



サーバ証明書の設定 StorageGRID

NetApp
October 03, 2025

目次

サーバ証明書の設定	1
サポートされているカスタムサーバ証明書のタイプ	1
ロードバランサエンドポイントの証明書	1
Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する	1
Grid ManagerおよびTenant Manager用のデフォルトのサーバ証明書のリストア	3
ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する	3
S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書のリストア	4
StorageGRID システムのCA証明書をコピーしています	5
FabricPool 用のStorageGRID 証明書を設定しています	6
管理インターフェイス用の自己署名サーバ証明書の生成	7

サーバ証明書の設定

StorageGRID システムで使用されるサーバ証明書をカスタマイズできます。

StorageGRID システムは、用途が異なる複数のセキュリティ証明書を使用します。

- 管理インターフェイスのサーバ証明書：Grid Manager、Tenant Manager、Grid管理API、およびテナント管理APIへのアクセスを保護するために使用します。
- ストレージAPIのサーバ証明書：ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、API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。

インストール時に作成されたデフォルトの証明書を使用できるほか、デフォルトの証明書のいずれか、または両方を独自のカスタム証明書に置き換えることもできます。

サポートされているカスタム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サーバ証明書がサポートされます。

StorageGRID でREST APIのクライアント接続を保護する方法の詳細については、S3またはSwiftの実装ガイドを参照してください。

ロードバランサエンドポイントの証明書

StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、ロードバランサエンドポイントの設定手順を参照してください。

関連情報

["S3 を使用する"](#)

["Swift を使用します"](#)

["ロードバランサエンドポイントの設定"](#)

Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する

デフォルトの StorageGRID サーバ証明書を単一のカスタムサーバ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。

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管理ノードに対して使用されるため、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、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ブラウザにルート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 アラートと**Legacy Management Interface Certificate Expiry (MCEP)** アラームの両方がトリガーされます。必要に応じて、Support > Tools > Grid Topology を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「*_ primary Admin Node_* CMN > Resources *」を選択します。



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サーバ証明書の有効期限が切れます。
- カスタムの管理インターフェイスサーバ証明書をデフォルトのサーバ証明書に戻した場合。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Management Interface Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 必要なサーバ証明書ファイルをアップロードします。
 - サーバー証明書：カスタムサーバー証明書ファイル (.crt) 。
 - * Server Certificate Private Key *：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。
4. [保存 (Save)] をクリックします。

以降すべての新しい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。

タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。



新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

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。

Grid ManagerおよびTenant Manager用のデフォルトのサーバ証明書のリストア

Grid ManagerおよびTenant Managerでデフォルトのサーバ証明書を使用するように戻すことができます。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Manage Interface Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

デフォルトのサーバ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、デフォルトのサーバ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。

ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する

ストレージノードまたはゲートウェイノード上のCLBサービス（廃止）へのS3またはSwiftクライアント接続に使用するサーバ証明書は、置き換えることができます。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あります。

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、ユーザがシステムへのアクセスに使用するS3またはSwift APIクライアントにルート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、Expiration of server certificate for Storage API Endpoints アラートと、ルートサーバ証明書の有効期限が近づくとき従来の**Storage API Service Endpoints Certificate Expiry (SCEP)** アラームの両方がトリガーされます。必要に応じて、「Support Tools * Grid Topology *」を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「*_ primary Admin Node_ CMN * Resources *」を選択します。

カスタム証明書は、クライアントがゲートウェイノード上の廃止されたCLBサービスを使用してStorageGRIDに接続する場合、またはクライアントがストレージノードに直接接続する場合にのみ使用されます。管理ノードまたはゲートウェイノード上のロードバランササービスを使用してStorageGRIDに接続するS3またはSwiftクライアントは、ロードバランサエンドポイント用に設定された証明書を使用します。



*ロードバランサエンドポイント証明書の有効期限*アラートは、まもなく期限切れになるロードバランサエンドポイントに対してトリガーされます。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 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 (.crt) 。
 - * Server Certificate Private Key *：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。
4. [保存 (Save)] をクリックします。

以降すべての新しいAPI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。

タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。



新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

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。

関連情報

["S3 を使用する"](#)

["Swift を使用します"](#)

["S3 APIエンドポイントのドメイン名を設定しています"](#)

S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書のリストア

S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書を使用する設定に戻すことができます。

手順

1. [* Configuration]>[Network Settings]>[Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

オブジェクトストレージAPIエンドポイント用のデフォルトサーバ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APIクライアント接続には、デフォルトのサーバ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。

StorageGRID システムのCA証明書をコピーしています

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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

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]>[Network Settings]>[Server Certificates*]を選択します。
2. [内部CA証明書 (* Internal CA Certificate *)]セクションで、すべての証明書テキストを選択します。

を含める必要があります -----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- を選択します。



ゲートウェイノード上の別の Connection Load Balancer (CLB) サービスは廃止され、FabricPool での使用は推奨されなくなりました。

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CAバンドルのアップロードを求めるプロンプトが表示されます。

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。

関連情報

["StorageGRID for FabricPool を設定します"](#)

管理インターフェイス用の自己署名サーバ証明書の生成

スクリプトを使用して、ホスト名の厳密な検証が必要な管理APIクライアント用の自己署名サーバ証明書を生成できます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。

このタスクについて

本番環境では、既知の認証局 (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。

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 Grid ManagerおよびTenant Managerで使用される証明書を設定するため。
- 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API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 365
```

出力には、管理APIクライアントに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 * Server Certificates * Management Interface Server Certificate *」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API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。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。