部署功能和集成

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

目录

部署功能和集成

BeeGFS CSI 驱动程序

为 BeeGFS v8 配置 TLS 加密

配置 TLS 加密以保护 BeeGFS v8 管理服务和客户端之间的通信。

概述

BeeGFS v8 引入了 TLS 支持，用于加密管理工具（如 `beegfs`命令行实用程序）和 BeeGFS 服务器服务（如 Management 或 Remote）之间的网络通信。本指南介绍了使用三种 TLS 配置方法在 BeeGFS 集群中配置 TLS 加密：

- 使用受信任的证书颁发机构： 在 BeeGFS 集群上使用现有 CA 签名的证书。
- 创建本地证书颁发机构： 创建本地证书颁发机构，并使用它为您的 BeeGFS 服务签名证书。此方法适用于希望在不依赖外部 CA 的情况下管理自己的信任链的环境。
- 禁用 **TLS**：对于不需要加密或用于故障排除的环境，完全禁用 TLS。不建议这样做，因为它会以明文形式暴露有关内部文件系统结构和配置的潜在敏感信息。

选择最适合您的环境和组织策略的方法。有关其他详细信息，请参见 "BeeGFS TLS" 文档。

> 运行 `beegfs-client` 服务的计算机不需要 TLS 来挂载 BeeGFS 文件系统。必须设置 TLS 以利用 BeeGFS CLI 和其他 beegfs 服务，例如远程和同步。

使用受信任的证书颁发机构

如果您具有受信任的证书颁发机构 (CA) 颁发的证书（无论是来自内部企业 CA 还是第三方提供商）的访问权限，则可以将 BeeGFS v8 配置为使用这些 CA 签名的证书而不是生成自签名证书。

部署新的 **BeeGFS v8** 群集

对于新的 BeeGFS v8 群集部署，配置 Ansible 清单的 `user_defined_params.yml`文件以引用您的 CA 签名证书：

```
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
```

如果 `beegfs_ha_tls_config_options.alt_names`不为空，Ansible 将使用提供的 alt_names 作为证书中的使用者备用名称 (SAN)，自动生成自签名 TLS 证书和密钥。要使用您自己的自定义 TLS 证书和密钥（由 `beegfs_ha_tls_cert_src_path`和 `beegfs_ha_tls_key_src_path`指定），您必须注释掉或删除整个 `beegfs_ha_tls_config_options`部分。否则，将优先生成自签名证书，并且不会使用您的自定义证书和密钥。

配置现有 **BeeGFS v8** 集群

对于现有的 BeeGFS v8 群集，将 BeeGFS 管理服务配置文件中的路径设置为文件节点的 CA 签名证书：

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

使用 **CA** 签名的证书配置 **BeeGFS v8** 客户端

要将 BeeGFS v8 客户端配置为使用系统的证书池信任 CA 签名的证书，请在每个客户端的配置中设置 tls-cert-file = ''。如果未使用系统证书池，请通过设置 tls-cert-file = <local cert> 提供本地证书的路径。此设置允许客户端对 BeeGFS 管理服务提供的证书进行身份验证。

创建本地证书颁发机构

如果您的组织希望为 BeeGFS 群集创建自己的证书基础架构，则可以创建一个本地证书颁发机构 (CA) 以颁发和签署 BeeGFS 群集的证书。这种方法涉及创建一个 CA，为 BeeGFS 管理服务签名证书，然后分发给客户端以建立信任链。按照以下说明设置本地 CA 并在现有或新的 BeeGFS v8 群集上部署证书。

部署新的 **BeeGFS v8** 群集

对于新的 BeeGFS v8 部署， `beegfs_8` Ansible 角色将处理在控制节点上创建本地 CA 并为管理服务生成必要的证书。可以通过在 Ansible 库存 `user_defined_params.yml`文件中设置以下参数来启用此功能：

```
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>]
```

如果未提供 `beegfs_ha_tls_config_options.alt_names`，则 Ansible 将尝试在指定的证书/密钥路径中使用现有证书。

配置现有 **BeeGFS v8** 集群

对于现有的 BeeGFS 群集，您可以通过创建本地证书颁发机构并为管理服务生成必要的证书来集成 TLS。更新 BeeGFS 管理服务配置文件中的路径，以指向新创建的证书。

本节中的说明将用作参考。处理私钥和证书时应采取适当的安全预防措施。

创建证书颁发机构

在受信任的计算机上，创建本地证书颁发机构以签署 BeeGFS 管理服务的证书。CA 证书将分发给客户端，以建立信任并实现与 BeeGFS 服务的安全通信。

以下说明是在基于 RHEL 的系统上创建本地证书颁发机构的参考。

1. 如果尚未安装 OpenSSL，请安装：

```
dnf install openssl
```

2. 创建工作目录以存储证书文件：

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

3. 生成 CA 私钥：

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

4. 创建名为 `ca.cnf` 的 CA 配置文件，并调整可分辨名称字段以匹配您的组织：

```
[ 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. 生成 CA 证书。此证书应在系统的有效期内有效，否则您需要计划在证书过期之前重新生成证书。证书过期后，某些组件之间将无法进行通信，更新 TLS 证书通常需要重新启动服务才能完成。

   以下命令生成有效期为 1 年的 CA 证书：

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

   虽然此示例使用 1 年的有效期以简化操作，但应根据组织的安全要求调整 `-days` 参数并建立证书续订流程。

创建管理服务证书

为您的 BeeGFS 管理服务生成证书，并使用您创建的 CA 对其进行签名。这些证书将安装在运行 BeeGFS 管理服务的文件节点上。

1. 生成管理服务私钥：

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

2. 创建一个名为 `tls_san.cnf`的证书配置文件，为所有管理服务 IP 地址添加 Subject Alternative Names (SANs)：

```
[ 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>
```

更新可分辨名称字段以匹配您的 CA 配置，并将 `IP.1` 和 `IP.2` 值更新为您的管理服务 IP 地址。

3. 生成证书签名请求 (CSR)：

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

4. 使用您的 CA 签署证书（有效期为 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
```

根据组织的安全策略调整证书有效期(`-days 365`）。许多组织要求每 1-2 年轮换一次证书。

5. 验证证书是否已正确创建：

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

确认"使用者备用名称"部分包含您的所有管理 IP 地址。

将证书分发到文件节点

向相应的文件节点和客户端分发 CA 证书和管理服务证书。

1. 将 CA 证书和管理服务证书和密钥复制到运行管理服务的文件节点：

```
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/
```

将管理服务指向 **TLS** 证书

更新 BeeGFS 管理服务配置以启用 TLS 并引用创建的 TLS 证书。

1. 从运行 BeeGFS 管理服务的文件节点中，编辑管理服务配置文件，例如 `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`。添加或更新以下与 TLS 相关的参数：

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

2. 采取适当措施安全地重新启动 BeeGFS 管理服务以使更改生效：

```
systemctl restart beegfs-mgmtd
```

3. 验证管理服务已成功启动：

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

查找指示成功 TLS 初始化和证书加载的日志条目。

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

为 **BeeGFS v8** 客户端配置 **TLS**

创建并分发由本地 CA 签名的证书到所有需要与 BeeGFS 管理服务通信的 BeeGFS 客户端。

1. 使用与上述管理服务证书相同的过程为客户端生成证书，但在使用者备用名称 (SAN) 字段中使用客户端的 IP 地址或主机名。
2. 安全远程将客户端的证书复制到客户端，并在客户端上将证书重命名为 `cert.pem`：

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

3. 在所有客户端上重新启动 BeeGFS 客户端服务：

```
systemctl restart beegfs-client
```

4. 通过执行 `beegfs CLI`命令验证客户端连接，例如：

```
beegfs health check
```

禁用 **TLS**

可以禁用 TLS 进行故障排除，或者如果用户需要的话。不鼓励这样做，因为它以明文形式暴露了有关内部文件系统结构和配置的潜在敏感信息。按照以下说明在现有或新的 BeeGFS v8 群集上禁用 TLS。

部署新的 **BeeGFS v8** 群集

对于新的 BeeGFS 集群部署，可以通过在 Ansible 库存 `user_defined_params.yml`文件中设置以下参数，在禁用 TLS 的情况下部署集群：

```
beegfs_ha_tls_enabled: false
```

配置现有 **BeeGFS v8** 集群

对于现有的 BeeGFS v8 群集，请编辑管理服务配置文件。例如，在 `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml` 编辑文件并设置：

```
tls-disable = true
```

采取适当措施，安全地重新启动管理服务以使更改生效。