



キー管理サーバの追加 (KMS)

StorageGRID 11.5

NetApp
April 11, 2024

目次

| | |
|---------------------------------|---|
| キー管理サーバの追加 (KMS) | 1 |
| 手順 1 : KMS の詳細を入力します | 1 |
| 手順 2 : サーバ証明書をアップロードする | 4 |
| 手順 3 : クライアント証明書をアップロードする | 5 |

キー管理サーバの追加（KMS）

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。

必要なもの

- を確認しておく必要があります ["キー管理サーバを使用する際の考慮事項と要件"](#)。
- が必要です ["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く必要があります
- Root Access 権限が必要です。
- 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。

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。

["サイトの KMS を変更する際の考慮事項"](#)

手順

1. ["手順 1：KMS の詳細を入力します"](#)
2. ["手順 2：サーバ証明書をアップロードする"](#)
3. ["手順 3：クライアント証明書をアップロードする"](#)

手順 1：KMS の詳細を入力します

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

手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

[Key Management Server] ページが表示され、[Configuration] [Details] タブが選択されます。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

| KMS Display Name | Key Name | Manages keys for | Hostname | Certificate Status |
|--|----------|------------------|----------|--------------------|
| No key management servers have been configured. Select Create. | | | | |

2. 「* Create *」を選択します。

Add a Key Management Server (キー管理サーバの追加) ウィザードの手順 1 (KMS の詳細を入力) が表示されます。

Add a Key Management Server

1 Enter KMS Details 2 Upload Server Certificate 3 Upload Client Certificates

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name

Key Name

Manages keys for

Port

Hostname

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 表示名 | 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。 |
| のキーを管理します | <p>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。</p> <ul style="list-style-type: none"> 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。 「* Sites not managed by another KMS (デフォルト KMS) *」を選択して、専用の KMS とその後の拡張で追加したサイトに適用されるデフォルトの KMS を設定します。 <ul style="list-style-type: none"> 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。 |
| ホスト名 | <p>KMS の完全修飾ドメイン名または IP アドレス。</p> <ul style="list-style-type: none"> 注：* サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。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。 |

- KMS クラスタを使用している場合は、プラス記号を選択します **+** クラスタ内の各サーバのホスト名を追加します。
- 「* 次へ *」を選択します。

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）が表示されます。

手順 2 : サーバ証明書をアップロードする

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）* から、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。

Add a Key Management Server

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate

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。

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ k170vCA.pem

Server Certificate Metadata

```
Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79
```

Cancel

Back

Next



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. 「* 次へ *」を選択します。

Add a Key Management Serverウィザードの手順3（クライアント証明書をアップロード）が表示されません。

手順 3 : クライアント証明書をアップロードする

キー管理サーバの追加ウィザードの手順3（クライアント証明書をアップロード）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. * 手順3（クライアント証明書をアップロード）* から、クライアント証明書の場所を参照します。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate 

Client Certificate Private Key 

Cancel

Back

Save

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。

クライアント証明書とクライアント証明書の秘密鍵のメタデータが表示されます。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate  k170vClientCert.pem

```
Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69
```

Client Certificate Private Key  k170vClientKey.pem

Cancel

Back

Save

5. [保存 (Save)] を選択します。

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. 「* Save * (保存)」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。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ⓘ k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ⓘ k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



[強制保存] を選択すると KMS の設定が保存されますが、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。

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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。

著作権に関する情報

Copyright © 2024 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。