Distribuisci funzionalità e integrazioni

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

Sommario

Distribuisci funzionalità e integrazioni

Driver CSI BeeGFS

Configura la crittografia TLS per BeeGFS v8

Configura la crittografia TLS per proteggere la comunicazione tra i servizi di gestione BeeGFS v8 e i client.

Panoramica

BeeGFS v8 introduce il supporto TLS per la crittografia delle comunicazioni di rete tra strumenti amministrativi (come l' `beegfs`utility da riga di comando) e servizi server BeeGFS come Management o Remote. Questa guida illustra la configurazione della crittografia TLS nel cluster BeeGFS utilizzando tre metodi di configurazione TLS:

- **Utilizzo di un'autorità di certificazione attendibile:** Usa i certificati firmati da CA esistenti sul tuo cluster BeeGFS.
- **Creazione di un'autorità di certificazione locale:** Creazione di un'autorità di certificazione locale e utilizzo di essa per firmare i certificati per i servizi BeeGFS. Questo approccio è adatto per ambienti in cui si desidera gestire la propria catena di fiducia senza affidarsi a una CA esterna.
- **TLS disabilitato:** Disattivare completamente TLS per gli ambienti in cui la crittografia non è richiesta o per la risoluzione dei problemi. Questa opzione è sconsigliata in quanto espone informazioni potenzialmente sensibili sulla struttura del file system interno e sulla configurazione come testo non crittografato.

Scegli il metodo più adatto al tuo ambiente e alle policy aziendali. Consulta la "BeeGFS TLS" documentazione per ulteriori dettagli.

> Le macchine che eseguono il `beegfs-client` servizio non richiedono TLS per montare il file system BeeGFS. TLS deve essere configurato per utilizzare la BeeGFS CLI e altri servizi beegfs, come remote e sync.

Utilizzo di un'autorità di certificazione attendibile

Se hai accesso ai certificati emessi da una Certificate Authority (CA) attendibile, sia essa una CA aziendale interna o un provider di terze parti, puoi configurare BeeGFS v8 per utilizzare questi certificati firmati dalla CA invece di generarne di autofirmati.

Distribuzione di un nuovo cluster BeeGFS v8

Per una nuova distribuzione del cluster BeeGFS v8, configura il file dell'inventario Ansible `user_defined_params.yml` per fare riferimento ai certificati firmati dalla CA:

```
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
```

> Se `beegfs_ha_tls_config_options.alt_names` non è vuoto, Ansible genererà automaticamente un certificato TLS autofirmato e una chiave, utilizzando gli alt_names forniti come Subject Alternative Names (SAN) nel certificato. Per utilizzare il proprio certificato TLS e la propria chiave personalizzati (come specificato da `beegfs_ha_tls_cert_src_path` e `beegfs_ha_tls_key_src_path`), è necessario commentare o rimuovere l'intera `beegfs_ha_tls_config_options` sezione. In caso contrario, la generazione del certificato autofirmato avrà la precedenza e il certificato e la chiave personalizzati non verranno utilizzati.

Configurazione di un cluster BeeGFS v8 esistente

Per un cluster BeeGFS v8 esistente, impostare i percorsi nel file di configurazione dei servizi di gestione BeeGFS sui certificati firmati dalla CA del nodo file:

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

Configurazione dei client BeeGFS v8 con certificati firmati da CA

Per configurare i client BeeGFS v8 in modo che considerino attendibili i certificati firmati da una CA utilizzando il pool di certificati del sistema, impostare tls-cert-file = "" nel file di configurazione di ciascun client. Se il pool di certificati del sistema non viene utilizzato, fornire il percorso a un certificato locale impostando tls-cert-file = <local cert>. Questa configurazione consente ai client di autenticare i certificati presentati dai servizi di gestione BeeGFS.

Creazione di un'autorità di certificazione locale

Se la tua organizzazione desidera creare una propria infrastruttura di certificazione per il cluster BeeGFS, puoi creare un'Autorità di Certificazione (CA) locale per emettere e firmare i certificati per il tuo cluster BeeGFS. Questo approccio prevede la creazione di una CA che firma i certificati per i servizi di gestione BeeGFS, che vengono poi distribuiti ai client per stabilire una catena di trust. Segui queste istruzioni per configurare una CA locale e distribuire i certificati sul tuo cluster BeeGFS v8 esistente o nuovo.

Distribuzione di un nuovo cluster BeeGFS v8

Per una nuova distribuzione di BeeGFS v8, il `beegfs_8` ruolo Ansible gestirà la creazione di una CA locale sul nodo di controllo e la generazione dei certificati necessari per i servizi di gestione. Questo può essere abilitato impostando i seguenti parametri nel file `user_defined_params.yml` di inventario di Ansible:

```
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>]
```

Se `beegfs_ha_tls_config_options.alt_names` non viene fornito, Ansible tenterà di utilizzare i certificati esistenti nei percorsi certificato/chiave specificati.

Configurazione di un cluster BeeGFS v8 esistente

Per un cluster BeeGFS esistente, puoi integrare TLS creando un'autorità di certificazione locale e generando i certificati necessari per i servizi di gestione. Aggiorna i percorsi nel file di configurazione dei servizi di gestione BeeGFS affinché puntino ai certificati appena creati.

Le istruzioni contenute in questa sezione sono da intendersi come riferimento. È necessario adottare le opportune precauzioni di sicurezza quando si maneggiano chiavi private e certificati.

Creare l'autorità di certificazione

Su una macchina attendibile, crea una Certificate Authority locale per firmare i certificati per i servizi di gestione BeeGFS. Il certificato della CA verrà distribuito ai client per stabilire la fiducia e abilitare la comunicazione sicura con i servizi BeeGFS.

Le seguenti istruzioni costituiscono un riferimento per la creazione di una Certificate Authority locale su un sistema basato su RHEL.

1. Installa OpenSSL se non è già installato:

```
dnf install openssl
```

2. Crea una directory di lavoro in cui archiviare i file dei certificati:

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

3. Genera la chiave privata CA:

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

4. Crea un file di configurazione CA denominato `ca.cnf` e modifica i campi del nome distinto in modo che

corrispondano alla tua organizzazione:

```
[ 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. Generare il certificato CA. Questo certificato deve essere valido per tutta la vita del sistema, altrimenti sarà necessario pianificare di rigenerare i certificati prima della loro scadenza. Una volta scaduto un certificato, la comunicazione tra alcuni componenti non sarà possibile e l'aggiornamento dei certificati TLS richiederà generalmente il riavvio dei servizi per completare l'operazione.

   Il seguente comando genera un certificato CA valido per 1 anno:

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

   Sebbene in questo esempio venga utilizzato un periodo di validità di 1 anno per semplicità, è opportuno adattare il `-days` parametro in base ai requisiti di sicurezza della propria organizzazione e stabilire una procedura di rinnovo del certificato.

Creare certificati del servizio di gestione

Genera certificati per i tuoi servizi di gestione BeeGFS e firmali con la CA che hai creato. Questi certificati verranno installati sui nodi file che eseguono i servizi di gestione BeeGFS.

1. Genera la chiave privata del servizio di gestione:

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

2. Crea un file di configurazione del certificato denominato `tls_san.cnf` con Subject Alternative Names

(SAN) per tutti gli indirizzi IP del servizio di gestione:

```
[ 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>
```

Aggiorna i campi del nome distinto in modo che corrispondano alla configurazione della CA e i `IP.1` e `IP.2` valori con gli indirizzi IP del servizio di gestione.

3. Genera una richiesta di firma del certificato (CSR):

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

4. Firma il certificato con la tua CA (valido per 1 anno):

```
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
```

Adatta il periodo di validità del certificato (`-days 365`) in base alle policy di sicurezza della tua organizzazione. Molte organizzazioni richiedono la rotazione dei certificati ogni 1-2 anni.

5. Verifica che il certificato sia stato creato correttamente:

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

   Conferma che la sezione Subject Alternative Name includa tutti i tuoi indirizzi IP di gestione.

Distribuisci i certificati ai nodi file

Distribuire il certificato CA e i certificati del servizio di gestione ai nodi file e ai client appropriati.

1. Copia il certificato CA, il certificato del servizio di gestione e la chiave nei nodi file che eseguono i servizi di gestione:

```
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/
```

Indirizzare il servizio di gestione ai certificati TLS

Aggiorna la configurazione del servizio di gestione BeeGFS per abilitare TLS e fare riferimento ai certificati TLS creati.

1. Da un nodo file che esegue il servizio di gestione BeeGFS, modifica il file di configurazione del servizio di gestione, ad esempio in `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`. Aggiungi o aggiorna i seguenti parametri relativi a TLS:

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

2. Adottare le misure appropriate per riavviare in modo sicuro il servizio di gestione BeeGFS affinché le modifiche abbiano effetto:

```
systemctl restart beegfs-mgmtd
```

3. Verificare che il servizio di gestione sia stato avviato correttamente:

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

   Cerca le voci di registro che indicano l'inizializzazione TLS e il caricamento del certificato riusciti.

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

Configurare TLS per i client BeeGFS v8

Creare e distribuire certificati firmati dalla CA locale a tutti i client BeeGFS che richiederanno la comunicazione con i servizi di gestione BeeGFS.

1. Generare un certificato per il client utilizzando lo stesso processo del certificato del servizio di gestione sopra, ma con l'indirizzo IP o il nome host del client nel campo Subject Alternative Name (SAN).
2. Copia in modo sicuro tramite copia remota il certificato del client sul client e rinomina il certificato in `cert.pem` sul client:

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

3. Riavvia il servizio client BeeGFS su tutti i client:

```
systemctl restart beegfs-client
```

4. Verificare la connettività del client eseguendo un `beegfs CLI` comando, ad esempio:

```
beegfs health check
```

Disabilitazione TLS

TLS può essere disabilitato per la risoluzione dei problemi o se desiderato dagli utenti. Questa operazione è sconsigliata in quanto espone informazioni potenzialmente sensibili sulla struttura interna del file system e sulla configurazione in chiaro. Seguire queste istruzioni per disabilitare TLS sul cluster BeeGFS v8 esistente o nuovo.

Distribuzione di un nuovo cluster BeeGFS v8

Per una nuova distribuzione del cluster BeeGFS, il cluster può essere distribuito con TLS disabilitato impostando il seguente parametro nel file dell'inventario Ansible `user_defined_params.yml`:

```
beegfs_ha_tls_enabled: false
```

Configurazione di un cluster BeeGFS v8 esistente

Per un cluster BeeGFS v8 esistente, modificare il file di configurazione del servizio di management. Ad esempio, modificare il file in `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml` e impostare:

```
tls-disable = true
```

Adottare le misure appropriate per riavviare in modo sicuro il servizio di gestione affinché le modifiche abbiano effetto.

Informazioni sul copyright

Informazioni sul marchio commerciale