



Aktualisieren Sie die HA-Cluster-Komponenten

BeeGFS on NetApp with E-Series Storage

NetApp
August 23, 2024

Inhalt

- Aktualisieren Sie die HA-Cluster-Komponenten 1
 - BeeGFS-Version aktualisieren 1
 - Upgrade von E-Series Storage-Arrays 4

Aktualisieren Sie die HA-Cluster-Komponenten

BeeGFS-Version aktualisieren

Führen Sie die folgenden Schritte aus, um die BeeGFS-Version des HA-Clusters mithilfe von Ansible zu aktualisieren.

Überblick

BeeGFS folgt einem `major.minor.patch` Versionsschema. Die BeeGFS HA-Ansible-Rollen werden für jede unterstützte `major.minor` Version (z. B. `beegfs_ha_7_2` und `beegfs_ha_7_3`) bereitgestellt. Jede HA-Rolle ist auf die neueste BeeGFS-Patch-Version fixiert, die zum Zeitpunkt der Veröffentlichung der Ansible Sammlung verfügbar ist.

Ansible sollte für alle BeeGFS Upgrades verwendet werden, einschließlich dem Verschieben zwischen größeren, kleineren und Patch-Versionen von BeeGFS. Um BeeGFS zu aktualisieren, müssen Sie zuerst die BeeGFS Ansible-Sammlung aktualisieren, die außerdem die neuesten Fixes und Verbesserungen an der Implementierungs-/Management-Automatisierung und dem zugrunde liegenden HA-Cluster heraufgibt. Selbst nach der Aktualisierung auf die neueste Version der Kollektion wird BeeGFS erst aktualisiert `ansible-playbook` Wird mit dem ausgeführt `-e "beegfs_ha_force_upgrade=true"` Einstellen.



Weitere Informationen zu BeeGFS-Versionen finden Sie im "[BeeGFS Upgrade-Dokumentation](#)".

Getestete Upgrade-Pfade

Jede Version der BeeGFS-Kollektion wird mit spezifischen Versionen von BeeGFS getestet, um die Interoperabilität zwischen allen Komponenten zu gewährleisten. Außerdem werden Tests durchgeführt, um sicherzustellen, dass Upgrades von der von der letzten Version der Sammlung unterstützten BeeGFS-Version(en) auf die in der neuesten Version unterstützten durchgeführt werden können.

Originalversion	Upgrade-Version	Multirail	Details
7.2.6	7.3.2	Ja.	Beegfs-Sammlung von v3.0.1 auf v3.1.0, multirail hinzugefügt
7.2.6	7.2.8	Nein	Beegfs-Sammlung wird von v3.0.1 auf v3.1 aktualisiert
7.2.8	7.3.1	Ja.	Upgrade mit beegfs Collection v3.1.0, multirail hinzugefügt
7.3.1	7.3.2	Ja.	Upgrade mit beegfs Collection v3.1.0
7.3.2	7.4.1	Ja.	Upgrade mit beegfs Collection v3.2.0
7.4.1	7.4.2	Ja.	Upgrade mit beegfs Collection v3.2.0

Schritte beim BeeGFS-Upgrade

In den folgenden Abschnitten werden die Schritte zum Aktualisieren der BeeGFS Ansible Sammlung und BeeGFS selbst beschrieben. Achten Sie besonders auf zusätzliche Schritte für die Aktualisierung von BeeGFS Major oder Minor Versionen.

Schritt: Upgrade der BeeGFS-Sammlung

Bei Erfassungs-Upgrades mit Zugriff auf "[Ansible-Galaxie](#)", Ausführen des folgenden Befehls:

```
ansible-galaxy collection install netapp_eseries.beegfs --upgrade
```

Laden Sie die Sammlung von herunter, um Offline-Sammlungs-Upgrades von zu erhalten "[Ansible-Galaxie](#)"
Durch Klicken auf das gewünschte `Install Version`` Und dann `Download tarball`. Übertragen Sie den
Tarball auf Ihren Ansible-Steuerungsknoten und führen Sie den folgenden Befehl aus.

```
ansible-galaxy collection install netapp_eseries-beegfs-<VERSION>.tar.gz  
--upgrade
```

Siehe "[Sammlungen Werden Installiert](#)" Finden Sie weitere Informationen.

Schritt 2: Aktualisieren Sie den Ansible-Bestand

Nehmen Sie alle erforderlichen oder gewünschten Aktualisierungen der Ansible-Bestandsdateien Ihres Clusters vor. Im "[Hinweise Zum Versionsupgrade](#)"folgenden Abschnitt finden Sie Einzelheiten zu Ihren spezifischen Upgrade-Anforderungen. "[Ansible-Bestandsübersicht](#)"Allgemeine Informationen zur Konfiguration Ihres BeeGFS HA-Bestands finden Sie im Abschnitt.

Schritt 3: Ansible-Playbook aktualisieren (nur bei Aktualisierung von Haupt- oder Nebenversionen)

Wenn Sie zwischen Haupt- oder Unterversionen wechseln, aktualisieren Sie in der `playbook.yml` Datei, die zum Bereitstellen und Warten des Clusters verwendet wird, den Namen der `beegfs_ha_<VERSION>` Rolle, damit die gewünschte Version angezeigt wird. Wenn Sie beispielsweise BeeGFS 7.4 bereitstellen möchten, wäre dies `beegfs_ha_7_4`:

```
- hosts: all  
  gather_facts: false  
  any_errors_fatal: true  
  collections:  
    - netapp_eseries.beegfs  
  tasks:  
    - name: Ensure BeeGFS HA cluster is setup.  
      ansible.builtin.import_role: # import_role is required for tag  
availability.  
        name: beegfs_ha_7_4
```

Weitere Informationen zum Inhalt dieser Playbook-Datei finden Sie im "[Implementieren Sie das BeeGFS HA-Cluster](#)" Abschnitt.

Schritt 4: Führen Sie das BeeGFS-Upgrade aus

So wenden Sie das BeeGFS-Update an:

```
ansible-playbook -i inventory.yml beegfs_ha_playbook.yml -e
"beegfs_ha_force_upgrade=true" --tags beegfs_ha
```

Hinter den Kulissen übernimmt die BeeGFS HA-Rolle:

- Stellen Sie sicher, dass sich das Cluster in einem optimalen Zustand befindet, wobei sich jeder BeeGFS-Service auf seinem bevorzugten Node befindet.
- Versetzen Sie das Cluster in den Wartungsmodus.
- Aktualisieren der HA-Cluster-Komponenten (falls erforderlich)
- Aktualisieren Sie jeden Dateiknoten nacheinander wie folgt:
 - Setzen Sie ihn in den Standby-Modus und führen Sie ein Failover seiner Dienste zum sekundären Knoten durch.
 - BeeGFS-Pakete aktualisieren.
 - Fallback-Services.
- Verschieben Sie das Cluster aus dem Wartungsmodus.

Hinweise zur Versionsaktualisierung

Upgrade von BeeGFS Version 7.2.6 oder 7.3.0

Änderungen an verbindungsbasierter Authentifizierung

BeeGFS-Versionen, die nach 7.3.1 veröffentlicht wurden, erlauben nicht mehr, dass Dienste ohne Angabe von `connAuthFile` Oder Einstellung `connDisableAuthentication=true` In der Konfigurationsdatei des Dienstes. Es wird dringend empfohlen, die verbindungsbasierte Authentifizierungssicherheit zu aktivieren. Siehe "[BeeGFS-Verbindungsbasierte Authentifizierung](#)" Finden Sie weitere Informationen.

Standardmäßig ist der festgelegt `beegfs_ha*` Rollen generieren und verteilen diese Datei und fügen sie auch zum Ansible-Steuerungsknoten bei hinzu

`<playbook_directory>/files/beegfs/<beegfs_mgmt_ip_address>_connAuthFile`. Der `beegfs_client` Die Rolle überprüft auch, ob diese Datei vorhanden ist, und liefert sie an die Clients, sofern verfügbar.



Wenn der `beegfs_client` Die Rolle wurde nicht zur Konfiguration von Clients verwendet. Diese Datei muss manuell auf jeden Client und auf den verteilt werden `connAuthFile` Konfiguration in `beegfs-client.conf` Dateisatz für die Verwendung. Beim Upgrade von einer früheren Version von BeeGFS, bei der die verbindungsbasierte Authentifizierung nicht aktiviert war, verlieren Clients den Zugriff, es sei denn, die auf der Verbindung basierende Authentifizierung ist als Teil des Upgrades durch die Einstellung deaktiviert `beegfs_ha_conn_auth_enabled: false` In `group_vars/ha_cluster.yml` (Nicht empfohlen).

Weitere Details und alternative Konfigurationsoptionen finden "[Festlegen Der Konfiguration Des Gemeinsamen Dateiknotens](#)" Sie im Abschnitt zum Konfigurieren der Verbindungsauthentifizierung.

Upgrade von E-Series Storage-Arrays

Führen Sie die folgenden Schritte aus, um die E-Series Storage-Arrays (Block-Nodes) des HA-Clusters zu aktualisieren.

Überblick

Die NetApp E-Series Storage Arrays Ihres HA Clusters mit der neuesten Firmware auf dem neuesten Stand zu halten, gewährleistet optimale Performance und verbesserte Sicherheit. Firmware-Updates für das Storage Array werden mithilfe von SANtricity OS-, NVSRAM- und Festplatten-Firmware-Dateien angewendet.



Obwohl ein Upgrade der Storage Arrays während des Online-Betriebs des HA-Clusters möglich ist, sollte das Cluster bei allen Upgrades in den Wartungsmodus versetzt werden.

Upgrade-Schritte für Block-Nodes

Im Folgenden wird beschrieben, wie die Firmware der Storage-Arrays mithilfe der `Netapp_Eseries.Santricity` Ansible-Sammlung aktualisiert wird. Bevor Sie fortfahren, lesen "[Upgrade-Überlegungen](#)" Sie das zur Aktualisierung von E-Series Systemen.



Ein Upgrade auf SANtricity OS 11.80 oder höhere Versionen ist nur ab 11.70.5P1 möglich. Das Speicher-Array muss vor der Anwendung weiterer Upgrades zuerst auf 11.70.5P1 aktualisiert werden.

1. Überprüfen Sie den Ansible Control-Node mithilfe der neuesten SANtricity Ansible Sammlung.
 - Bei Erfassungs-Updates mit Zugriff auf "[Ansible-Galaxie](#)", Ausführen des folgenden Befehls:

```
ansible-galaxy collection install netapp_eseries.santricity --upgrade
```

- Laden Sie für Offline-Updates den Sammeltarball von herunter "[Ansible-Galaxie](#)", übertragen Sie ihn auf Ihren Steuerungsknoten und führen Sie Folgendes aus:

```
ansible-galaxy collection install netapp_eseries-santricity-  
<VERSION>.tar.gz --upgrade
```

Siehe "[Sammlungen Werden Installiert](#)" Finden Sie weitere Informationen.

2. Holen Sie sich die neueste Firmware für Ihr Speicher-Array und die Laufwerke.
 - a. Laden Sie die Firmware-Dateien herunter.
 - **SANtricity OS und NVSRAM:** Navigieren "[NetApp Support Website](#)" Sie zum und laden Sie die neueste Version von SANtricity OS und NVSRAM für Ihr Speicherarray-Modell herunter.
 - **Laufwerksfirmware:** Navigieren "[E-Series Festplatten-Firmware-Website](#)" Sie zum und laden Sie die neueste Firmware für jedes Laufwerkmodell Ihres Speicherarrays herunter.
 - b. Speichern Sie SANtricity OS-, NVSRAM- und Laufwerk-Firmware-Dateien im `<inventory_directory>/packages` Verzeichnis Ihres Ansible Control Node.

- Bei Bedarf aktualisieren Sie die Ansible-Bestandsdateien Ihres Clusters, damit alle Storage-Arrays (Block-Nodes), die aktualisiert werden müssen, einbezogen werden. Weitere Informationen finden Sie im ["Ansible-Bestandsübersicht"](#) Abschnitt.
- Stellen Sie sicher, dass sich das Cluster in einem optimalen Zustand befindet, wobei sich jeder BeeGFS-Service auf seinem bevorzugten Node befindet. Weitere Informationen finden Sie unter ["Untersuchen Sie den Status des Clusters"](#) .
- Versetzen Sie das Cluster gemäß den Anweisungen in in ["Versetzen Sie das Cluster in den Wartungsmodus"](#)den Wartungsmodus.
- Erstellen Sie ein neues Ansible-Playbook mit dem Namen `update_block_node_playbook.yml`. Füllen Sie das Playbook mit den folgenden Inhalten aus und ersetzen Sie die Versionen des SANtricity Betriebssystems, des NVSRAM und der Festplatten-Firmware auf Ihren gewünschten Upgrade-Pfad:

```
- hosts: eseries_storage_systems
gather_facts: false
any_errors_fatal: true
collections:
  - netapp_eseries.santricity
vars:
  eseries_firmware_firmware: "packages/<SantricityOS>.dlp"
  eseries_firmware_nvram: "packages/<NVSRAM>.dlp"
  eseries_drive_firmware_firmware_list:
    - "packages/<drive_firmware>.dlp"
  eseries_drive_firmware_upgrade_drives_online: true

tasks:
  - name: Configure NetApp E-Series block nodes.
    import_role:
      name: nar_santricity_management
```

- Führen Sie über Ihren Ansible-Steuerknoten den folgenden Befehl aus, um die Updates zu starten:

```
ansible-playbook -i inventory.yml update_block_node_playbook.yml
```

- Überprüfen Sie nach Abschluss des Playbook, ob sich jedes Speicher-Array in einem optimalen Zustand befindet.
- Entfernen Sie das Cluster aus dem Wartungsmodus und überprüfen Sie, ob sich das Cluster in einem optimalen Zustand befindet, wobei sich jeder BeeGFS-Service auf seinem bevorzugten Node befindet.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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 BESCHRÄNKT 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, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT 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 VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER 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.