セキュリティを管理します

StorageGRID 11.8

NetApp
March 19, 2024

目次

セキュリティを管理します . . . 1
セキュリティの管理：概要 . . . 1
StorageGRID の暗号化方式を確認します . . . 1
証明書を管理します . . . 4
セキュリティを設定します . . . 37
キー管理サーバを設定 . . . 43
プロキシ設定を管理します . . . 61
ファイアウォールを制御します . . . 63

セキュリティを管理します

セキュリティの管理：概要

StorageGRID システムのセキュリティを保護するために、 Grid Manager でさまざまなセキュリティ設定を行うことができます。

暗号化を管理します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。お勧めします "使用可能な暗号化方式を確認します" をクリックして、データ保護の要件を満たすものを特定します。

証明書を管理します

可能です "サーバ証明書を設定および管理します" HTTP接続、またはサーバに対するクライアントIDまたはユーザIDの認証に使用されるクライアント証明書に使用されます。

キー管理サーバを設定

を使用します "キー管理サーバ" アプライアンスがデータセンターから取り外された場合でも、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ると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

> 暗号化キー管理を使用するには、インストール時にアプライアンスをグリッドに追加する前に、アプライアンスごとに * Node Encryption * の設定を有効にする必要があります。

プロキシ設定を管理します

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する場合は、を設定できます "ストレージプロキシサーバ" ストレージノードと外部のS3エンドポイントの間。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" 管理ノードとテクニカルサポートの間。

ファイアウォールを制御します

システムのセキュリティを強化するために、で特定のポートを開いたり閉じたりして、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"。各ノードのを設定して、各ノードへのネットワークアクセスを制御することもできます "内部ファイアウォール"。導入に必要なポート以外のすべてのポートでアクセスを禁止できます。

StorageGRID の暗号化方式を確認します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。使用可能な方法を確認して、データ保護の要件を満たす方法を決定する必要があります。

次の表に、 StorageGRID で使用できる暗号化方式の概要を示します。

暗号化オプション	動作の仕組み	環境
Grid Manager からキー管理サーバ（ KMS ）を取得します	あなた "キー管理サーバを設定" StorageGRID サイトおよびの場合 "アプライアンスのノード暗号化を有効にします"。次に、アプライアンスノードが KMS に接続して、 Key Encryption Key （ KEK ；キー暗号化キー）を要求します。このキーは、各ボリューム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[Drive Encryption]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、インストール時にドライブ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復元することはできません。インストールを開始する前に、[ハードウェアの設定]>*[ドライブ暗号化]* に移動し、ノード内のすべてのStorageGRIDが管理する自己暗号化ドライブを環境に設定します。	自己暗号化ドライブを搭載したアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて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。 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コントローラを搭載したストレージアプライアンスを使用している場合は、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	SG5700またはSG6000ストレージ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、を使用できます "SANtricity システムマネージャ" をクリックしてセキュリティキーを作成および管理します。このキーは、セキュリティ保護されたドライブ上のデータにアクセスするために必要です。	Full Disk Encryption（FDE）ドライブまたは自己暗号化ドライブを搭載したストレージアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて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。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。
格納オブジェクトの暗号化	を有効にします "格納オブジェクトの暗号化" オプションを選択します。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が取り込み時に暗号化されます。	新たに取り込まれた S3 および Swift オブジェクトデータ。 既存の格納オブジェクトは暗号化されません。オブジェクト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	動作の仕組み	環境
S3 バケットの暗号化	PutBucketEncryption要求を問題して、バケットの暗号化を有効にします。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、取り込み時に暗号化されます。	新たに取り込まれた S3 オブジェクトデータのみ。 バケットに対して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。 "バケットの処理"
S3 オブジェクトのサーバ側の暗号化（ SSE ）	オブジェクトを格納してを含めるS3要求を問題 した `x-amz-server-side-encryption` 要求ヘッダー。	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクト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 で管理されます。 "サーバ側の暗号化を使用します"
ユーザ指定のキーによる S3 オブジェクトのサーバ側暗号化（ SSE-C ）	オブジェクトを格納する S3 要求を問題 し、 3 つの要求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`	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクト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。 "サーバ側の暗号化を使用します"

暗号化オプション	動作の仕組み	環境
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暗号化がサポートされている場合は、StorageGRID の外部の暗号化方式を使用して、ボリュームまたはデータストア全体を暗号化できます。	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ことを前提として、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。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、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 の外部でのオブジェクトの暗号化	StorageGRID に取り込まれる前にオブジェクトデータとメタデータを暗号化するには、 StorageGRID の外部の暗号化メソッドを使用します。	オブジェクトデータとメタデータのみ（システム設定データは暗号化されません）。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、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 - Developer Guide ：クライアント側の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します

要件に応じて、一度に複数の暗号化方式を使用できます。例：

- KMSを使用してアプライアンスノードを保護できます。また、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できます。また、[Stored Object Encryption]オプションを使用して、取り込み時にすべてのオブジェクトを暗号化することもできます。

暗号化を必要とするオブジェクトがごく一部しかない場合は、暗号化をバケットレベルまたは個々のオブジェクトレベルで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増加します。

証明書を管理します

セキュリティ証明書の管理：概要

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セキュアで信頼された接続の確立に使用される小さいデータファイルです。

StorageGRID では、 2 種類のセキュリティ証明書が使用されます。

- * HTTPS 接続を使用する場合は、サーバー証明書 * が必要です。サーバ証明書は、クライアントとサーバ間のセキュアな接続を確立し、クライアントに対するサーバの ID を認証し、データのセキュアな通信パスを提供するために使用されます。サーバとクライアントには、それぞれ証明書のコピーがあります。
- * クライアント証明書 * は、クライアントまたはユーザー ID をサーバーに対して認証し、パスワードだけではなく、より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 を使用してサーバに接続すると、サーバはサーバ証明書を返します。このサーバ証明書には公開鍵が含まれています。クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してサーバ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）のサーバとして、または他の接続（ 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 Grid CA 証明書 *

StorageGRID には、システムのインストール時に内部のグリッド CA 証明書を生成する認証局（ CA ）が組み込まれています。デフォルトでは、グリッド CA 証明書を使用して内部 StorageGRID トラフィックが保護されます。外部の認証局（ 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問題 カスタム証明書を作成できます。グリッド CA 証明書は非本番環境で使用できますが、本番環境では外部の認証局が署名したカスタム証明書を使用することを推奨します。証明書のないセキュアでない接続もサポートされますが、推奨されません。

- カスタムCA証明書は内部証明書を削除しません。ただし、カスタム証明書は、サーバ接続の確認用に指定した証明書である必要があります。
- カスタム証明書はすべてがを満たしている必要があります "サーバ証明書に関するシステムセキュリティ強化ガイドライン"。
- StorageGRID では、 CA からの証明書を 1 つのファイル（ CA 証明書バンドル）にバンドルすることがサポートされています。

> 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の CA 証明書も含まれています。本番環境では、オペレーティングシステムの CA 証明書の代わりに、外部の認証局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。

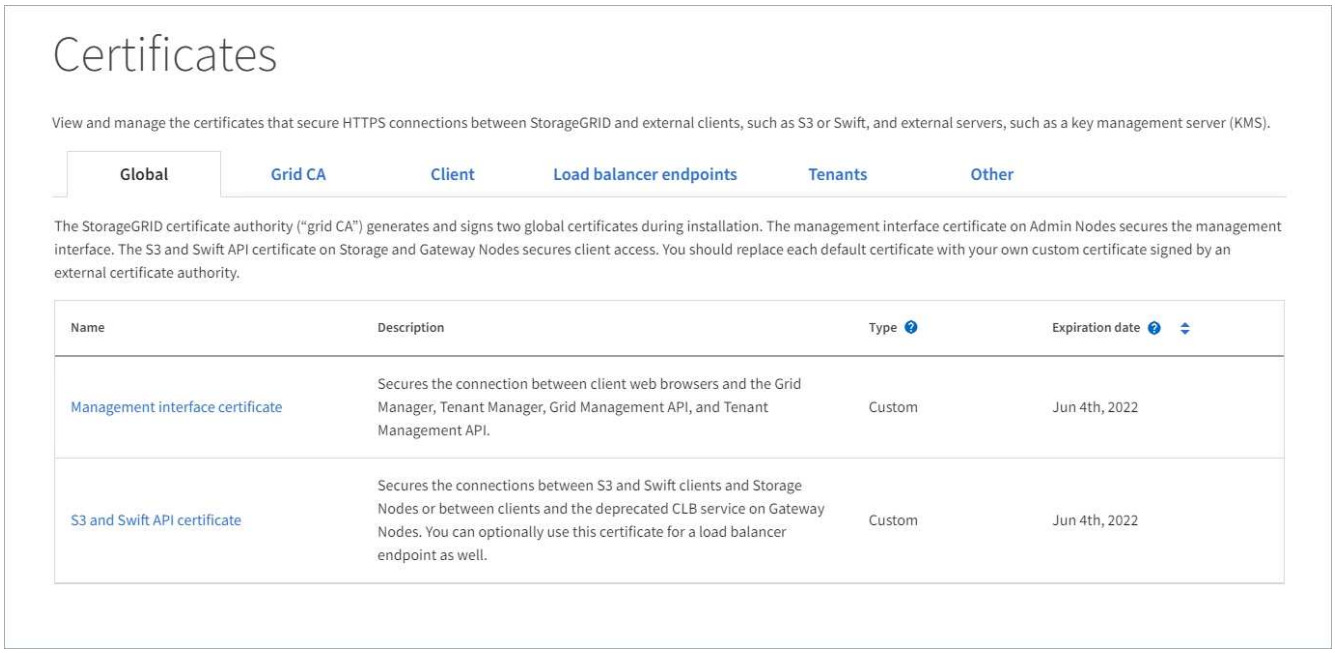
サーバ証明書とクライアント証明書のタイプのバリエーションは、いくつかの方法で実装されます。システムを設定する前に、特定の StorageGRID 構成に必要なすべての証明書を準備しておく必要があります。

アクセスセキュリティ証明書

すべての StorageGRID 証明書に関する情報に一元的にアクセスでき、各証明書の設定ワークフローへのリンクも含まれます。

手順

1. Grid Managerで、* configuration > Security > Certificates *を選択します。



2. [証明書] ページのタブを選択して、各証明書カテゴリの情報を表示し、証明書設定にアクセスします。タブにアクセスできるのは、 "適切な権限"。

   - * 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。
   - * Grid 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 データベースの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 および Swift 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 * ：アイデンティティフェデレーションサーバー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、証明書の詳細へのリンクを次に示します。

グローバル

グローバル証明書は、 Web ブラウザおよび外部の S3 および Swift API クライアントからの StorageGRID アクセスを保護します。2 つのグローバル証明書は、最初にインストール時に StorageGRID 認証局によって生成されます。本番環境では、外部の認証局によって署名されたカスタム証明書を使用することを推奨します。

- [管理インターフェイスの証明書]: クライアントの Web ブラウザ接続を StorageGRID 管理インターフェイスに保護します。
- S3 および Swift API 証明書：ストレージノード、管理ノード、および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。これらのノードは、 S3 および Swift クライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストールされるグローバル証明書には次の情報が含まれます。

- * 名前 * ：証明書の管理リンクを持つ証明書の名前。
- * 概要 *
- * 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ために、必ずカスタム証明書を使用してください。
- * 失効日 * ：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。

可能です

- グリッドセキュリティを向上させるには、外部の認証局によって署名されたカスタム証明書でデフォルト証明書を置き換えます。
  - "StorageGRID で生成されたデフォルトの管理インターフェイス証明書を置き換えます" Grid Manager 接続と Tenant Manager 接続に使用されます。
  - "S3 および Swift API 証明書を置き換えます" 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。
- "管理インターフェイスのデフォルトの証明書をリストア"
- "S3 および Swift のデフォルトの API 証明書をリストア"
- "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イス証明書を生成します。"
- をコピーまたはダウンロードします "管理インターフェイスの証明書" または "S3 および Swift API 証明書"。

Grid CA

。 Grid CA 証明書は、 StorageGRID のインストール時に StorageGRID 認証局によって生成され、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その内容が含まれます。

可能です "グリッドCA証明書をコピーまたはダウンロードします"しかし、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は外部の認証局によって生成され、外部の監視ツールと StorageGRID の Prometheus データベースとの間の接続を保護します。

証明書テーブルには、設定されている各クライアント証明書の行があり、証明書の有効期限とともにPrometheus データベースへのアクセスに証明書を使用できるかどうかが示されます。

可能です

- "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。"
- 証明書名を選択して証明書の詳細を表示します。表示される情報は次のとおりです。
  - "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 * （ Actions * ）] を選択して、すばやく "編集"、 "添付（ Attach ）"または "取り外します" クライアント証明書。最大 10 個のクライアント証明書を選択し、 * Actions * > * Remove * を使用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

ロードバランサエンドポイントの証明書 S3およびSwiftクライアントと、ゲートウェイノードと管理ノード上のStorageGRID ロードバランササービスの間の接続を保護します。

ロードバランサエンドポイントテーブルには、設定されている各ロードバランサエンドポイント用の行があり、グローバルな S3 および Swift API 証明書とカスタムのロードバランサエンドポイント証明書のどちらがエンドポイントに使用されているかを示しています。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 分かかることがあります。

可能です

- "ロードバランサエンドポイントを表示します"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。"
- "グローバルな S3 および Swift API 証明書を使用します" 代わりに、新しいロードバランサエンドポイント証明書を生成します。

テナント

テナントで使用できる アイデンティティフェデレーションサーバの証明書 または プラットフォームサービスエンドポイントの証明書 StorageGRID を使用して接続を保護します。

テナントテーブルには、テナントごとに 1 つの行があり、各テナントに独自のアイデンティティ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。

可能です

- "Tenant Manager にサインインするテナント名を選択します"
- "テナントのアイデンティティフェデレーションの詳細を表示するテナント名を選択します"
- "テナントプラットフォームサービスの詳細を表示するテナント名を選択します"

- "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 では、特定の目的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、機能名で一覧表示されます。その他のセキュリティ証明書には、次のもの

- クラウドストレージプールの証明書
- E メールアラート通知の証明書
- 外部 syslog サーバ証明書
- グリッドフェデレーション接続の証明書
- 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（ KMS ）の証明書
- 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、その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表示およびアクセスできるのは、 "適切な権限"。

可能です

- "S3 、 C2S S3 、または Azure 用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 E メール通知用の証明書を指定します"
- "外部syslogサーバの証明書を使用する"
- "グリッドフェデレーション接続の証明書をローテーションします"
- "アイデンティティフェデレーション証明書を表示および編集する"
- "キー管理サーバ（ KMS ）のサーバ証明書とクライアント証明書をアップロードします"
- "証明書利用者信頼のSSO証明書を手動で指定します"

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、実装手順へのリンクとともに以下に説明します。

管理インターフェイスの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。 この証明書は、 Grid 管理 API 接続とテナント管理 API 接続も認証します。 インストール時に作成される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。	• 設定 * > * セキュリティ * > * 証明書 * 、 * グローバル * タブを選択し、 * 管理インターフェイス証明書 * を選択します	"管理インターフェイス証明書を設定"

S3 および **Swift API** 証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	ストレージノードとロードバランサエンドポイントへのS3またはSwiftクライアントのセキュアな接続を認証します（オプション）。	• configuration * > * Security * > * Certificates * を選択し、 * Global * タブを選択して、 * S3 および Swift API certificate * を選択します	"S3 および Swift API 証明書を設定する"

Grid CA 証明書

を参照してください デフォルトの Grid CA 証明書概要。

管理者クライアント証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
クライアント	StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。 • 許可された外部クライアントから 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 をセキュアに監視できます。	• 設定 * > * 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設定"

ロードバランサエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	S3 または Swift クライアントと、ゲートウェイノードおよび管理ノード上の StorageGRID ロードバランササービス間の接続を認証します。ロードバランサエンドポイントの設定時に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では、 StorageGRID に接続する際にロードバランサ証明書を使用してオブジェクトデータを保存および読み出します。 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 および Swift API 証明書 ロードバランササービスへの接続を認証する証明書。グローバル証明書を使用してロードバランサ接続を認証する場合は、ロードバランサ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： * ロードバランサ認証に使用される証明書は、通常の StorageGRID 処理で最もよく使用される証明書です。	• 設定 * > * ネットワーク * > * ロードバランサエンドポイント *	• "ロードバランサエンドポイントを設定する" • "FabricPool のロードバランサエンドポイントを作成します"

クラウドストレージプールのエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	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への接続を認証します。クラウドプロバイダのタイプごとに別の証明書が必要です。	• ilm * > * ストレージ・プール *	"クラウドストレージプールを作成"

E メールアラート通知の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。 • SMTP サーバとの通信に Transport Layer Security （ TLS ）が必要な場合は、 E メールサーバの CA 証明書を指定する必要があります。 • SMTP E メールサーバで認証用のクライアント証明書が必要な場合にのみ、クライアント証明書を指定してください。	• アラート > 電子メールセットアップ *	"アラート用の E メール通知を設定します"

外部 **syslog** サーバの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	StorageGRID にイベントを記録する外部 syslog サーバ間で、 TLS 接続または 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。	設定>*監視*>*監査およびsyslogサーバ*	"外部 syslog サーバを使用します"

[[grid-federation-certificate]グリッドフェデレーション接続証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	グリッドフェデレーション接続で、現在のStorageGRID システムと別のグリッドの間で送信される情報を認証して暗号化します。	設定>*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します"

アイデンティティフェデレーション証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory 、 OpenLDAP 、 Oracle Directory Server などの外部のアイデンティティプロバイダと StorageGRID の間の接続を認証します。アイデンティティフェデレーションに使用します。管理者グループとユーザを外部システムで管理できます。	• 設定 * > * アクセス制御 * > * アイデンティティフェデレーション *	"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（ **KMS** ）の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	StorageGRID と外部キー管理サーバ（ KMS ）の間の接続を認証します。この接続により、 StorageGRID アプライアンスノードに暗号化キーが提供されます。	• 設定 * > * セキュリティ * > * キー管理サーバ *	"キー管理サーバの追加（ KMS ）"

プラットフォームサービスのエンドポイント証明書

証明書のタイプ	説明	ナビゲーションの場所	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。	• Tenant Manager * > * storage （ S3 ） * > * Platform services endpoints *	"プラットフォームサービスエンドポイントを作成します" "プラットフォームサービスエンドポイントを編集します"

シングルサインオン（ **SSO** ）証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory フェデレーションサービス（ AD FS ）やシングルサインオン（ SSO ）要求に使用される StorageGRID などのアイデンティティフェデレーションサービスとの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設定します"

証明書の例

例 **1** ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

1. ロードバランサエンドポイントを設定し、 StorageGRID でサーバ証明書をアップロードまたは生成します。
2. S3 または Swift クライアント接続をロードバランサエンドポイントに設定し、同じ証明書をクライアントにアップロードします。
3. クライアントは、データを保存または取得する際に HTTPS を使用してロードバランサエンドポイントに接続します。
4. StorageGRID は、公開鍵を含むサーバ証明書と、秘密鍵に基づく署名を返します。
5. クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、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. クライアントがオブジェクトデータを StorageGRID に送信

例 **2** ：外部キー管理サーバ（ **KMS** ）

この例では、 StorageGRID がクライアントとして機能します。

1. 外部キー管理サーバソフトウェアを使用する場合は、 StorageGRID を KMS クライアントとして設定し、 CA 署名済みサーバ証明書、パブリッククライアント証明書、およびクライアント証明書の秘密鍵を取得します。
2. Grid Manager を使用して KMS サーバを設定し、サーバ証明書とクライアント証明書およびクライアント秘密鍵をアップロードします。
3. StorageGRID ノードで暗号化キーが必要な場合、証明書からのデータと秘密鍵に基づく署名を含む KMS サーバに要求が送信されます。
4. KMS サーバは証明書の署名を検証し、 StorageGRID を信頼できることを決定します。
5. KMS サーバは、検証済みの接続を使用して応答します。

サーバ証明書を設定

サポートされているサーバ証明書のタイプ

StorageGRID システムでは、 RSA または ECDSA （ Elliptic Curve Digital Signature

Algorithm ）で暗号化されたカスタム証明書がサポートされます。

セキュリティポリシーの暗号タイプは、サーバ証明書タイプと一致している必要があります。たとえば、RSA暗号にはRSA証明書が必要で、ECDSA暗号にはECDSA証明書が必要です。を参照してください "セキュリティ証明書を管理する"。サーバ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設定する場合は、設定できます "一時的にデフォルトのセキュリティポリシーに戻します"。

StorageGRIDによるクライアント接続の保護方法の詳細については、を参照してください。 "S3オヨヒSwiftクライアントノセキユリテイ"。

管理インターフェイス証明書を設定

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ると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。デフォルトの管理インターフェイス証明書に戻すか、新しい証明書を生成することもできます。

このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタム管理インターフェイス証明書および対応する秘密鍵に置き換えることができます。

Grid Manager および Tenant Manager への接続時にクライアントがホスト名を確認する必要がある場合は、単一のカスタム管理インターフェイスの証明書がすべての管理ノードに対して使用されるため、ワイルドカード証明書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に一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（ CA ）によっては、ユーザが Grid Manager および Tenant Manager へのアクセスに使用する Web ブラウザに Grid CA 証明書をインストールすることも必要になります。

サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと* Expiration of server certificate for Management Interface *アラートがトリガーされます。必要に応じて、 ［グローバル］ タブで ［* 設定 *］ > ［* セキュリティ *］ > ［* 証明書 *］ を選択し、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 にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイ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イス証明書をデフォルトのサーバ証明書に戻します。

カスタム管理インターフェイス証明書を追加します

カスタムの管理インターフェイス証明書を追加するには、 Grid Manager を使用して独自の証明書を指定するか、証明書を生成します。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] 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する

必要なサーバ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. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ 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 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）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し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は、各証明書が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 * を選択します。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。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.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、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。[+] 以降、Grid Manager、Tenant Manager、Grid Manager API、またはTenant Manager APIへのすべての新規接続には、カスタムの管理インターフェイス証明書が使用されます。

証明書の生成

サーバ証明書ファイルを生成します。

> 本番環境では、外部の認証局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を推奨します。

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。

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（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、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。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 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:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （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。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.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、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。[+] 以降、Grid Manager、Tenant Manager、Grid Manager API、またはTenant Manager APIへのすべての新規接続には、カスタムの管理インターフェイス証明書が使用されます。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

新しい証明書をアップロードまたは生成したあと、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に最大 1 日かかります。

6. カスタムの管理インターフェイス証明書を追加すると、使用中の証明書の詳細な証明書情報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。[+] 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。

管理インターフェイスのデフォルトの証明書をリストア

Grid Manager 接続と Tenant Manager 接続での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. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   管理インターフェイスのデフォルトの証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降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. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

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イス証明書を生成します

ホスト名の厳密な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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を使用することができます `Passwords.txt` ファイル。

このタスクについて

本番環境では、外部の認証局によって署名された証明書を使用することを推奨します。

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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. 新しい自己署名証明書を使用して StorageGRID を設定します。

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

   - の場合 `--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： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 終了： `management` 管理インターフェイスの証明書を設定します。この証明書はGrid ManagerとTenant Managerで使用されます。

◦ 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）です。この期間を過ぎる前に証明書を再作成する必要があります。を使用できます `--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、で始まります `make-certificate` を実行します。管理クライアントが StorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが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
```

出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. [* configuration * > * Security * > * Certificates *] を選択します
   c. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
7. コピーしたパブリック証明書を使用するように管理クライアントを設定します。BEGIN タグと END タグを含めてください。

管理インターフェイ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. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [**Server**] タブまたは [**CA Bundle**] 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します

証明書またはCAバンドルをダウンロードします `.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は、バンドル内の各証明書が独自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にあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   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にある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に貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

S3 および **Swift 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エンドポイントへのS3 / Swiftクライアント接続に使用されるサーバ証明書を置き換えたりリストアしたりできます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

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 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書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カスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（ CA ）によっては、システムへのアクセスに使用する S3 または Swift API クライアントにグリッド CA 証明書をインストールすることも必要になる場合があ

ります。

> サーバ証明書の問題によって処理が中断されないようにするために、ルートサーバ証明書の有効期限が近づくと* Expiration of global server certificate for S3 and Swift API *アラートがトリガーされます。必要に応じて、現在の証明書の有効期限を確認するには、 * configuration * > * Security * > * Certificates * を選択し、 S3 および Swift API 証明書の有効期限を Global タブで確認します。

S3 および Swift のカスタム API 証明書をアップロードまたは生成できます。

S3 および Swift のカスタム API 証明書を追加します

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift 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する

必要なサーバ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. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ 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 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局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して含まれている必要があります。

c. 証明書の詳細を選択して、アップロードしたカスタムの S3 および Swift API 証明書ごとにメタデータと PEM 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は、各証明書が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 * を選択します。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。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.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、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

証明書の生成

サーバ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（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、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。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 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:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. Certificate Details * を選択して、生成されたカスタムの S3 および Swift API 証明書のメタデータと PEM を表示します。

- 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。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.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、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

5. タブを選択して、デフォルトの StorageGRID サーバ証明書、アップロードされた CA 署名証明書、または生成されたカスタム証明書のメタデータを表示します。

> 新しい証明書をアップロードまたは生成したあと、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に最大 1 日かかります。

6. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

7. カスタムの S3 および Swift API 証明書を追加すると、使用中のカスタムの S3 および Swift API 証明書の詳細な証明書情報が S3 および Swift API の証明書ページに表示されます。[+] 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。

S3 および Swift のデフォルトの API 証明書をリストア

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

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift API 証明書 * を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   S3およびSwift APIのグローバル証明書のデフォルトバージョンをリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからリカバリすることはできません。ストレージノードへの以降の新しいS3およびSwiftクライアント接続には、デフォルトのS3およびSwift API証明書が使用されます。

4. 警告を確認し、デフォルトの S3 および Swift API 証明書をリストアするには、「 * OK 」を選択します。

   Root Access 権限がある環境で、 S3 および Swift API のカスタム証明書をロードバランサエンドポイントの接続に使用していた場合は、デフォルトの S3 および Swift 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エンドポイントのリストが表示されます。に進みます "ロードバランサエンドポイントを設定する" 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. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

S3 および Swift API 証明書をダウンロードまたはコピーします

S3 および Swift 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. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift API 証明書 * を選択します。
3. [**Server**] タブまたは [**CA Bundle**] 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します

証明書またはCAバンドルをダウンロードします `.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は、バンドル内の各証明書が独自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にあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   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にある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に貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

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

Grid CA 証明書をコピーする

StorageGRID は、内部の認証局（ 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ても、この証明書は変更されません。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。

このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用

してサーバ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。

手順

1. [* configuration * > * Security * > * Certificates *] を選択し、 [* Grid CA *] タブを選択します。
2. [Certificate 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します

   証明書をダウンロードします `.pem` ファイル。

   a. [証明書のダウンロード] を選択します。
   b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

      例： `storagegrid_certificate.pem`

   証明書 **PEM** をコピーします

   証明書のテキストをコピーして別の場所に貼り付けてください。

   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に貼り付けます。
   c. 拡張子を付けてテキストファイルを保存します `.pem`。

      例： `storagegrid_certificate.pem`

FabricPool の **StorageGRID** 証明書を設定します

S3クライアントが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場合（FabricPool を使用するONTAP クライアントなど）は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（ CA ）によって署名された証明書をアップロードできます。本番環境では、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、システムを停止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としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、を参照してください "StorageGRID for FabricPool を設定します"。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する 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際に、サーバ証明書、証明書の秘密鍵、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. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

> 中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定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 証明書を指定する必要があります。

クライアント証明書を設定

クライアント証明書を使用すると、許可された外部クライアントから StorageGRID の Prometheus データベースにアクセスして、外部ツールで StorageGRID を監視するための安全な方法を提供できます。

外部の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、グリッドマネージャ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、証明書の情報を外部ツールにコピーする必要があります。

を参照してください "セキュリティ証明書を管理する" および "カスタムサーバ証明書を設定する"。

> サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと* Expiration of client certificates configured on the Certificates page *アラートがトリガーされます。必要に応じて、 ［クライアント］ タブで ［* 設定 *］ > ［* セキュリティ *］ > ［* 証明書 *］ を選択し、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。

> 特別に設定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（ KMS ）を使用する場合は、についての具体的な情報を参照してください "KMS クライアント証明書をアップロードする"。

作業を開始する前に

- Root Access 権限が割り当てられている。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- クライアント証明書を設定するには：
  - 管理ノードの IP アドレスまたはドメイン名を確認しておきます。
  - 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の設定に使用するCA、クライアント証明書、および秘密鍵を用意しておきます。
  - 独自の証明書をアップロードするには、証明書の秘密鍵をローカルコンピュータで使用できます。
  - 秘密鍵は、作成時に保存または記録しておく必要があります。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を確認しておきます。
  - 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、ローカルコンピュータ上で秘密鍵、クライアント証明書、およびCA（使用している場合）を使用できます。

クライアント証明書を追加します

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実行します。

- [管理インターフェイス証明書はすでに設定されています]
- CAによって発行されたクライアント証明書
- Grid Managerから証明書が生成されました

管理インターフェイス証明書はすでに設定されています

顧客が指定したCA、クライアント証明書、および秘密鍵を使用して管理インターフェイス証明書がすでに設定されている場合は、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. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * 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. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. [証明書の接続]*ステップでは、管理インターフェイ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、管理インターフェイスの証明書ファイルを選択します (`.pem`）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が [クライアント] タブに表示されます。
7. 外部監視ツールを設定します（Grafanaなど）。

CAによって発行されたクライアント証明書

管理インターフェイス証明書が設定されていない場合や、CAによって発行されたクライアント証明書と秘密鍵を使用するPrometheusのクライアント証明書を追加する場合は、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. 手順~を実行します "管理インターフェイス証明書を設定します"。
2. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * 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. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 「 * Continue * 」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、秘密鍵、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、およびCAバンドルファイルを選択します (`.pem`）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が[クライアント]タブに表示されます。
8. 外部監視ツールを設定します（Grafanaなど）。

Grid Managerから証明書が生成されました

管理インターフェイス証明書が設定されていない場合や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. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * 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. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. ステップで、[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：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     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で接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

8. [*Generate （生成）] を選択します
9. 証明書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、証明書の秘密鍵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、 * 証明書の PEM をコピー * 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。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 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。

  秘密鍵ファイルの名前とダウンロード先を指定します。

10. 証明書を Grid Manager に保存するには、 * Create * を選択します。

    新しい証明書が [クライアント] タブに表示されます。

11. Grid Managerで、* configuration > Security > Certificates を選択し、 Global *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. 証明書の.pemファイルとprivate_key.pemファイルをから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します (`.pem`）。
    c. 証明書をGrid Managerに保存するには、* Save *を選択します。

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

15. 外部監視ツールを設定します（Grafanaなど）。

外部監視ツールを設定します

手順

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

      StorageGRID ではこの情報は必要ありませんが、接続をテストするための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. CA 証明書を使用して、 * TLS クライアント認証 * および * を有効にします。

d. TLS/SSL Auth Detailsの下で、+をコピーして貼り付けます

- 管理インターフェイスのCA証明書を**CA Cert**に追加します
- クライアント証明書をクライアント証明書に送信します
- クライアントキー**への秘密鍵

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鍵を保存してテストします。

これで、外部の監視ツールを使用して StorageGRID から Prometheus 指標にアクセスできるようになります。

これらの指標の詳細については、を参照してください "StorageGRID の監視手順"。

クライアント証明書を編集します

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. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、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. 「 * Edit * 」を選択し、「 * 名前と権限を編集 * 」を選択します
4. 証明書名を入力します。
5. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 証明書を Grid Manager に保存するには、「 * Continue * 」を選択します。

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接続します

現在の証明書の期限が切れたときに新しい証明書をアップロードできます。

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。

   証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、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する

証明書のテキストをコピーして別の場所に貼り付けてください。

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します (`.pem`）。

   クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   - 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。

     証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.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、 * 証明書の PEM をコピー * を選択します。

c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

   更新された証明書が [クライアント] タブに表示されます。

証明書の生成

証明書のテキストを生成して他の場所に貼り付けます。

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：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     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で接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

c. [*Generate （生成）] を選択します

d. クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   ダイアログを閉じると、証明書の秘密鍵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、 * 証明書の PEM をコピー * 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。

証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 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。

  秘密鍵ファイルの名前とダウンロード先を指定します。

e. 証明書を Grid Manager に保存するには、 * Create * を選択します。

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します

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

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] 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します

証明書をダウンロードします `.pem` ファイル。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

証明書をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

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に貼り付けます。
c. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

クライアント証明書を削除します

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. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] 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」を選択して確定します。

> 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。

証明書を削除したあと、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の新しいクライアント証明書を指定する必要があります。

セキュリティを設定します

TLSおよびSSHポリシーを管理します

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セキュアなTLS接続の確立および内部StorageGRID サービスへのセキュアなSSH接続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による移動中のデータの暗号化方法を制御します。一般に、お使いのシステムがCC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ある場合を除き、最新の互換性（デフォルト）ポリシーを使用してください。

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

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセス権限"。

セキュリティポリシーを選択します

手順

1. * configuration > Security > Security settings *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。ポリシーのタイルには、現在アクティブなポリシーが緑のチェックマークで表示されます。

2. タイルで使用可能なポリシーを確認します。

ポリシー	説明
最新の互換性（デフォルト）	特別な要件がないかぎり、強力な暗号化が必要な場合はデフォルト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	古いクライアントの互換性オプションを追加する必要がある場合は、このポリシーを使用します。このポリシーにオプションを追加すると、最新の互換性ポリシーよりもセキュリティが低下する可能性があります。
Common Criteriaの略	情報セキュリティ国際評価基準の認定が必要な場合は、このポリシーを使用します。
FIPS strict	このポリシーは、Common Criteria認定が必要で、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に使用します。このポリシーを使用するとパフォーマンスが低下することがあります。 注：このポリシーを選択したあと、すべてのノードは "ローリング方式でリブートされた" NetApp暗号セキュリティモジュールをアクティブにするには、次の手順を実行します。再起動を開始および監視するには、* Maintenance > Rolling reboot *を使用してください。
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、および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、*[ポリシーを使用]*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します

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近いポリシーのタイルで、*[詳細を表示]*を選択します。
2. を選択し、[キャンセル]*を選択します。

3. [カスタムポリシー]タイルで、*[設定と使用]*を選択します。
4. コピーしたJSONを貼り付けて、必要な変更を行います。
5. [ポリシーを使用]*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]*の横に緑のチェックマークが表示されます。

6. 必要に応じて、*[設定の編集]*を選択して、新しいカスタムポリシーをさらに変更します。

一時的にデフォルトのセキュリティポリシーに戻します

カスタムセキュリティポリシーを設定した場合、設定したTLSポリシーがと互換性がないと、Grid Managerにサインインできないことがあります "サーバ証明書を設定しました"。

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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

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 Grid Manager にアクセスする。
4. の手順に従います セキュリティポリシーを選択します をクリックして、ポリシーを再設定します。

ネットワークとオブジェクトのセキュリティを設定します

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、格納オブジェクトの暗号化、特定のS3およびSwift要求の防止、または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することができます。

格納オブジェクトの暗号化

格納オブジェクトの暗号化を使用すると、S3経由で取り込まれたすべてのオブジェクトデータを暗号化できます。デフォルトでは、格納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ができます。この設定を有効にすると、新たに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、既存の格納オブジェクトに対する変更はありません。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ですが、新しく取り込まれたオブジェクトは暗号化されません

格納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で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、を参照してください "StorageGRID の暗号化方式を確認します"。

クライアントの変更を防止します

[Prevent client modification]は、システム全体の設定です。[Prevent client modification *]オプションを選択すると、次の要求が拒否されます。

S3 REST API

- DeleteBucketヨウキユウ
- 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

Swift REST API

- コンテナの削除要求
- 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

ストレージノード接続用の**HTTP**を有効にします

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。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

ストレージノード接続にHTTPを使用するのは、S3およびSwiftクライアントからストレージノードへのHTTP接続を直接確立する必要がある場合のみです。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（を使用できるため）には、このオプションを使用する必要はありません "

各ロードバランサエンドポイントを設定します" HTTPまたはHTTPSを使用する場合）。

を参照してください "Summary ：クライアント接続の IP アドレスとポート" を参照してください。HTTPまたはHTTPSを使用してストレージノードに接続する際にS3およびSwiftクライアントが使用するポートを確認できます。

オプションを選択します

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Root Access 権限が割り当てられている。

手順

1. * configuration > Security > Security settings *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. 格納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、格納オブジェクトを暗号化する場合は* AES-128 または AES-256 *を選択します。
4. 必要に応じて、S3およびSwiftクライアントが特定の要求を実行しないようにする場合は、*[Prevent client modification]*を選択します。

   この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

5. 必要に応じて、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、*[ストレージノード接続用のHTTPを有効にする]*を選択します。

   要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

6. [保存（ Save ）] を選択します。

インターフェイスセキュリティ設定の変更

インターフェイスのセキュリティ設定では、ユーザが指定した時間以上非アクティブであった場合にサインアウトするかどうか、およびスタックトレースをAPIエラー応答に含めるかどうかを制御できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "rootアクセス権限"。

このタスクについて

[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

ユーザのブラウザが非アクティブになってからサインアウトされるまでの時間を示します。デフォルトは15 分です。

ブラウザの非アクティブ時のタイムアウトは、次の方法でも制御されます。

- システムセキュリティ用の、個別の設定不可能な 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。ユーザの認証が期限切れになると、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、再度サインインする必要があります。
- アイデンティティプロバイダのタイムアウト設定（StorageGRID でシングルサインオン（SSO）が有効になっている場合）。

  SSOが有効になっていて、ユーザのブラウザがタイムアウトした場合、StorageGRID に再度アクセスするには、SSOクレデンシャルを再入力する必要があります。を参照してください "シングルサインオンを設定します"。

管理**API**スタックトレース

Grid ManagerおよびTenant Manager APIのエラー応答でスタックトレースを返すかどうかを制御します。

このオプションはデフォルトでは無効になっていますが、テスト環境では有効にすることもできます。一般に、本番環境では、APIエラーが発生したときに内部ソフトウェアの詳細が表示されないように、スタックトレースは無効のままにしておく必要があります。

手順

1. * configuration > Security > Security settings *を選択します。
2. [インターフェイス]*タブを選択します。
3. ブラウザ非アクティブタイムアウトの設定を変更するには、次の手順を実行します。
   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（ Save ）] 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、ユーザが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、次の手順を実行します。
   a. アコーディオンを展開します。
   b. Grid ManagerおよびTenant Manager APIのエラー応答でスタックトレースを返す場合は、チェックボックスを選択します。

      APIエラーが発生したときに内部ソフトウェアの詳細が表示されないように、本番環境ではスタックトレースを無効のままにします。

c. [保存（ Save ）] を選択します。

キー管理サーバを設定

キー管理サーバの設定：概要

1 つ以上の外部キー管理サーバ（ KMS ）を設定して、特別に設定したアプライアンスノード上のデータを保護することができます。

StorageGRIDでは、特定のキー管理サーバのみがサポートされます。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、 "ネットアップの Interoperability Matrix Tool （ IMT ）"。

キー管理サーバ（ **KMS** ）とは何ですか？

キー管理サーバ（ KMS ）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol （ KMIP ）を使用して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。

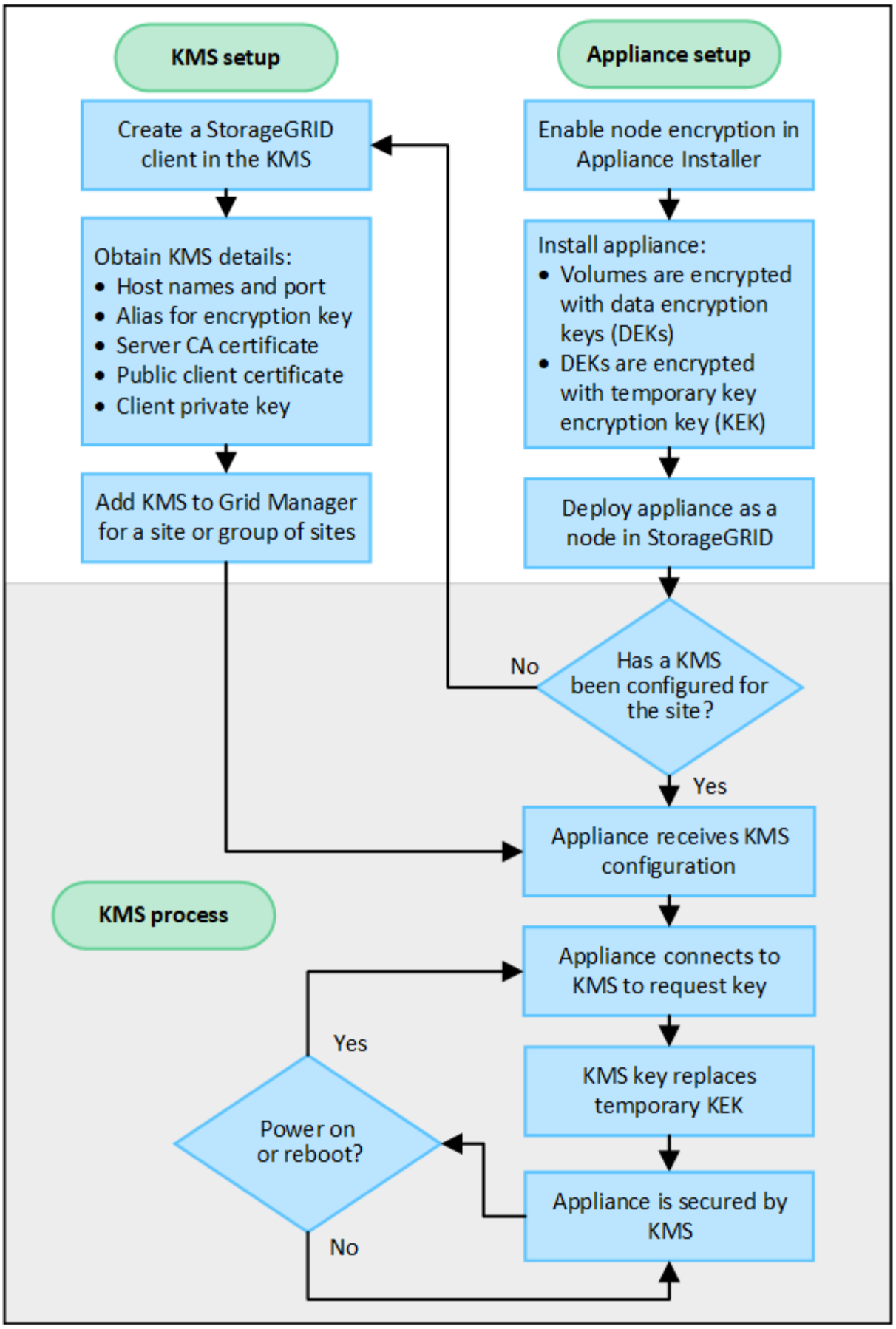
インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバ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設定の概要

キー管理サーバ（ 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 サーバを設定して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 つの設定タスクを完了しておく必要があります。これらの 2 つの設定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。

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 データを保護する手順の概要を示しています。



フローチャートには、 KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、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後にキー管理サーバをセットアップできます。

キー管理サーバ（ KMS ）のセットアップ

キー管理サーバのセットアップには、主に次の手順が含まれます。

ステップ	を参照してください
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。	"KMS でクライアントとして StorageGRID を設定します"
KMS で StorageGRID クライアントの必要な情報を入手します。	"KMS でクライアントとして StorageGRID を設定します"
Grid Manager に KMS を追加して 1 つ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 の設定を保存します。	"キー管理サーバ（ KMS ）を追加する"

アプライアンスをセットアップします

KMS を使用するためにアプライアンスノードをセットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、 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したあとに* Node Encryption *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。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（ DEK ）が割り当てられます。
   - DEK は、各ボリュームのデータの暗号化に使用されます。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、変更することはできません。
   - 各 DEK は、 KEK （ Master Key Encryption Key ）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

を参照してください "ノード暗号化を有効にします" を参照してください。

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの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 設定が存在するかどうかを確認します。

- KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
- KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、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たままになります。

2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、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から設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、 KMS に接続してキーを要求します。揮発性メモリに保存されているキーは、電源の喪失や再起動に耐えられません。

キー管理サーバを使用する際の考慮事項と要件

外部キー管理サーバ（ KMS ）を設定する前に、考慮事項と要件を確認しておく必要があります。

サポートされている**KMIP**のバージョンを教えてください。

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

"Key Management Interoperability Protocol （キー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

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol （ KMIP ）の通信に使用す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に、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

サポートされている**TLS**のバージョンを教えてください。

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRIDでは、KMSまたはKMSクラスタへのKMIP接続を確立する際に、どのKMSがサポートしているかに基づいて、TLS 1.2またはTLS 1.3のいずれかのプロトコルをサポートできます。 "TLSおよびSSHポリシー" を使用しています。

StorageGRIDは、接続時にプロトコルと暗号（TLS 1.2）または暗号スイート（TLS 1.3）をKMSとネゴシエートします。使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（* configuration > Security * Security settings *）。

サポートされているアプライアンスはどれですか。

キー管理サーバ（ KMS ）を使用して、「ノード暗号化 * 」が有効になっているグリッド内の 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てアプライアンスをインストールするハードウェア構成の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したあとに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できません。

StorageGRID アプライアンスおよびアプライアンスノードに対して設定したKMSを使用できます。

次のようなソフトウェアベース（アプライアンス以外）のノードでは、設定されたKMSを使用できません。

- 仮想マシン（ VM ）として導入されたノード
- Linux ホストのコンテナエンジン内に導入されたノード

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

キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

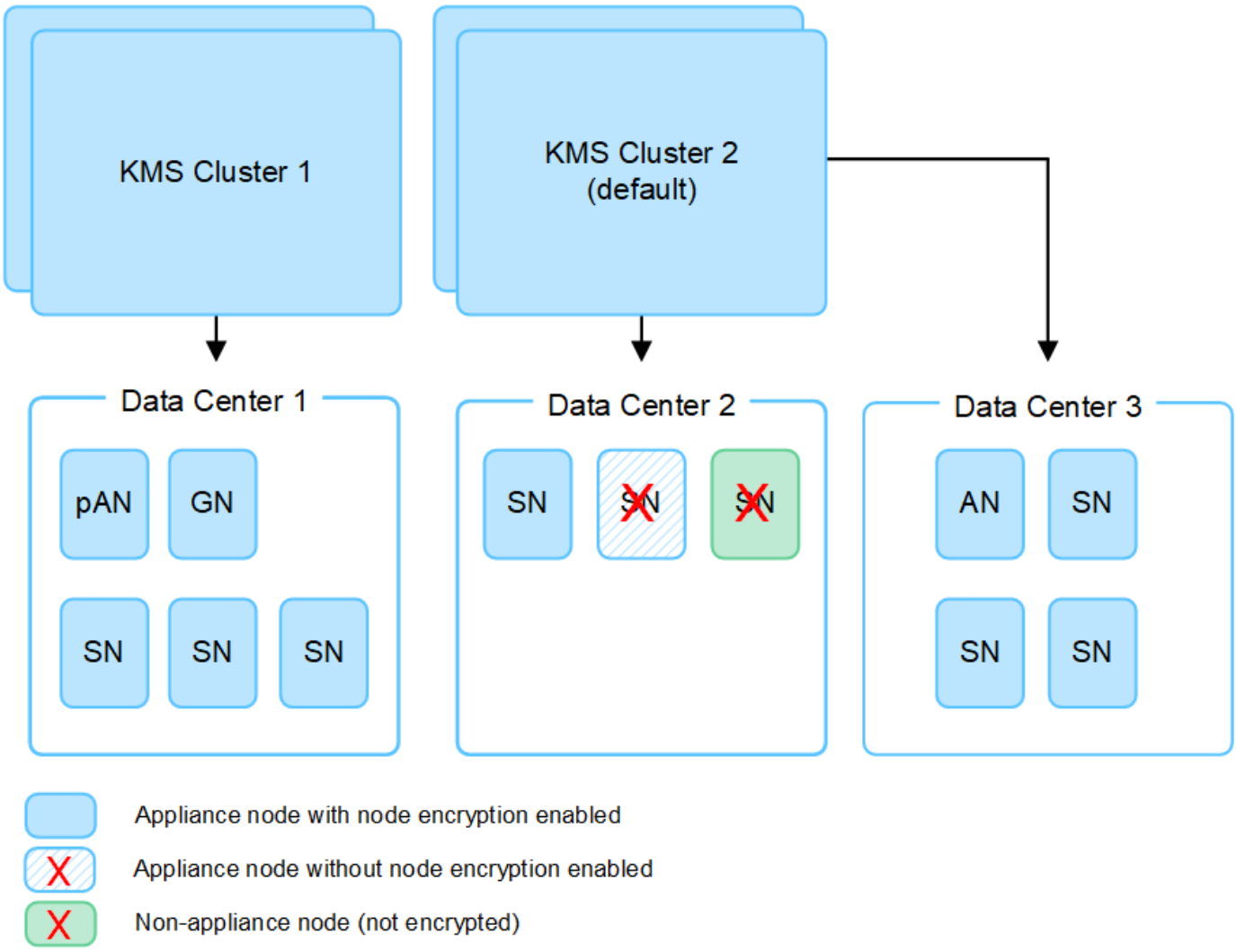
必要なキー管理サーバの数

1 つ以上の外部キー管理サーバを設定して、 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できます。各 KMS は、 1 つ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に単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、 KMS クラスタをキー管理に使用することを推奨します。

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 クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノード、またはインストール時に* Node Encryption *設定が有効になっていないアプライアンスノードには、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どうなりますか。

セキュリティのベストプラクティスとして、定期的に "暗号化キーのローテーション" 設定された各KMSで使用されます。

新しいキーバージョンが利用可能になった場合：

- このサービスは、 KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が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アプライアンスノードがオフラインになっている場合、ノードはリブート後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バージョンのキー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 encryption key rotation failed *アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあと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、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRID アプライアンスインストーラを使用してを実行できます "KMS構成をクリアします"。KMS

の設定をクリアすると、「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 設定の間の関連付けが解除されます。

KMS 暗号化キーにアクセスできないため、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、永続的にロックされます。

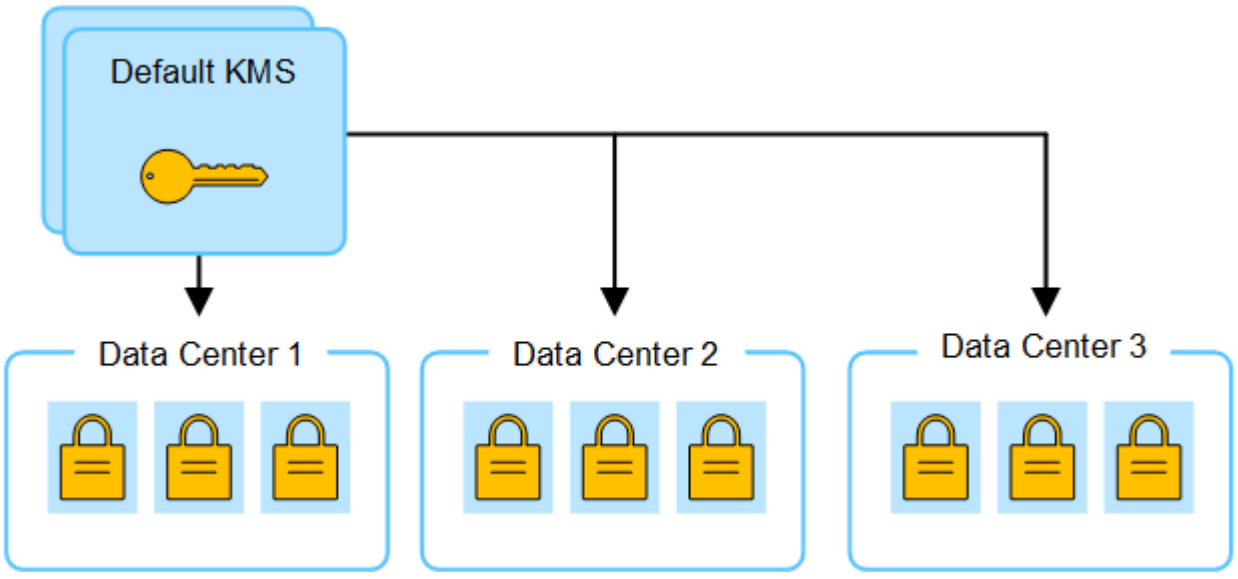
サイトの **KMS** を変更する際の考慮事項

各キー管理サーバ（ KMS ）または KMS クラスタは、 1 つ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。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

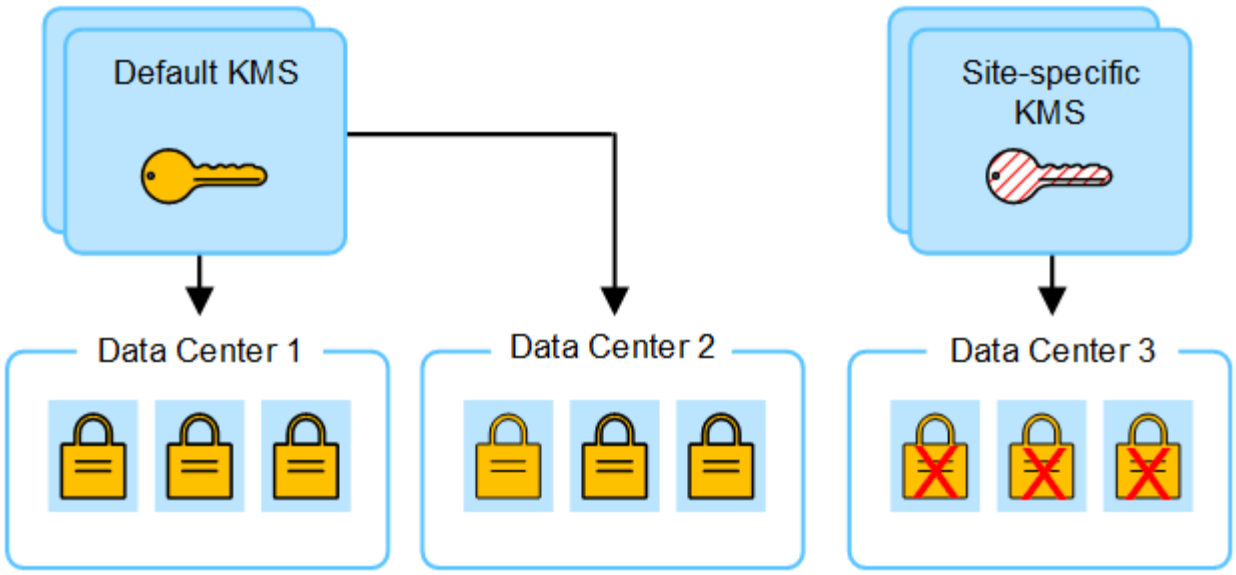
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

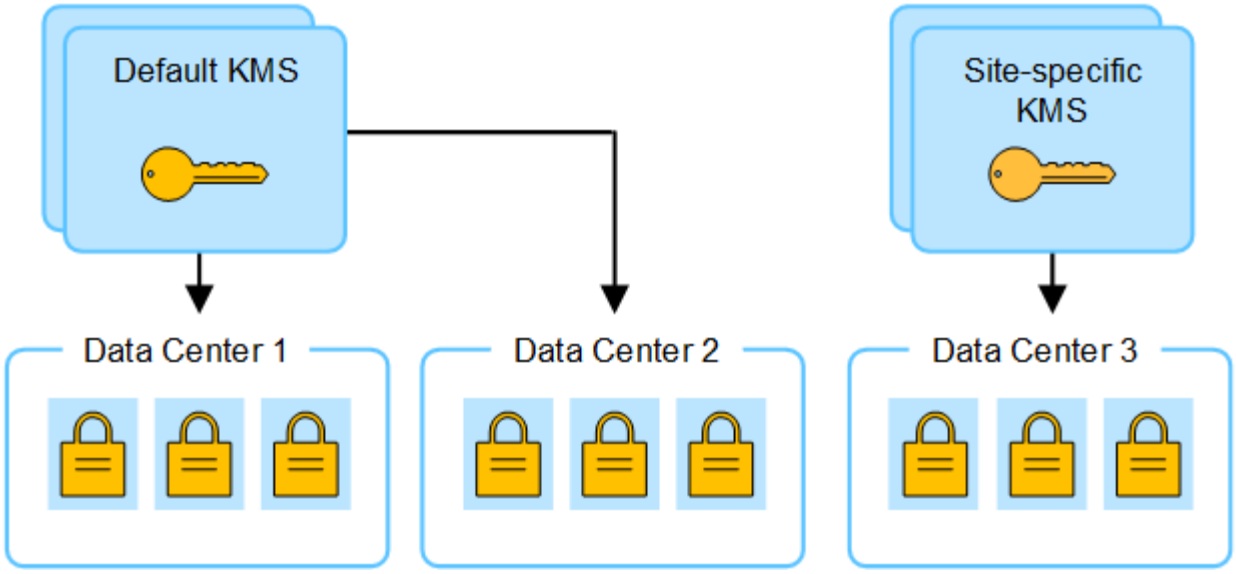
1. 最初に、専用のKMSを持たないすべてのサイトを環境 するデフォルトKMSを構成します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。



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 の設定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、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。



4. 問題 に対応するには、現在のバージョンの暗号化キーをデフォルトの 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。元のキーが新しいキーの前のバージョンになります）。 サイト固有の KMS に、データセンター 3 で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付与されるようになり、 StorageGRID に保存できるようになりました。



サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

サイトの **KMS** を変更するユースケース	必要な手順
サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。	サイト固有の KMS を編集します。[* キー管理対象 *] フィールドで、別の KMS （デフォルト KMS ）で管理されていないサイト * 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。それは専用のKMSを持っていないすべてのサイトに適用されます。 "キー管理サーバ（ KMS ）を編集する"
デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトのKMSを使用しないでください。	1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。 2. Grid Manager 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（ KMS ）を追加する"
サイトの KMS で別のサーバを使用するとします。	1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。 2. Grid Manager を使用して既存の KMS 設定を編集し、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（ KMS ）を追加する"

KMS でクライアントとして StorageGRID を設定します

KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

これらの手順は、タレスCipherTrust Managerと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、 "ネットアップの Interoperability Matrix Tool （ IMT ）"。

手順

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

   各 KMS は、 1 つ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。KMSまたはKMSクラスタごとに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にキーを作成してもらいます。次の後に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. KMS または KMS クラスタごとに次の情報を記録します。

   KMSをStorageGRIDに追加するときは、次の情報が必要です。

   - 各サーバのホスト名または 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. KMS または KMS クラスタごとに、認証局（ CA ）が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

   サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

   - 証明書では、 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。
   - 各サーバ証明書の Subject Alternative Name （ 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 アドレスを含める必要があります。

     StorageGRID で KMS を設定する場合は、「 * Hostname * 」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。

   - サーバ証明書は、 KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。

5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

   クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

キー管理サーバ（ **KMS** ）を追加する

StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

作業を開始する前に

- を確認しておきます "キー管理サーバを使用する際の考慮事項と要件"。
- これで完了です "KMS でクライアントとして StorageGRID を設定"をクリックし、 KMS または KMS クラスタごとに必要な情報を確認しておきます。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセス権限"。

このタスクについて

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化された

すべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、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。を参照してください "サイトの KMS を変更する際の考慮事項" を参照してください。

ステップ**1**：**KMS**の詳細

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

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [設定の詳細]タブが選択された状態で、[キー管理サーバ]ページが表示されます。

2. 「 * Create * 」を選択します。

   キー管理サーバの追加ウィザードの手順1（KMSの詳細）が表示されます。

3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

フィールド	説明
KMS名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
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 文字で指定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要求されます。
のキーを管理します	この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。 • 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。 • 専用のKMSを持たないサイトや、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KMSを設定するには、*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。 ◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。

フィールド	説明
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力する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 クラスタ内のすべてのサーバに接続できなくなります。

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

手順**2:**サーバー証明書をアップロードします

キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）で、KMSのサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

手順

1. [手順2（サーバ証明書のアップロード）]*で、保存されているサーバ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は、各証明書のメタデータが独自のタブに表示されます。

3. 「 * Continue * 」を選択します。

手順**3**：クライアント証明書をアップロードします

キー管理サーバ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、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

1. ステップ3（クライアント証明書のアップロード）*で、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鍵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でキーを作成するように求めるメッセージが表示されます。

キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

> KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. を選択したときに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、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返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設定を保存する必要がある場合は、*[強制保存]*を選択します。

   > [Force save]*を選択すると、KMSの構成が保存されますが、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。構成を含む問題 がある場合、該当す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リブートできない可能性があります。問題が解決す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、設定を強制的に保存する場合は、「 * OK 」を選択します。

   KMS の設定は保存されますが、 KMS への接続はテストされません。

KMSの管理

キー管理サーバ（KMS）の管理には、詳細の表示と編集、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。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "必要なアクセス権限"。

KMS の詳細を確認します

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

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページに次の情報が表示されます。

   - [Configuration details]タブには、設定済みのキー管理サーバが表示されます。
   - [Encrypted nodes]タブには、ノード暗号化が有効になっているノードが表示されます。

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
のキーを管理します	KMS に関連付けられている 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 （デフォルト KMS ）で管理されていないサイト * 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 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。 例： `10.10.10.10 and 10.10.10.11` または `10.10.10.10 and 2 others`。 クラスタ内のすべてのホスト名を表示するには、KMSを選択して*または[アクション]>[編集]*を選択します。

3. KMSの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。

タブをクリックする	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付と時刻。	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、有効期限の日時、証明書PEMなど）。	証明書PEM	証明書のPEM（Privacy Enhanced Mail）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、有効期限の日時、証明書PEMなど）。

4. 組織のセキュリティ対策で必要に応じて、*[Rotate key]*を選択するか、KMSソフトウェアを使用してキーの新しいバージョンを作成します。

   キーのローテーションが成功すると、[Key UID]フィールドと[Last modified]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、最後に使用したバージョンのキーから新しいバージョンの同じキーにローテーションします。完全に別の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、キーの回転を試みないでください。StorageGRID では、以前に使用されていたすべてのキーバージョン（および今後使用するすべてのバージョン）に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。

証明書を管理します

サーバ証明書またはクライアント証明書の問題に迅速に対処します。可能であれば、有効期限が切れる前に証明書を交換してください。

データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。
2. 表で、KMSごとの証明書有効期限の値を確認します。
3. 任意のKMSの証明書の有効期限が不明な場合は、30分ほど待ってから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に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、サーバー証明書ではなく*クライアント証明書*を選択します。
5. 「* kms CA certificate expiration 」、「 kms client certificate expiration 」、「 kms server certificate expiration *」の各アラートがトリガーされたら、各アラートの概要 をメモして推奨される対処方法を実行します。

証明書の有効期限の更新がStorageGRIDで取得されるまでに30分ほどかかることがあります。現在の値を確認するには、Webブラウザをリフレッシュしてください。

暗号化されたノードを表示する

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

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべてのキー管理サーバが表示されます。

2. ページの上部で、*[暗号化されたノード]*タブを選択します。

[Encrypted nodes]タブには、*[Node Encryption]*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が表示されます。

3. 各アプライアンスノードについて、表の情報を確認します。

列（ **Column** ）	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。 Storage 、 Admin 、または Gateway 。
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名	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、[Configuration details]タブを選択してKMSを追加します。 "キー管理サーバ（ KMS ）を追加する"
キー UID	アプライアンスノードでデータの暗号化と復号化に使用す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、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。
ステータス	KMS とアプライアンスノード間の接続のステータス。ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。 *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 問題 と表示されている場合は、問題 にすぐに対処してください。

   通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が（意図的に停止しているか不明である）と表示されます。

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

   - KMS の設定をロードできませんでした
   - 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 キーでアプライアンスボリュームを復号化できませんでした
   - KMS は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対処方法を実行します。

問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

KMSの編集

証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

作業を開始する前に

- KMS 用に選択したサイトを更新する予定がある場合は、を確認してください "サイトの KMS を変更する際の考慮事項"。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセス権限"。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

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

   テーブルで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名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
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 文字で指定する必要があります。 キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、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ている場合は、キー名を編集する必要があります。
のキーを管理します	サイト固有のKMSを編集していて、まだデフォルトKMSを持っていない場合は、オプションで*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。このオプションを選択すると、サイト固有のKMSがデフォルトのKMSに変換されます。これは、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:*サイト固有のKMSを編集している場合、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、特定のサイトを選択することはできません。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。

フィールド	説明
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力する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 クラスタ内のすべてのサーバに接続できなくなります。

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

   [キー管理サーバの編集]ウィザードの手順2（サーバ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. 「 * Continue * 」を選択します。

   [Edit a Key Management Server]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）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鍵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。

   キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテストします。すべてのノード接続が有効で、 KMS に正しいキーがある場合は、キー管理サーバが Key Management Server ページの表に追加されます。

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 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テストに失敗した場合は、「 422 ： Unprocessable Entity 」というエラーが表示されます。

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

    [Force save]*を選択すると、KMSの構成が保存されますが、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。構成を含む問題 がある場合、該当す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リブートできない可能性があります。問題が解決す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 の設定が保存されます。

12. 確認の警告を確認し、設定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（ **KMS** ）を削除する

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイトの運用を停止した場合は、サイト固有の KMS を削除できます。

作業を開始する前に

- を確認しておきます "キー管理サーバを使用する際の考慮事項と要件"。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセス権限"。

このタスクについて

KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに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なアプライアンスノードがあるサイトごとにサイト固有の 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. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

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

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

3. 次の条件に該当することを確認します。
   - アプライアンスノードでノード暗号化が有効になっていないサイトのサイト固有のKMSを削除する場合。
   - デフォルトのKMSを削除しようとしていますが、ノード暗号化を使用して各サイトにサイト固有のKMSがすでに存在しています。
4. 「 * はい * 」を選択します。

   KMS の設定は削除されます。

プロキシ設定を管理します

ストレージプロキシの設定

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の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、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へプラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

設定されている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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。

このタスクについて

設定できるストレージプロキシは1つです。

手順

1. [* 設定 * > * セキュリティ * > * プロキシ設定 *] を選択します。
2. 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、プロキシサーバへの接続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）を使用する場合は、このフィールドを空白のままにします。

6. [保存（ Save ）] を選択します。

   ストレージプロキシが保存されたら、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設定およびテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連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。

管理プロキシの設定

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）の間に非透過型プロキシサーバを設定できます。

AutoSupportの詳細については、を参照してください。 "AutoSupport を設定します"。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。

このタスクについて

単一の管理プロキシの設定を行うことができます。

手順

1. [* 設定 * > * セキュリティ * > * プロキシ設定 *] を選択します。

   [Proxy Settings]ページが表示されます。デフォルトでは、タブメニューで[Storage]が選択されています。

2. [Admin]*タブを選択します。
3. [Enable Admin Proxy]*チェックボックスをオンにします。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシサーバのユーザ名とパスワードを入力します。

   プロキシサーバでユーザ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、*[証明書の確認]*を選択します。管理プロキシサーバから提示されたSSL証明書の信頼性を確認するには、CAバンドルをアップロードしてください。

     プロキシ証明書が検証されている場合、StorageGRID On Demand、E-Series AutoSupport Through StorageGRID、およびAutoSupportの[Upgrade]ページでの更新パスの決定が機能しません。

     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との通信時に証明書を検証しない場合は、*[証明書を検証しない]*を選択します。

8. [保存（ Save ）] 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の間にプロキシサーバが設定されます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

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します

外部ファイアウォールでアクセスを制御します

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できます。

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、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ができます。

StorageGRID 内部ファイアウォールを設定する場合は、を参照してください "内部ファイアウォールを設定します"。

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 ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、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 Grid Manager 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 Grid Manager とグリッド管理 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、Tenant Managerまたはテナント管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。
ポート 1	管理ノード上の制限された Tenant Manager 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 Tenant Manager 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、Grid Managerまたはグリッド管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

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

- "Grid Manager にサインインします"
- "テナントアカウントを作成する"
- "外部との通信"

内部ファイアウォールコントロールを管理します

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、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、特定のグリッド環境に必要なポートを除くすべてのポートでネットワークアクセスを禁止します。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

Firewallコントロールページの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、選択したポートへのアクセスを許可します。[Manage external access]タブを使用して閉じ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るか、以前閉じていたポートを再度開きます。
- 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インバウンド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]タブの設定よりも優先されます。

  - 信頼されていないクライアントネットワークを使用するノードは、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）の接続のみを受け入れます。
  - ロードバランサエンドポイントのポート_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で唯一開いているポート_です。
  - 信頼されている場合は、[Manage external access]タブで開いたすべてのポートおよびクライアントネットワークで開いているロードバランサエンドポイントにアクセスできます。

> あるタブで行った設定は、別のタブで行ったアクセス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確認して、ネットワークが想定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コントロールを設定するには、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"。

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、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します"。

[Privileged address list]タブと**[Manage external access]**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を許可する1つ以上のIPアドレスを登録できます。[Manage external access]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（デフォルトではグリッド以外のノードからアクセス可能なポート）への外部アクセスを閉じることができます。多くの場合、この2つのタブを一緒に使用して、グリッドに必要な正確なネットワークアクセスをカスタマイズできます。

> 特権IPアドレスには、デフォルトで内部グリッドポートへのアクセスはありません。

例**1:**メンテナンスタスクにジャンプホストを使用します

ネットワーク管理にジャンプホスト（セキュリティ強化ホスト）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. [Manage external access]タブを使用して、すべてのポートをブロックします。

> ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分の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にアクセスできません。

設定を保存すると、グリッド内の管理ノード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。これにより、ジャンプホストを使用して、グリッドでより安全にメンテナンスタスクを実行できるようになります。

例**2**：**Grid Manager**と**Tenant Manager**へのアクセスを制限する

セキュリティ上の理由から、Grid ManagerとTenant Manager（プリセットポート）へのアクセスを制限するとします。次の一般的な手順を使用できます。

1. [Manage external access]タブのトグルを使用して、ポート443をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート8443へのアクセスを許可します。
3. [Manage external access]タブのトグルを使用して、ポート9443へのアクセスを許可します。

設定を保存すると、ホストはポート443にアクセスできなくなりますが、引き続きGrid Managerにはポート8443経由で、Tenant Managerにはポート9443経由でアクセスできます。

ポート443、8443、9443は、Grid ManagerおよびTenant Managerのプリセットポートです。任意のポートを切り替えて、特定のGrid Managerまたはテナントマネージャにアクセスを制限できます。

例**3**：敏感なポートをロックダウンします

機密性の高いポートとそのポート上のサービス（たとえば、ポート22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. サービスへのアクセスを必要とするホストにのみアクセスを許可するには、特権アドレスリストタブを使用します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。

Grid ManagerおよびTenant Managerへのアクセスを割り当てられているポート（事前設定ポートは443および8443）へのアクセスをブロックする前に、権限付きIPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分の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にアクセスできません。

設定を保存すると、特権アドレスリストのホストでポート22とSSHサービスを使用できるようになります。要求の送信元インターフェイスに関係なく、他のすべてのホストはサービスへのアクセスを拒否されます。

例**4**：未使用のサービスへのアクセスを無効にします

ネットワークレベルでは、使用する予定のない一部のサービスを無効にすることができます。たとえば、Swiftアクセスを許可しない場合は、次の一般的な手順を実行します。

1. [Manage external access]タブのトグルを使用して、ポート18083をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート18085をブロックします。

設定を保存すると、ストレージノードでSwift接続は許可されなくなりますが、ブロックされていないポートで他のサービスへのアクセスは引き続き許可されます。

[信頼されていないクライアントネットワーク]タブ

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 はデフォルトで、すべてののグリッドノードへのインバウンド接続を信頼します "使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「 *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。を参照してください "ロードバランサエンドポイントを設定する" および "ファイアウォールコントロールを設定します"。

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. から "ロードバランサエンドポイント" ページで、HTTPS経由のS3用のロードバランサエンドポイントをポート443に設定します。
2. [Firewall control]ページで、[Untrusted]を選択して、ゲートウェイノードのクライアントネットワークを信頼されていないネットワークとして指定します。

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は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。

- [Firewall]制御ページの[Untrusted Client Networks]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、設定されているプラットフォームサービスのデスティネーションへのアウトバウンド要求は引き続き許可します。

例**3**：**Grid Manager**へのアクセスをサブネットに制限する

Grid Managerに特定のサブネットに対するアクセスのみ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. [Untrusted Client Network]タブを使用して、クライアントネットワークを信頼されていないものとして設定します。
3. 管理インターフェイスのロードバランサエンドポイントを作成する場合は、「port」と入力し、ポートからアクセスする管理インターフェイスを選択します。
4. 信頼されていないクライアントネットワークについては*[はい]*を選択します。
5. [Manage external access]タブを使用して、すべての外部ポートをブロックします（サブネット外のホス

トに対して特権IPアドレスが設定されているかどうかに関係なく）。

設定を保存すると、指定したサブネットのホストだけがGrid Managerにアクセスできるようになります。他のすべてのホストはブロックされます。

内部ファイアウォールを設定します

StorageGRID ノードの特定のポートへのネットワークアクセスを制御するようにStorageGRID ファイアウォールを設定できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。
- の情報を確認しておきます "ファイアウォールコントロールを管理します" および "ネットワークのガイドライン"。
- 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。

> クライアントネットワークの設定を変更する際、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ことがあります。

このタスクについて

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用して、グリッドのノードの一部のポートを開いたり閉じたりできます。[Firewall]制御タブを使用して、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できます。閉じ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インバウンドトラフィックを信頼するかどうかを指定できます。また、クライアントネットワークの特定のポートへのアクセスを設定できます。

グリッドの外部のIPアドレスに対して開くポートの数を絶対に必要なポートだけに制限すると、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コントロールタブのそれぞれの設定を使用して、必要なポートだけが開いていることを確認します。

ファイアウォールコントロールの使用方法（例を含む）の詳細については、を参照してください "ファイアウォールコントロールを管理します"。

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、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します"。

ファイアウォールコントロールにアクセスします

手順

1. * configuration > Security > Firewall control *を選択します。

   このページの3つのタブについては、を参照してください "ファイアウォールコントロールを管理します"。

2. 任意のタブを選択して、ファイアウォールコントロールを設定します。

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設定では、他のタブで実行できる操作は制限されません。ただし、1つのタブで設定を変更すると、他のタブで設定されたポートの動作が変更される可能性があります。

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アクセスをホストに許可します。

権限付きIPアドレスとサブネットには、デフォルトで内部のグリッドアクセスはありません。また、[Manage external access]タブでブロックされていても、ロードバランサエンドポイントと、[Privileged address list]タブで開いている追加のポートにアクセスできます。

[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することはできません。

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、*[Add another IP address or subnet in CIDR notation]*を選択して、権限付きクライアントを追加します。

   特権リストにできるだけ少ないアドレスを追加します。

3. 必要に応じて、*[特権IPアドレスによるStorageGRID 内部ポートへのアクセスを許可する]*を選択します。を参照してください "StorageGRID の内部ポート"。

   このオプションを使用すると、内部サービスの保護が一部解除されます。可能であれば無効のままにしておきます。

4. [保存（ Save ）] を選択します。

外部アクセスの管理

[Manage external access]タブでポートを閉じると、特権アドレスリストにIPアドレスを追加しないかぎり、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だけです。また、閉じたポートのみを開くことができます。

[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することはできません。たとえば、ノードが信頼されていない場合、クライアントネットワークでポートSSH/22が[外部アクセスの管理]タブで開いていてもブロックされます。[Untrusted Client Network]タブの設定は、クライアントネットワークの閉じているポート（443、8443、9443など）よりも優先されます。

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（デフォルトではグリッド以外のノードからアクセス可能なポート）が表示されます。
2. 次のオプションを使用して、開いたり閉じたりするポートを設定します。

- 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。
- 表に示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の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。

> テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのポートが表示されていることを確認します。検索フィールドを使用して、ポート番号を入力して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（ Save ）] を選択します

Untrusted Client Networkの略

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設定されたポート、およびオプションでこのタブで選択した追加のポートでのみインバウンドトラフィックを受け入れます。このタブを使用して、拡張時に追加する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。

タブで設定を変更すると、[外部アクセスの管理]*タブの設定が上書きされます。

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. [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際のデフォルト設定を指定します。
   - * Trusted *（デフォルト）：拡張でノードを追加すると、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. 次のオプションを使用して、明示的に設定されたロードバランサエンドポイントまたは選択した追加の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します。
   - テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストに追加するには、*[表示されたノードで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。

- テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストから削除するには、*[表示されたノードで信頼する]*を選択します。
- 各ノードの横にある切り替えボタンを使用して、選択したノードのクライアントネットワークを[Trusted]または[Untrusted]に設定します。

  たとえば、*表示されているノードで[Untrust on displayed nodes]*を選択してすべてのノードを[Untrusted Client Network]リストに追加し、個 々 のノードの横にある切り替えを使用してその1つのノードを[Trusted Client Network]リストに追加できます。

テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのノードが表示されていることを確認します。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、名前に文字列「gw」を含むすべてのノードが表示されます。

4. [保存（ Save ）] を選択します。

   新しいファイアウォール設定がすぐに適用され、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。

著作権に関する情報

商標に関する情報