィザードのステップ 3 (クライアント証明書のアップロード) が表示されます。

8. クライアント証明書とクライアント証明書の秘密キーを置き換える必要がある場合は、[参照] を選択して新しいファイルをアップロードします。
9. *テストして保存*を選択します。

   影響を受けるサイトにあるキー管理サーバーとすべてのノード暗号化アプライアンス ノード間の接続がテストされます。すべてのノード接続が有効で、正しいキーが KMS 上に見つかった場合、キー管理サーバーが「キー管理サーバー」ページのテーブルに追加されます。

10. エラーメッセージが表示された場合は、メッセージの詳細を確認し、「**OK**」を選択します。

    たとえば、この KMS に選択したサイトが既に別の KMS によって管理されている場合、または接続テストが失敗した場合は、「422: 処理できないエンティティ」エラーが表示されることがあります。

11. 接続エラーを解決する前に現在の構成を保存する必要がある場合は、[強制保存] を選択します。

*強制保存*を選択すると、KMS 構成は保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成に問題がある場合は、影響を受けるサイトでノード暗号化が有効になっているアプライアンス ノードを再起動できない可能性があります。問題が解決されるまで、データにアクセスできなくなる可能性があります。

KMS 構成が保存されます。

12. 確認の警告を確認し、構成を強制的に保存する場合は [**OK**] を選択します。

    KMS 構成は保存されますが、KMS への接続はテストされません。

キー管理サーバー（**KMS**）を削除する

場合によっては、キー管理サーバーを削除する必要がある場合があります。たとえば、サイトを廃止した場合は、サイト固有の KMS を削除する必要がある場合があります。

開始する前に

- あなたは、"キー管理サーバーの使用に関する考慮事項と要件" 。
- 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"。

タスク概要

次の場合には KMS を削除できます。

- サイトが廃止された場合、またはサイトにノード暗号化が有効になっているアプライアンス ノードが含まれていない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効になっているアプライアンス ノードがある各サイトにサイト固有の KMS がすでに存在する場合は、デフォルトの KMS を削除できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示され、構成されているすべてのキー管理サーバーが表示されます。

2. 削除する KMS を選択し、[アクション] > [削除] を選択します。

   テーブル内の KMS 名を選択し、KMS 詳細ページで 削除 を選択して、KMS を削除することもできます。

3. 次の点を確認してください。
   - ノード暗号化が有効になっているアプライアンス ノードがないサイトのサイト固有の KMS を削除しています。
   - デフォルトの KMS を削除していますが、ノード暗号化が行われたサイトごとにサイト固有の KMS が既に存在しています。
4. *はい*を選択してください。

   KMS 構成が削除されます。

プロキシ設定を管理する

ストレージプロキシを構成する

プラットフォーム サービスまたはクラウド ストレージ プールを使用している場合は、ストレージ ノードと外部 S3 エンドポイント間に非透過プロキシを構成できます。たとえば、プラットフォーム サービス メッセージを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に送信できるようにするには、非透過プロキシが必要になる場合があります。

> 構成されたストレージ プロキシ設定は、Kafka プラットフォーム サービス エンドポイントには適用されません。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- 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" 。

タスク概要

単一のストレージ プロキシの設定を構成できます。

手順

1. 構成 > セキュリティ > *プロキシ設定*を選択します。
2. *ストレージ*タブで、*ストレージ プロキシを有効にする*チェックボックスをオンにします。
3. ストレージ プロキシのプロトコルを選択します。
4. プロキシ サーバーのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシ サーバーに接続するために使用するポートを入力します。

   プロトコルのデフォルト ポート (HTTP の場合は 80、SOCKS5 の場合は 1080) を使用するには、このフィールドを空白のままにします。

6. *保存*を選択します。

   ストレージ プロキシを保存した後、プラットフォーム サービスまたはクラウド ストレージ プールの新しいエンドポイントを構成してテストできます。

   > プロキシの変更が有効になるまでに最大 10 分かかる場合があります。

7. プロキシ サーバーの設定を確認し、 StorageGRIDからのプラットフォーム サービス関連のメッセージがブロックされないようにします。
8. ストレージ プロキシを無効にする必要がある場合は、チェックボックスをオフにして、[保存] を選択します。

管理プロキシ設定を構成する

HTTP または HTTPS を使用してAutoSupportパッケージを送信する場合は、管理ノード

とテクニカル サポート (AutoSupport) の間に非透過プロキシ サーバーを設定できます。

AutoSupportの詳細については、以下を参照してください。"AutoSupportを構成する" 。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- 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" 。

タスク概要

単一の管理プロキシの設定を構成できます。

手順

1. 構成 > セキュリティ > *プロキシ設定*を選択します。

   プロキシ設定ページが表示されます。デフォルトでは、タブ メニューで [ストレージ] が選択されています。

2. *管理者*タブを選択します。
3. *管理プロキシを有効にする*チェックボックスを選択します。
4. プロキシ サーバーのホスト名または IP アドレスを入力します。
5. プロキシ サーバーに接続するために使用するポートを入力します。
6. 必要に応じて、プロキシ サーバーのユーザー名とパスワードを入力します。

   プロキシ サーバーでユーザー名またはパスワードが不要な場合は、これらのフィールドを空白のままにしておきます。

7. 次のいずれかを選択します。

   - 管理プロキシへの接続を保護する場合は、「プロキシ証明書の検証」を選択します。管理プロキシ サーバーによって提示された SSL 証明書の信頼性を検証するために、CA バンドルをアップロードします。

     プロキシ証明書が検証されている場合、 AutoSupport on Demand、 StorageGRID経由の E シリーズAutoSupport 、およびStorageGRIDアップグレード ページでの更新パスの決定は機能しません。

   CA バンドルをアップロードすると、そのメタデータが表示されます。

   - 管理プロキシ サーバーと通信するときに証明書を検証しない場合は、[プロキシ証明書を検証しない] を選択します。

8. *保存*を選択します。

   管理プロキシが保存されると、管理ノードとテクニカル サポート間のプロキシ サーバーが構成されます。

   プロキシの変更が有効になるまでに最大 10 分かかる場合があります。

9. 管理プロキシを無効にする必要がある場合は、[管理プロキシを有効にする] チェックボックスをオフにし

て、[保存] を選択します。

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