部署功能和集成

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

目錄

部署功能和集成

BeeGFS CSI 驅動程式

為 BeeGFS v8 配置 TLS 加密

配置 TLS 加密以保護 BeeGFS v8 管理服務和用戶端之間的通訊。

總覽

BeeGFS v8 引入了 TLS 支援，用於加密管理工具（例如 `beegfs` 命令列實用程式）與 BeeGFS 伺服器服務（例如 Management 或 Remote）之間的網路通訊。本指南介紹如何使用三種 TLS 設定方法在 BeeGFS 叢集中設定 TLS 加密：

- 使用受信任的憑證授權單位：在您的 BeeGFS 叢集上使用現有的 CA 簽署憑證。
- 建立本地憑證授權單位： 建立本地憑證授權單位並使用它來簽署 BeeGFS 服務的憑證。這種方法適用於您希望管理自己的信任鏈而不依賴外部 CA 的環境。
- **TLS** 已停用： 在不需要加密的環境或進行故障排除時，可以完全停用 TLS。不建議這樣做，因為它會將內部檔案系統結構和配置等潛在敏感資訊以明文形式暴露出來。

選擇最適合您環境和組織政策的方法。請參閱 "BeeGFS TLS" 文件以獲取更多詳細資訊。

> 運行 `beegfs-client`服務的機器無需 TLS 即可掛載 BeeGFS 檔案系統。必須設定 TLS 才能使用 BeeGFS CLI 和其他 beegfs 服務，例如 remote 和 sync。

使用受信任的憑證授權單位

如果您可以存取受信任的憑證授權單位 (CA) 所頒發的憑證（無論是來自企業內部 CA 還是第三方提供者），您可以設定 BeeGFS v8 使用這些 CA 簽署的憑證，而不是產生自簽名憑證。

部署新的 **BeeGFS v8** 叢集

對於新的 BeeGFS v8 叢集部署，請設定 Ansible 清單的 `user_defined_params.yml` 檔案以引用您的 CA 簽署憑證：

```
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`不為空，Ansible 會自動產生自簽名 TLS 憑證和金鑰，並使用提供的 alt_names 作為憑證中的主題備用名稱（SAN）。若要使用您自己的自訂 TLS 憑證和金鑰（如 `beegfs_ha_tls_cert_src_path`和 `beegfs_ha_tls_key_src_path`所指定），您必須註解掉或刪除整個 `beegfs_ha_tls_config_options`部分。否則，自簽名憑證的產生將優先，您的自訂憑證和金鑰將不會被使用。

配置現有的 **BeeGFS v8** 叢集

對於現有的 BeeGFS v8 集群，請將 BeeGFS 管理服務的設定檔中的路徑設定為檔案節點的 CA 簽章憑證：

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

使用 **CA** 簽署憑證設定 **BeeGFS v8** 用戶端

若要設定 BeeGFS v8 用戶端以信任使用系統憑證池的 CA 簽章證書，請在每個用戶端的設定中設定 tls-cert-file = ""。如果未使用系統憑證池，請透過設定 tls-cert-file = <local cert> 來提供本機憑證的路徑。此設定允許用戶端驗證 BeeGFS 管理服務提供的憑證。

建立本地憑證授權單位

如果您的組織希望為 BeeGFS 叢集建立自己的憑證基礎架構，您可以建立一個本機憑證授權單位（CA）來頒發和簽署 BeeGFS 叢集的憑證。此方法涉及建立一個 CA，該 CA 為 BeeGFS 管理服務簽署憑證，然後將這些憑證分發給客戶端以建立信任鏈。請依照下列說明設定本機 CA 並在現有或新的 BeeGFS v8 叢集上部署憑證。

部署新的 **BeeGFS v8** 叢集

對於新的 BeeGFS v8 部署， `beegfs_8` Ansible 角色將負責在控制節點上建立本機 CA，並為管理服務產生必要的憑證。可以透過在 Ansible 清單的`user_defined_params.yml`檔案中設定以下參數來啟用此功能：

```
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`，則 Ansible 將嘗試使用指定憑證/金鑰路徑中的現有憑證。

配置現有的 **BeeGFS v8** 叢集

對於現有的 BeeGFS 集群，您可以透過建立本機憑證授權單位並為管理服務產生必要的憑證來整合 TLS。更新 BeeGFS 管理服務設定檔中的路徑，使其指向新建立的憑證。

本節的說明僅供參考。處理私鑰和憑證時，應採取適當的安全預防措施。

建立憑證授權單位

在受信任的電腦上，建立一個本機憑證授權單位 (CA)，用於簽署 BeeGFS 管理服務的憑證。CA 憑證將分發給用戶端，以建立信任並實現與 BeeGFS 服務的安全通訊。

以下說明是在基於 RHEL 的系統上建立本機憑證授權單位的參考。

1. 如果尚未安裝 OpenSSL，請安裝它：

```
dnf install openssl
```

2. 建立用於儲存憑證檔案的工作目錄：

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

3. 產生 CA 私鑰：

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

4. 建立一個名為 `ca.cnf`的 CA 設定檔，並調整專有名稱欄位以符合您的組織：

```
[ 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. 產生 CA 憑證。此憑證的有效期限應與系統生命週期相同，否則您需要在憑證過期前規劃重新產生憑證。憑證過期後，某些元件之間的通訊將無法進行，更新 TLS 憑證通常需要重新啟動服務才能完成。

   以下指令產生有效期限為 1 年的 CA 憑證：

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

> ⓘ 雖然為了簡單起見，本範例使用了 1 年的有效期，但您應該根據貴組織的安全要求調整 `-days`參數，並建立憑證續約流程。

建立管理服務憑證

為您的 BeeGFS 管理服務產生證書，並使用您建立的 CA 對其進行簽署。這些證書將安裝在執行 BeeGFS 管理服務的檔案節點上。

1. 產生管理服務私鑰：

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

2. 建立一個名為 `tls_san.cnf` 的憑證設定檔，其中包含所有管理服務 IP 位址的主體別名（SAN）：

```
[ 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>
```

更新專有名稱欄位以符合您的 CA 配置，並將 `IP.1`和 `IP.2`值更新為您的管理服務 IP 位址。

3. 產生憑證簽章請求 (CSR)：

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

4. 使用您的 CA 簽署憑證（有效期為 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
```

根據貴組織的安全策略調整證書有效期限 (`-days 365`。許多組織要求每 1-2 年輪換一次證書。

5. 驗證憑證是否已正確建立：

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

請確認「主題備用名稱」部分包含所有管理 IP 位址。

將證書分發到檔案節點

將 CA 憑證和管理服務憑證分發到對應的檔案節點和用戶端。

1. 將 CA 憑證、管理服務憑證和金鑰複製到執行管理服務的檔案節點：

```
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/
```

將管理服務指向 **TLS** 憑證

更新 BeeGFS 管理服務設定以啟用 TLS 並引用已建立的 TLS 憑證。

1. 在執行 BeeGFS 管理服務的檔案節點上，編輯管理服務設定檔，例如位於 `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`。新增或更新以下與 TLS 相關的參數：

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

2. 請採取適當措施，安全地重新啟動 BeeGFS 管理服務，以使變更生效：

```
systemctl restart beegfs-mgmtd
```

3. 驗證管理服務是否已成功啟動：

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

查看日誌條目，確認 TLS 初始化和憑證載入是否成功。

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

為 **BeeGFS v8** 用戶端設定 **TLS**

建立並向所有需要與 BeeGFS 管理服務通訊的 BeeGFS 用戶端分發由本機 CA 簽署的憑證。

1. 使用與上述管理服務證書相同的流程為用戶端產生證書，但在 Subject Alternative Name (SAN) 欄位中使用用戶端的 IP 位址或主機名稱。
2. 將客戶端憑證安全地遠端複製到客戶端，並在客戶端上將該憑證重新命名為 `cert.pem`：

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

3. 在所有客戶端上重新啟動 BeeGFS 用戶端服務：

```
systemctl restart beegfs-client
```

4. 透過執行 `beegfs CLI` 命令驗證客戶端連線，例如：

```
beegfs health check
```

停用 **TLS**

TLS 可以停用，用於故障排除或使用者本身需要。但不建議這樣做，因為它會以明文形式暴露內部檔案系統結構和配置等潛在敏感資訊。請依照以下說明在現有或新建的 BeeGFS v8 叢集上停用 TLS。

部署新的 **BeeGFS v8** 叢集

對於新的 BeeGFS 叢集部署，可以透過在 Ansible 清單的 `user_defined_params.yml` 檔案中設定以下參數來停用 TLS 進行叢集部署：

```
beegfs_ha_tls_enabled: false
```

配置現有的 **BeeGFS v8** 叢集

對於現有的 BeeGFS v8 集群，請編輯管理服務設定檔。例如，編輯位於 `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`的檔案並設定：

```
tls-disable = true
```

採取適當措施安全地重新啟動管理服務，以使變更生效。