機能と統合を展開する

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

目次

機能と統合を展開する

BeeGFS CSI ドライバー

BeeGFS v8のTLS暗号化を設定する

BeeGFS v8 管理サービスとクライアント間の通信を保護するために TLS 暗号化を構成します。

概要

BeeGFS v8では、管理ツール（ `beegfs`コマンドラインユーティリティなど）とBeeGFSサーバーサービス（ManagementやRemoteなど）間のネットワーク通信を暗号化するためのTLSサポートが導入されました。このガイドでは、3つのTLS設定方法を使用して、BeeGFSクラスターでTLS暗号化を設定する方法について説明します：

- 信頼できる証明機関の使用： BeeGFS クラスターで既存の CA 署名証明書を使用します。
- ローカル認証局の作成： ローカル認証局を作成し、それを使用してBeeGFSサービスの証明書に署名します。このアプローチは、外部CAに依存せずに独自の信頼チェーンを管理したい環境に適しています。
- **TLS** 無効： 暗号化が不要な環境やトラブルシューティングを行う場合は、TLS を完全に無効にしてください。内部ファイルシステムの構造や設定に関する機密情報が平文で公開される可能性があるため、この方法は推奨されません。

環境と組織のポリシーに最適な方法を選択してください。詳細については、"BeeGFS TLS"ドキュメントを参照してください。

> ⓘ `beegfs-client`サービスを実行しているマシンでは、BeeGFS ファイルシステムをマウントするために TLS は必要ありません。BeeGFS CLI や、リモートや同期などの他の beegfs サービスを利用するには、TLS を設定する必要があります。

信頼できる証明機関の使用

信頼できる証明機関（CA）によって発行された証明書（社内のエンタープライズ CA またはサードパーティプロバイダーの CA）にアクセスできる場合は、自己署名証明書を生成する代わりに、これらの CA 署名証明書を使用するように BeeGFS v8 を構成できます。

新しい **BeeGFS v8** クラスターのデプロイ

新しい BeeGFS v8 クラスターのデプロイメントでは、Ansible インベントリの `user_defined_params.yml`ファイルを設定して CA 署名付き証明書を参照します：

```
beegfs_ha_tls_enabled: true

beegfs_ha_ca_cert_src_path: files/beegfs/cert/ca_cert.pem

beegfs_ha_tls_cert_src_path: files/beegfs/cert/mgmtd_tls_cert.pem

beegfs_ha_tls_key_src_path: files/beegfs/cert/mgmtd_tls_key.pem
```

`beegfs_ha_tls_config_options.alt_names`が空でない場合、Ansibleは指定されたalt_namesを証明書のサブジェクト別名（SAN）として使用し、自己署名TLS証明書と鍵を自動的に生成します。 `beegfs_ha_tls_cert_src_path`および`beegfs_ha_tls_key_src_path`で指定された独自のカスタムTLS証明書と鍵を使用するには、`beegfs_ha_tls_config_options`セクション全体をコメントアウトするか削除する必要があります。そうしないと、自己署名証明書の生成が優先され、カスタム証明書と鍵は使用されません。

既存の **BeeGFS v8** クラスターの構成

既存の BeeGFS v8 クラスターの場合は、BeeGFS 管理サービスの設定ファイル内のパスをファイルノードの CA 署名証明書に設定します：

```
tls-cert-file = /path/to/cert.pem
tls-key-file = /path/to/key.pem
```

CA署名証明書を使用した**BeeGFS v8**クライアントの構成

BeeGFS v8クライアントがシステムの証明書プールを使用してCA署名証明書を信頼するように設定するには、各クライアントの設定で tls-cert-file = "" を設定します。システム証明書プールを使用していない場合は、tls-cert-file = <local cert> を設定してローカル証明書へのパスを指定します。この設定により、クライアントはBeeGFS管理サービスによって提示された証明書を認証できるようになります。

ローカル認証局の作成

BeeGFSクラスタ用に独自の証明書インフラストラクチャを構築する場合は、ローカル証明機関（CA）を作成して、BeeGFSクラスタ用の証明書の発行と署名を行うことができます。このアプローチでは、BeeGFS管理サービスの証明書に署名するCAを作成し、署名された証明書をクライアントに配布して信頼チェーンを確立します。以下の手順に従ってローカルCAを設定し、既存または新規のBeeGFS v8クラスタに証明書を展開してください。

新しい **BeeGFS v8** クラスターのデプロイ

BeeGFS v8の新規デプロイメントでは、 `beegfs_8` Ansibleロールがコントロールノード上のローカルCAの作成と、管理サービスに必要な証明書の生成を処理します。これは、Ansibleインベントリの `user_defined_params.yml` ファイルで以下のパラメータを設定することで有効化できます：

```
beegfs_ha_tls_enabled: true

beegfs_ha_ca_cert_src_path: files/beegfs/cert/local_ca_cert.pem

beegfs_ha_tls_cert_src_path: files/beegfs/cert/mgmtd_tls_cert.pem

beegfs_ha_tls_key_src_path: files/beegfs/cert/mgmtd_tls_key.pem

beegfs_ha_tls_config_options:
  alt_names: [<mgmt_service_ip>]
```

`beegfs_ha_tls_config_options.alt_names`が指定されていない場合、Ansibleは指定された証明書/キーパス内の既存の証明書の使用を試みます。

既存の **BeeGFS v8** クラスターの構成

既存のBeeGFSクラスタでは、ローカル証明機関を作成し、管理サービスに必要な証明書を生成することでTLSを統合できます。BeeGFS管理サービスの設定ファイル内のパスを、新しく作成した証明書を指すように更新してください。

このセクションの手順は参考としてご利用ください。秘密鍵と証明書を扱う際には、適切なセキュリティ対策を講じてください。

認証局を作成する

信頼できるマシンに、BeeGFS管理サービスの証明書に署名するためのローカル証明機関（CA）を作成します。CA証明書はクライアントに配布され、信頼関係を確立し、BeeGFSサービスとの安全な通信を可能にします。

次の手順は、RHEL ベースのシステムでローカル認証局を作成するためのリファレンスです。

1. OpenSSL がまだインストールされていない場合はインストールします：

```
dnf install openssl
```

2. 証明書ファイルを保存するための作業ディレクトリを作成します：

```
mkdir -p ~/beegfs_tls && cd ~/beegfs_tls
```

3. CA 秘密キーを生成します：

```
openssl genrsa -out ca_key.pem 4096
```

4. `ca.cnf`という名前の CA 構成ファイルを作成し、識別名フィールドを組織に合わせて調整します：

```
[ req ]
default_bits        = 4096
distinguished_name  = req_distinguished_name
x509_extensions     = v3_ca
prompt              = no

[ req_distinguished_name ]
C  = <Country>
ST = <State>
L  = <City>
O  = <Organization>
OU = <OrganizationalUnit>
CN = BeeGFS-CA

[ v3_ca ]
basicConstraints = critical,CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
```

5. CA証明書を生成します。この証明書はシステムの運用期間中有効である必要があります。有効でない場合は、有効期限が切れる前に証明書を再生成する必要があります。証明書の有効期限が切れると、一部のコンポーネント間の通信が不可能になり、TLS証明書の更新を完了するには通常、サービスの再起動が必要になります。

   次のコマンドは、1 年間有効な CA 証明書を生成します：

```
openssl req -new -x509 -key ca_key.pem -out ca_cert.pem -days 365
-config ca.cnf
```

> この例では、簡潔にするために 1 年間の有効期間を使用していますが、組織のセキュリティ要件に応じて `-days`パラメータを調整し、証明書の更新プロセスを確立する必要があります。

管理サービス証明書を作成する

BeeGFS管理サービス用の証明書を生成し、作成したCAで署名します。これらの証明書は、BeeGFS管理サービスを実行するファイルノードにインストールされます。

1. 管理サービスの秘密キーを生成します：

```
openssl genrsa -out mgmtd_tls_key.pem 4096
```

2. `tls_san.cnf`という名前の証明書構成ファイルを作成し、すべての管理サービス IP アドレスに対してサブジェクト別名（SAN）を設定します：

```
[ req ]
default_bits        = 4096
distinguished_name  = req_distinguished_name
req_extensions      = req_ext
prompt              = no

[ req_distinguished_name ]
C  = <Country>
ST = <State>
L  = <City>
O  = <Organization>
OU = <OrganizationalUnit>
CN = beegfs-mgmt

[ req_ext ]
subjectAltName = @alt_names

[ v3_ca ]
subjectAltName = @alt_names
basicConstraints = CA:FALSE

[ alt_names ]
IP.1 = <beegfs_mgmt_service_ip_1>
IP.2 = <beegfs_mgmt_service_ip_2>
```

識別名フィールドを更新して、CA 構成と `IP.1`および `IP.2`値を管理サービスの IP アドレスと一致させます。

3. 証明書署名要求（CSR）を生成します：

```
openssl req -new -key mgmtd_tls_key.pem -out mgmtd_tls_csr.pem -config
tls_san.cnf
```

4. CA を使用して証明書に署名します（有効期間 1 年）：

```
openssl x509 -req -in mgmtd_tls_csr.pem -CA ca_cert.pem -CAkey
ca_key.pem -CAcreateserial -out mgmtd_tls_cert.pem -days 365 -sha256
-extensions v3_ca -extfile tls_san.cnf
```

組織のセキュリティポリシーに基づいて証明書の有効期間(`-days 365`を調整してください。多くの組織では、1～2年ごとに証明書のローテーションが必要です。

5. 証明書が正しく作成されたことを確認します：

```
openssl x509 -in mgmtd_tls_cert.pem -text -noout
```

Subject Alternative Name セクションにすべての管理 IP アドレスが含まれていることを確認します。

ファイルノードに証明書を配布する

CA 証明書と管理サービス証明書を適切なファイル ノードとクライアントに配布します。

1. CA 証明書と管理サービス証明書およびキーを管理サービスを実行しているファイル ノードにコピーします：

```
scp ca_cert.pem mgmtd_tls_cert.pem mgmtd_tls_key.pem
user@beegfs_01:/etc/beegfs/
scp ca_cert.pem mgmtd_tls_cert.pem mgmtd_tls_key.pem
user@beegfs_02:/etc/beegfs/
```

管理サービスを**TLS**証明書に指定する

BeeGFS 管理サービスの構成を更新して TLS を有効にし、作成された TLS 証明書を参照します。

1. BeeGFS 管理サービスを実行しているファイルノードから、管理サービス構成ファイル（例：`/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`）を編集します。次の TLS 関連パラメータを追加または更新します：

```
tls-disable = false
tls-cert-file = "/etc/beegfs/mgmtd_tls_cert.pem"
tls-key-file = "/etc/beegfs/mgmtd_tls_key.pem"
```

2. 変更を有効にするには、適切なアクションを実行して BeeGFS 管理サービスを安全に再起動してください：

```
systemctl restart beegfs-mgmtd
```

3. 管理サービスが正常に開始されたことを確認します：

```
journalctl -xeu beegfs-mgmtd
```

TLS の初期化と証明書の読み込みが成功したことを示すログエントリを探します。

```
Successfully initialized certificate verification library.
Successfully loaded license certificate: TMP-XXXXXXXXXX
```

BeeGFS v8クライアントのTLSを設定する

BeeGFS 管理サービスとの通信を必要とするすべての BeeGFS クライアントに、ローカル CA によって署名された証明書を作成して配布します。

1. 上記の管理サービス証明書と同じプロセスを使用してクライアントの証明書を生成しますが、Subject Alternative Name（SAN）フィールドにクライアントの IP アドレスまたはホスト名を指定します。
2. クライアントの証明書をクライアントに安全にリモートコピーし、クライアント上で証明書の名前を `cert.pem`に変更します：

```
scp client_cert.pem user@client:/etc/beegfs/cert.pem
```

3. すべてのクライアントで BeeGFS クライアント サービスを再起動します：

```
systemctl restart beegfs-client
```

4. `beegfs CLI`コマンドを実行して、クライアントの接続を確認します。次に例を示します：

```
beegfs health check
```

TLSの無効化

TLSはトラブルシューティングのため、またはユーザーの希望に応じて無効にすることができます。ただし、内部ファイルシステムの構造や設定に関する機密情報が平文で公開される可能性があるため、無効にすることは推奨されません。既存または新規のBeeGFS v8クラスターでTLSを無効にするには、以下の手順に従ってください。

新しい **BeeGFS v8** クラスターのデプロイ

新しい BeeGFS クラスターのデプロイメントでは、Ansible インベントリの `user_defined_params.yml`ファイルで次のパラメーターを設定することで、TLS を無効にしてクラスターをデプロイできます：

```
beegfs_ha_tls_enabled: false
```

既存の **BeeGFS v8** クラスターの構成

既存のBeeGFS v8クラスタの場合は、管理サービスの設定ファイルを編集します。例えば、`/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`のファイルを編集し、以下のように設定します：

```
tls-disable = true
```

変更を有効にするには、適切な処置を行って管理サービスを安全に再起動してください。

著作権に関する情報

商標に関する情報