



Funktionen und Integrationen bereitstellen

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

Inhalt

Funktionen und Integrationen bereitstellen	1
BeeGFS CSI-Treiber	1
TLS-Verschlüsselung für BeeGFS v8 konfigurieren	1
Überblick	1
Verwendung einer vertrauenswürdigen Zertifizierungsstelle	1
Erstellung einer lokalen Zertifizierungsstelle	2
TLS deaktivieren	7

Funktionen und Integrationen bereitstellen

BeeGFS CSI-Treiber

TLS-Verschlüsselung für BeeGFS v8 konfigurieren

Konfigurieren Sie die TLS-Verschlüsselung, um die Kommunikation zwischen BeeGFS v8 Management Services und Clients zu sichern.

Überblick

BeeGFS v8 führt TLS-Unterstützung für die Verschlüsselung der Netzwerkkommunikation zwischen Verwaltungstools (wie dem `beegfs` Befehlszeilenprogramm) und BeeGFS-Serverdiensten wie Management oder Remote ein. Dieser Leitfaden beschreibt die Konfiguration der TLS-Verschlüsselung in Ihrem BeeGFS-Cluster anhand von drei TLS-Konfigurationsmethoden:

- **Verwendung einer vertrauenswürdigen Zertifizierungsstelle:** Verwenden Sie vorhandene, von einer CA signierte Zertifikate auf Ihrem BeeGFS-Cluster.
- **Lokale Zertifizierungsstelle erstellen:** Erstellen einer lokalen Zertifizierungsstelle und deren Verwendung zum Signieren von Zertifikaten für Ihre BeeGFS-Services. Dieser Ansatz eignet sich für Umgebungen, in denen Sie Ihre eigene Vertrauenskette verwalten möchten, ohne auf eine externe Zertifizierungsstelle angewiesen zu sein.
- **TLS deaktiviert:** Deaktivieren Sie TLS vollständig für Umgebungen, in denen keine Verschlüsselung erforderlich ist oder zur Fehlerbehebung. Dies wird nicht empfohlen, da dadurch potenziell sensible Informationen über die interne Dateisystemstruktur und Konfiguration im Klartext offengelegt werden.

Wählen Sie die Methode, die am besten zu Ihrer Umgebung und Ihren Unternehmensrichtlinien passt. Siehe die ["BeeGFS TLS"](#) Dokumentation für weitere Details.



Rechner, auf denen der `beegfs-client` Dienst ausgeführt wird, benötigen kein TLS, um das BeeGFS-Dateisystem einzubinden. TLS muss eingerichtet werden, um die BeeGFS CLI und andere BeeGFS-Dienste wie `remote` und `sync` zu nutzen.

Verwendung einer vertrauenswürdigen Zertifizierungsstelle

Wenn Sie Zugriff auf Zertifikate haben, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurden—sei es von einer internen Unternehmens-CA oder einem Drittanbieter—, können Sie BeeGFS v8 so konfigurieren, dass diese CA-signierten Zertifikate anstelle von selbstsignierten verwendet werden.

Bereitstellung eines neuen BeeGFS v8 Clusters

Konfigurieren Sie für eine neue BeeGFS v8-Clusterbereitstellung die `user_defined_params.yml`-Datei des Ansible-Inventars so, dass sie auf Ihre von der CA signierten Zertifikate verweist:

```
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
```

 Wenn `beegfs_ha_tls_config_options.alt_names` nicht leer ist, generiert Ansible automatisch ein selbstsigniertes TLS-Zertifikat und einen Schlüssel, wobei die angegebenen `alt_names` als Subject Alternative Names (SANs) im Zertifikat verwendet werden. Um Ihr eigenes TLS-Zertifikat und Ihren eigenen Schlüssel zu verwenden (wie durch `beegfs_ha_tls_cert_src_path` und `beegfs_ha_tls_key_src_path` angegeben), müssen Sie den gesamten `beegfs_ha_tls_config_options` Abschnitt auskommentieren oder entfernen. Andernfalls hat die Generierung des selbstsignierten Zertifikats Vorrang, und Ihr benutzerdefiniertes Zertifikat und Ihr benutzerdefinierter Schlüssel werden nicht verwendet.

Konfigurieren eines bestehenden BeeGFS v8 Clusters

Für einen bestehenden BeeGFS v8-Cluster legen Sie die Pfade in der Konfigurationsdatei der BeeGFS-Managementdienste auf die CA-signierten Zertifikate des Dateiknotens fest:

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

Konfigurieren von BeeGFS v8-Clients mit CA-signierten Zertifikaten

Um BeeGFS v8-Clients so zu konfigurieren, dass sie von einer Zertifizierungsstelle signierten Zertifikaten aus dem Systemzertifikatspool vertrauen, setzen Sie `tls-cert-file = ""` in der Konfiguration jedes Clients. Wenn der Systemzertifikatspool nicht verwendet wird, geben Sie den Pfad zu einem lokalen Zertifikat an, indem Sie `tls-cert-file = <local cert>` setzen. Diese Konfiguration ermöglicht es Clients, die von den BeeGFS-Managementdiensten präsentierten Zertifikate zu authentifizieren.

Erstellung einer lokalen Zertifizierungsstelle

Wenn Ihre Organisation eine eigene Zertifikatsinfrastruktur für den BeeGFS-Cluster erstellen möchte, können Sie eine lokale Zertifizierungsstelle (CA) einrichten, die Zertifikate für Ihren BeeGFS-Cluster ausstellt und signiert. Dieser Ansatz beinhaltet die Erstellung einer CA, die Zertifikate für BeeGFS-Managementdienste signiert, welche dann an Clients verteilt werden, um eine Vertrauenskette herzustellen. Befolgen Sie diese Anweisungen, um eine lokale CA einzurichten und Zertifikate auf Ihrem bestehenden oder neuen BeeGFS v8 Cluster bereitzustellen.

Bereitstellung eines neuen BeeGFS v8 Clusters

Für eine neue BeeGFS v8-Bereitstellung wird die `beegfs_8` Ansible-Rolle die Erstellung einer lokalen CA auf dem Kontrollknoten übernehmen und die notwendigen Zertifikate für die Managementdienste generieren. Dies kann aktiviert werden, indem die folgenden Parameter in der Ansible-Inventar `user_defined_params.yml`-Datei gesetzt werden:

```
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>]
```



Wenn `beegfs_ha_tls_config_options.alt_names` nicht angegeben wird, versucht Ansible, vorhandene Zertifikate in den angegebenen Zertifikats-/Schlüsselpfaden zu verwenden.

Konfigurieren eines bestehenden BeeGFS v8 Clusters

Für einen bestehenden BeeGFS-Cluster können Sie TLS integrieren, indem Sie eine lokale Zertifizierungsstelle erstellen und die erforderlichen Zertifikate für die Managementdienste generieren. Aktualisieren Sie die Pfade in der BeeGFS-Managementdienste-Konfigurationsdatei, sodass sie auf die neu erstellten Zertifikate verweisen.



Die Anweisungen in diesem Abschnitt dienen als Referenz. Beim Umgang mit privaten Schlüsseln und Zertifikaten sollten angemessene Sicherheitsvorkehrungen getroffen werden.

Erstellen Sie die Zertifizierungsstelle

Erstellen Sie auf einem vertrauenswürdigen Rechner eine lokale Certificate Authority, um Zertifikate für Ihre BeeGFS-Managementdienste zu signieren. Das CA-Zertifikat wird an die Clients verteilt, um Vertrauen herzustellen und eine sichere Kommunikation mit BeeGFS-Services zu ermöglichen.

Die folgenden Anweisungen sind eine Referenz für die Erstellung einer lokalen Zertifizierungsstelle auf einem RHEL-basierten System.

1. Installieren Sie OpenSSL, falls es noch nicht installiert ist:

```
dnf install openssl
```

2. Erstellen Sie ein Arbeitsverzeichnis zum Speichern der Zertifikatsdateien:

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

3. Generieren Sie den privaten CA-Schlüssel:

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

4. Erstellen Sie eine CA Konfigurationsdatei mit dem Namen ca.cnf und passen Sie die Felder für den individuellen Namen an Ihre Organisation an:

```
[ 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. Generieren Sie das CA-Zertifikat. Dieses Zertifikat sollte für die gesamte Lebensdauer des Systems gültig sein, andernfalls müssen Sie die Zertifikate vor ihrem Ablaufdatum neu generieren. Sobald ein Zertifikat abläuft, ist die Kommunikation zwischen einigen Komponenten nicht mehr möglich und die Aktualisierung von TLS-Zertifikaten erfordert in der Regel einen Neustart der Dienste, um sie abzuschließen.

Der folgende Befehl generiert ein CA-Zertifikat, das 1 Jahr gültig ist:

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



Während in diesem Beispiel der Einfachheit halber eine Gültigkeitsdauer von 1 Jahr verwendet wird, sollten Sie den -days Parameter entsprechend den Sicherheitsanforderungen Ihrer Organisation anpassen und einen Prozess zur Zertifikaterneuerung einrichten.

Management-Service-Zertifikate erstellen

Generieren Sie Zertifikate für Ihre BeeGFS management services und signieren Sie diese mit der von Ihnen erstellten CA. Diese Zertifikate werden auf den Dateiknoten installiert, auf denen BeeGFS management services ausgeführt werden.

1. Generieren Sie den privaten Schlüssel des Verwaltungsdienstes:

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

2. Erstellen Sie eine Konfigurationsdatei `tls_san.cnf` mit Subject Alternative Names (SANs) für alle Management-Service-IP-Adressen:

```
[ 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>
```

Aktualisieren Sie die Felder für den individuellen Namen, damit sie mit Ihrer CA-Konfiguration sowie die IP.1 und IP.2 Werte mit den IP-Adressen Ihres Management-Dienstes übereinstimmen.

3. Generieren Sie eine Certificate Signing Request (CSR):

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

4. Signieren Sie das Zertifikat mit Ihrer CA (gültig für 1 Jahr):

```
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
```



Passen Sie die Gültigkeitsdauer des Zertifikats (-days 365) an die Sicherheitsrichtlinien Ihrer Organisation an. Viele Organisationen verlangen eine Zertifikatsrotation alle 1–2 Jahre.

5. Überprüfen Sie, ob das Zertifikat korrekt erstellt wurde:

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

Bestätigen Sie, dass der Abschnitt „Subject Alternative Name“ alle Ihre Management-IP-Adressen enthält.

Zertifikate an Dateiknoten verteilen

Verteilen Sie das CA-Zertifikat und die Management-Service-Zertifikate an die entsprechenden Dateiknoten und Clients.

1. Kopieren Sie das CA-Zertifikat sowie das Zertifikat und den Schlüssel des Verwaltungsdienstes auf die Dateiknoten, auf denen die Verwaltungsdienste ausgeführt werden:

```
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/
```

Weisen Sie den Verwaltungsdienst auf die TLS-Zertifikate zu.

Aktualisieren Sie die Konfiguration des BeeGFS-Managementdienstes, um TLS zu aktivieren und auf die erstellten TLS-Zertifikate zu verweisen.

1. Bearbeiten Sie auf einem Dateiknoten, auf dem der BeeGFS-Managementdienst ausgeführt wird, die Konfigurationsdatei, zum Beispiel unter /mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml. Fügen Sie die folgenden TLS-bezogenen Parameter hinzu oder aktualisieren Sie sie:

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

2. Ergreifen Sie geeignete Maßnahmen, um den BeeGFS management service sicher neu zu starten, damit die Änderungen wirksam werden:

```
systemctl restart beegfs-mgmtd
```

3. Überprüfen Sie, ob der Managementdienst erfolgreich gestartet wurde:

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

Suchen Sie nach Logeinträgen, die eine erfolgreiche TLS-Initialisierung und das Laden des Zertifikats anzeigen.

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

TLS für BeeGFS v8-Clients konfigurieren

Erstellen und verteilen Sie von der lokalen CA signierte Zertifikate an alle BeeGFS-Clients, die eine Kommunikation mit den BeeGFS-Managementdiensten benötigen.

1. Generieren Sie ein Zertifikat für den Client nach dem gleichen Verfahren wie das oben beschriebene Management-Service-Zertifikat, jedoch mit der IP-Adresse oder dem Hostnamen des Clients im Feld Subject Alternative Name (SAN).
2. Kopieren Sie das Client-Zertifikat sicher per Remote auf den Client und benennen Sie das Zertifikat auf dem Client in `cert.pem` um:

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

3. Starten Sie den BeeGFS client service auf allen Clients neu:

```
systemctl restart beegfs-client
```

4. Überprüfen Sie die Client-Verbindung, indem Sie einen `beegfs CLI`-Befehl ausführen, zum Beispiel:

```
beegfs health check
```

TLS deaktivieren

TLS kann zur Fehlerbehebung oder auf Wunsch der Benutzer deaktiviert werden. Davon wird abgeraten, da dadurch potenziell sensible Informationen über die interne Dateisystemstruktur und Konfiguration im Klartext offengelegt werden. Befolgen Sie diese Anweisungen, um TLS auf Ihrem bestehenden oder neuen BeeGFS v8 Cluster zu deaktivieren.

Bereitstellung eines neuen BeeGFS v8 Clusters

Für die Bereitstellung eines neuen BeeGFS-Clusters kann der Cluster mit deaktiviertem TLS bereitgestellt werden, indem der folgende Parameter in der Ansible-Inventar `user_defined_params.yml`-Datei festgelegt wird:

```
beegfs_ha_tls_enabled: false
```

Konfigurieren eines bestehenden BeeGFS v8 Clusters

Bearbeiten Sie für einen bestehenden BeeGFS v8-Cluster die Konfigurationsdatei des Management-Dienstes. Bearbeiten Sie beispielsweise die Datei unter `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml` und legen Sie Folgendes fest:

```
tls-disable = true
```

Ergreifen Sie geeignete Maßnahmen, um den Managementdienst sicher neu zu starten, damit die Änderungen wirksam werden.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.