기능 및 통합 배포

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

목차

기능 및 통합 배포

BeeGFS CSI 드라이버

BeeGFS v8용 TLS 암호화 구성

BeeGFS v8 관리 서비스와 클라이언트 간의 통신을 보호하기 위해 TLS 암호화를 구성하십시오.

개요

BeeGFS v8은 관리 도구(예: `beegfs` 명령줄 유틸리티)와 Management 또는 Remote와 같은 BeeGFS 서버 서비스 간의 네트워크 통신을 암호화하기 위한 TLS 지원을 도입했습니다. 이 가이드에서는 세 가지 TLS 구성 방법을 사용하여 BeeGFS 클러스터에서 TLS 암호화를 구성하는 방법을 설명합니다.

- **신뢰할 수 있는 인증 기관 사용:** BeeGFS 클러스터에서 기존 CA 서명 인증서를 사용하십시오.
- **로컬 인증 기관 생성:** 로컬 인증 기관을 생성하고 이를 사용하여 BeeGFS 서비스용 인증서에 서명합니다. 이 방법은 외부 CA에 의존하지 않고 자체 신뢰 체인을 관리하려는 환경에 적합합니다.
- **TLS 비활성화:** 암호화가 필요하지 않은 환경이나 문제 해결을 위해 TLS를 완전히 비활성화할 수 있습니다. 하지만 내부 파일 시스템 구조 및 구성에 대한 잠재적으로 민감한 정보가 평문으로 노출될 수 있으므로 권장하지 않습니다.

귀사의 환경 및 조직 정책에 가장 적합한 방법을 선택하십시오. 자세한 내용은 "BeeGFS TLS" 문서를 참조하십시오.

> `beegfs-client` 서비스를 실행하는 머신은 BeeGFS 파일 시스템을 마운트하기 위해 TLS가 필요하지 않습니다. BeeGFS CLI 및 원격, 동기화와 같은 다른 beegfs 서비스를 사용하려면 TLS를 설정해야 합니다.

신뢰할 수 있는 인증 기관 사용

내부 기업 CA 또는 타사 공급업체에서 발급한 신뢰할 수 있는 인증 기관(CA)의 인증서에 액세스할 수 있는 경우 BeeGFS v8이 자체 서명 인증서를 생성하는 대신 이러한 CA 서명 인증서를 사용하도록 구성할 수 있습니다.

새로운 **BeeGFS v8** 클러스터 배포

새로운 BeeGFS v8 클러스터 배포를 위해 Ansible 인벤토리의 `user_defined_params.yml` 파일에서 CA 서명 인증서를 참조하도록 구성하십시오.

```
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`이 비어 있지 않으면 Ansible은 제공된 `alt_names`를 인증서의 SAN(Subject Alternative Names)으로 사용하여 자체 서명된 TLS 인증서와 키를 자동으로 생성합니다. 사용자 지정 TLS 인증서와 키(`beegfs_ha_tls_cert_src_path` 및 `beegfs_ha_tls_key_src_path`에 지정된 대로)를 사용하려면 `beegfs_ha_tls_config_options` 섹션 전체를 주석 처리하거나 삭제해야 합니다. 그렇지 않으면 자체 서명된 인증서 생성이 우선시되어 사용자 지정 인증서와 키가 사용되지 않습니다.

기존 **BeeGFS v8** 클러스터 구성

기존 BeeGFS v8 클러스터의 경우 BeeGFS 관리 서비스의 구성 파일에서 파일 노드의 CA 서명 인증서 경로를 설정하십시오.

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

CA 서명 인증서를 사용하여 **BeeGFS v8** 클라이언트 구성

BeeGFS v8 클라이언트가 시스템 인증서 풀을 사용하여 CA 서명 인증서를 신뢰하도록 구성하려면 각 클라이언트 구성에서 tls-cert-file = ""로 설정하십시오. 시스템 인증서 풀을 사용하지 않는 경우 tls-cert-file = <local cert>로 설정하여 로컬 인증서의 경로를 제공하십시오. 이 설정을 통해 클라이언트는 BeeGFS 관리 서비스에서 제공하는 인증서를 인증할 수 있습니다.

로컬 인증 기관 생성

조직에서 BeeGFS 클러스터용 자체 인증서 인프라를 구축하려면 로컬 인증 기관(CA)을 생성하여 BeeGFS 클러스터용 인증서를 발급하고 서명할 수 있습니다. 이 방법은 BeeGFS 관리 서비스용 인증서에 서명하는 CA를 생성한 다음, 해당 인증서를 클라이언트에 배포하여 신뢰 체인을 구축하는 방식입니다. 다음 지침에 따라 로컬 CA를 설정하고 기존 또는 신규 BeeGFS v8 클러스터에 인증서를 배포하십시오.

새로운 **BeeGFS v8** 클러스터 배포

새로운 BeeGFS v8 배포의 경우, `beegfs_8` Ansible 역할은 제어 노드에 로컬 CA를 생성하고 관리 서비스에 필요한 인증서를 생성합니다. 이 기능은 Ansible 인벤토리의 `user_defined_params.yml` 파일에 다음 매개변수를 설정하여 활성화할 수 있습니다:

```
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`가 제공되지 않으면 Ansible은 지정된 인증서/키 경로에 있는 기존 인증서를 사용하려고 시도합니다.

기존 **BeeGFS v8** 클러스터 구성

기존 BeeGFS 클러스터의 경우 로컬 인증 기관을 생성하고 관리 서비스에 필요한 인증서를 생성하여 TLS를 통합할 수 있습니다. BeeGFS 관리 서비스의 구성 파일에서 경로를 업데이트하여 새로 생성된 인증서를 가리키도록 하십시오.

이 섹션의 지침은 참고용으로 사용됩니다. 개인 키와 인증서를 다룰 때는 적절한 보안 예방 조치를 취해야 합니다.

인증 기관 생성

신뢰할 수 있는 시스템에서 로컬 인증 기관(CA)을 생성하여 BeeGFS 관리 서비스용 인증서를 서명하십시오. 생성된 CA 인증서는 클라이언트에 배포되어 신뢰를 구축하고 BeeGFS 서비스와의 안전한 통신을 가능하게 합니다.

다음 지침은 RHEL 기반 시스템에서 로컬 Certificate Authority를 생성하기 위한 참조 자료입니다.

1. OpenSSL이 아직 설치되어 있지 않은 경우 설치하십시오.

```
dnf install openssl
```

2. 인증서 파일을 저장할 작업 디렉터리를 생성합니다:

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

3. CA 개인 키를 생성합니다.

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

4. `ca.cnf`라는 이름의 CA 구성 파일을 생성하고 고유 이름 필드를 조직에 맞게 조정하십시오.

```
[ 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 인증서를 생성하십시오. 이 인증서는 시스템 수명 동안 유효해야 하며, 그렇지 않으면 만료 전에 인증서를 다시 생성해야 합니다. 인증서가 만료되면 일부 구성 요소 간의 통신이 불가능해지며, TLS 인증서를 업데이트하려면 일반적으로 서비스를 재시작해야 합니다.

   다음 명령은 1년 동안 유효한 CA 인증서를 생성합니다:

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

   이 예시에서는 간단하게 하기 위해 1년 유효 기간을 사용하지만, 조직의 보안 요구 사항에 따라 `-days` 매개변수를 조정하고 인증서 갱신 프로세스를 수립해야 합니다.

관리 서비스 인증서 생성

BeeGFS 관리 서비스용 인증서를 생성하고 생성한 CA로 서명하십시오. 이러한 인증서는 BeeGFS 관리 서비스가 실행되는 파일 노드에 설치됩니다.

1. 관리 서비스 개인 키를 생성합니다:

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

2. 모든 관리 서비스 IP 주소에 대한 주체 대체 이름(SAN)을 포함하는 `tls_san.cnf`이라는 이름의 인증서 구성 파일을 생성합니다:

```
[ 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>
```

고유 이름 필드를 CA 구성에 맞게 업데이트하고 `IP.1` 및 `IP.2` 값을 관리 서비스 IP 주소로 업데이트하십시오.

3. 인증서 서명 요청(CSR) 생성:

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

4. CA로 인증서에 서명(1년간 유효):

```
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
```

조직의 보안 정책에 따라 인증서 유효 기간(`-days 365`을 조정하십시오. 많은 조직에서는 1~2년마다 인증서를 갱신하도록 요구합니다.

5. 인증서가 올바르게 생성되었는지 확인합니다.

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

주체 대체 이름 섹션에 모든 관리 IP 주소가 포함되어 있는지 확인하십시오.

파일 노드에 인증서 배포

CA 인증서와 관리 서비스 인증서를 해당 파일 노드 및 클라이언트에 배포합니다.

1. CA 인증서와 관리 서비스 인증서 및 키를 관리 서비스를 실행하는 파일 노드에 복사합니다.

```
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/
```

관리 서비스가 **TLS** 인증서를 가리키도록 설정

TLS를 활성화하고 생성된 TLS 인증서를 참조하도록 BeeGFS 관리 서비스 구성을 업데이트하십시오.

1. BeeGFS 관리 서비스가 실행 중인 파일 노드에서 관리 서비스 구성 파일을 편집합니다(예: `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`). 다음 TLS 관련 매개변수를 추가하거나 업데이트합니다:

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

2. 변경 사항을 적용하려면 BeeGFS 관리 서비스를 안전하게 다시 시작하는 적절한 조치를 취하십시오:

```
systemctl restart beegfs-mgmtd
```

3. 관리 서비스가 성공적으로 시작되었는지 확인합니다.

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

성공적인 TLS 초기화 및 인증서 로딩을 나타내는 로그 항목을 찾으십시오.

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

BeeGFS v8 클라이언트에 대한 TLS 구성

BeeGFS 관리 서비스와의 통신이 필요한 모든 BeeGFS 클라이언트에 로컬 CA에서 서명한 인증서를 생성하고 배포합니다.

1. 위의 관리 서비스 인증서와 동일한 프로세스를 사용하여 클라이언트용 인증서를 생성하되, 주체 대체 이름(SAN) 필드에 클라이언트의 IP 주소 또는 호스트 이름을 입력합니다.
2. 클라이언트의 인증서를 안전한 원격 복사 방식으로 클라이언트에 복사하고 클라이언트에서 인증서 이름을 `cert.pem`로 변경합니다.

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

3. 모든 클라이언트에서 BeeGFS 클라이언트 서비스를 다시 시작하십시오.

```
systemctl restart beegfs-client
```

4. `beegfs CLI` 명령어를 실행하여 클라이언트 연결을 확인하십시오. 예:

```
beegfs health check
```

TLS 비활성화

TLS는 문제 해결을 위해 또는 사용자가 원할 경우 비활성화할 수 있습니다. 이는 내부 파일 시스템 구조 및 구성에 대한 잠재적으로 민감한 정보가 평문 형태로 노출될 수 있으므로 권장하지 않습니다. 기존 또는 새 BeeGFS v8 클러스터에서 TLS를 비활성화하려면 다음 지침을 따르십시오.

새로운 BeeGFS v8 클러스터 배포

새로운 BeeGFS 클러스터를 배포할 때, Ansible 인벤토리의 `user_defined_params.yml` 파일에 다음 매개변수를 설정하여 TLS를 비활성화한 상태로 클러스터를 배포할 수 있습니다:

```
beegfs_ha_tls_enabled: false
```

기존 BeeGFS v8 클러스터 구성

기존 BeeGFS v8 클러스터의 경우 관리 서비스 구성 파일을 편집합니다. 예를 들어, `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml` 경로에 있는 파일을 편집하고 다음과 같이 설정합니다:

```
tls-disable = true
```

변경 사항을 적용하려면 관리 서비스를 안전하게 재시작하기 위한 적절한 조치를 취하십시오.