Erweitertes System konfigurieren

StorageGRID

NetApp
March 12, 2025

Inhalt

Erweitertes System konfigurieren

Konfiguration Schritte nach Erweiterung

Nach Abschluss einer Erweiterung müssen Sie weitere Integrations- und Konfigurationsschritte durchführen.

Über diese Aufgabe

Sie müssen die unten aufgeführten Konfigurationsaufgaben für die Grid-Nodes oder Standorte, die Sie in Ihrer Erweiterung hinzufügen, ausführen. Einige Aufgaben können optional sein, je nachdem, welche Optionen bei der Installation und Administration des Systems ausgewählt wurden und wie Sie die während der Erweiterung hinzugefügten Knoten und Standorte konfigurieren möchten.

Schritte

1. Wenn Sie eine Site hinzugefügt haben:
   - "Erstellen Sie einen Speicherpool" Für den Standort und jede für die neuen Storage-Nodes ausgewählte Speicherklasse.
   - Vergewissern Sie sich, dass die ILM-Richtlinie den neuen Anforderungen entspricht. Wenn Regeländerungen erforderlich sind, "Erstellen Sie neue Regeln" und "Aktualisieren Sie die ILM-Richtlinie". Wenn die Regeln bereits korrekt sind, ohne dass die Regeln "Aktivieren Sie eine neue Richtlinie"geändert werden, um sicherzustellen, dass StorageGRID die neuen Nodes verwendet.
   - Vergewissern Sie sich, dass auf NTP-Server (Network Time Protocol) von diesem Standort aus zugegriffen werden kann. Siehe "Managen von NTP-Servern".

   > Vergewissern Sie sich, dass mindestens zwei Nodes an jedem Standort auf mindestens vier externe NTP-Quellen zugreifen können. Wenn nur ein Node an einem Standort die NTP-Quellen erreichen kann, treten Probleme mit dem Timing auf, wenn dieser Node ausfällt. Durch die Festlegung von zwei Nodes pro Standort als primäre NTP-Quellen ist zudem ein genaues Timing gewährleistet, wenn ein Standort vom Rest des Grid isoliert ist.

2. Wenn Sie einem vorhandenen Standort einen oder mehrere Storage-Nodes hinzugefügt haben:
   - "Zeigen Sie Details zum Speicherpool an" Um zu bestätigen, dass jeder hinzugefügte Node in den erwarteten Speicherpools enthalten und in den erwarteten ILM-Regeln verwendet wird.
   - Vergewissern Sie sich, dass die ILM-Richtlinie den neuen Anforderungen entspricht. Wenn Regeländerungen erforderlich sind, "Erstellen Sie neue Regeln" und "Aktualisieren Sie die ILM-Richtlinie". Wenn die Regeln bereits korrekt sind, ohne dass die Regeln "Aktivieren Sie eine neue Richtlinie"geändert werden, um sicherzustellen, dass StorageGRID die neuen Nodes verwendet.
   - "Vergewissern Sie sich, dass der Speicherknoten aktiv ist" Und in der Lage, Objekte aufzunehmen.
   - Wenn Sie die empfohlene Anzahl an Storage-Nodes nicht hinzufügen konnten, sollten Sie einen Ausgleich für Daten finden, die nach der Löschung codiert wurden. Siehe "Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes".
3. Wenn Sie einen Gateway-Node hinzugefügt haben:
   - Wenn Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) für Client-Verbindungen verwendet werden, fügen Sie optional den Gateway-Node einer HA-Gruppe hinzu. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe "Konfigurieren Sie

Hochverfügbarkeitsgruppen".

4. Wenn Sie einen Admin-Node hinzugefügt haben:
   a. Wenn SSO (Single Sign-On) für Ihr StorageGRID-System aktiviert ist, erstellen Sie für den neuen Admin-Node eine Vertrauensbasis von einer Vertrauensbasis. Sie können sich erst beim Knoten anmelden, wenn Sie diese Vertrauensstellung von vertrauenswürdigen Parteien erstellt haben. Siehe "Konfigurieren Sie Single Sign-On".
   b. Wenn Sie den Load Balancer-Service auf Admin-Nodes verwenden möchten, fügen Sie optional den neuen Admin-Node einer HA-Gruppe hinzu. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe "Konfigurieren Sie Hochverfügbarkeitsgruppen".
   c. Kopieren Sie optional die Admin-Node-Datenbank vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie das Attribut und die Audit-Informationen auf jedem Admin-Knoten konsistent halten möchten. Siehe "Kopieren Sie die Admin-Knoten-Datenbank".
   d. Kopieren Sie optional die Prometheus-Datenbank vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Metriken auf jedem Admin-Knoten konsistent halten möchten. Siehe "Kopieren Sie die Prometheus-Kennzahlen".
   e. Kopieren Sie optional die vorhandenen Audit-Protokolle vom primären Admin-Node zum ErweiterungAdmin-Node, wenn Sie die historischen Protokollinformationen auf jedem Admin-Knoten konsistent halten möchten. Siehe "Prüfprotokolle kopieren".
5. Um zu überprüfen, ob Erweiterungsknoten mit einem nicht vertrauenswürdigen Client-Netzwerk hinzugefügt wurden, oder um zu ändern, ob das Client-Netzwerk eines Knotens nicht vertrauenswürdig oder vertrauenswürdig ist, gehen Sie zu **CONFIGURATION** > **Security** > **Firewall Control**.

   Wenn das Client-Netzwerk auf dem Erweiterungsknoten nicht vertrauenswürdig ist, müssen Verbindungen zum Knoten im Client-Netzwerk über einen Load Balancer-Endpunkt hergestellt werden. Siehe "Konfigurieren von Load Balancer-Endpunkten" und "Management der Firewall-Kontrollen".

6. Konfigurieren Sie den DNS.

   Wenn Sie für jeden Grid-Node DNS-Einstellungen separat angegeben haben, müssen Sie für die neuen Nodes benutzerdefinierte DNS-Einstellungen pro Node hinzufügen. Siehe "Ändern der DNS-Konfiguration für einen einzelnen Grid-Node".

Um einen ordnungsgemäßen Betrieb zu gewährleisten, geben Sie zwei oder drei DNS-Server an. Wenn Sie mehr als drei angeben, können aufgrund bekannter Einschränkungen des Betriebssystems auf einigen Plattformen nur drei verwendet werden. Wenn Sie in Ihrer Umgebung Routingbeschränkungen haben, können Sie "Passen Sie die DNS-Serverliste an"für einzelne Knoten (in der Regel alle Knoten an einem Standort) einen anderen Satz von bis zu drei DNS-Servern verwenden.

Verwenden Sie nach Möglichkeit DNS-Server, auf die jeder Standort lokal zugreifen kann, um sicherzustellen, dass ein Inselstandort die FQDNs für externe Ziele auflösen kann.

Vergewissern Sie sich, dass der Speicherknoten aktiv ist

Nachdem ein Erweiterungsvorgang abgeschlossen ist, der neue Speicherknoten hinzugefügt hat, sollte das StorageGRID-System automatisch mit den neuen Speicherknoten beginnen. Sie müssen das StorageGRID-System verwenden, um sicherzustellen, dass der neue Speicherknoten aktiv ist.

Schritte

1. Melden Sie sich mit einem beim Grid-Manager an"Unterstützter Webbrowser".
2. Wählen Sie **NODES** > ***Expansion Storage Node*** > **Storage** aus.
3. Bewegen Sie den Cursor über die Grafik **verwendeter Speicher - Objektdaten**, um den Wert für **Used** anzuzeigen, der die Menge des gesamten nutzbaren Speicherplatzes ist, der für Objektdaten verwendet wurde.
4. Vergewissern Sie sich, dass der Wert von **verwendet** erhöht wird, wenn Sie den Cursor nach rechts auf dem Diagramm bewegen.

Admin-Knoten-Datenbank kopieren

Beim Hinzufügen von Admin-Nodes durch ein Erweiterungsverfahren können Sie optional die Datenbank vom primären Admin-Node zum neuen Admin-Node kopieren. Durch das Kopieren der Datenbank können Sie historische Informationen über Attribute, Warnmeldungen und Warnmeldungen aufbewahren.

Bevor Sie beginnen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Der StorageGRID-Softwareaktivierungsprozess erstellt eine leere Datenbank für den NMS-Dienst auf dem Erweiterungs-Admin-Knoten. Wenn der NMS-Dienst auf dem Erweiterungs-Admin-Knoten startet, zeichnet er Informationen für Server und Dienste auf, die derzeit Teil des Systems sind oder später hinzugefügt werden. Diese Admin-Knoten-Datenbank enthält die folgenden Informationen:

- Meldungsverlauf
- Historische Attributdaten, die in Diagrammen im Legacy-Stil auf der Seite Knoten verwendet werden

Um sicherzustellen, dass die Admin-Node-Datenbank zwischen den Knoten konsistent ist, können Sie die Datenbank vom primären Admin-Node auf den Erweiterungs-Admin-Node kopieren.

> Das Kopieren der Datenbank vom primären Admin-Node (der__Source Admin-Node_) zu einem Erweiterungs-Admin-Node kann bis zu mehrere Stunden dauern. In diesem Zeitraum ist der Grid Manager nicht zugänglich.

Führen Sie diese Schritte aus, um den MI-Dienst und den Management-API-Dienst sowohl auf dem primären Admin-Node als auch auf dem Erweiterungs-Admin-Node zu beenden, bevor Sie die Datenbank kopieren.

Schritte

1. Führen Sie die folgenden Schritte auf dem primären Admin-Knoten aus:
   a. Melden Sie sich beim Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
      iii. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
      iv. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

b. Führen Sie den folgenden Befehl aus: `recover-access-points`

c. Geben Sie die Provisionierungs-Passphrase ein.

d. Halten Sie den MI-Dienst an: `service mi stop`

e. Beenden Sie den Management Application Program Interface (Management API)-Service: `service mgmt-api stop`

2. Führen Sie die folgenden Schritte auf dem Erweiterungs-Admin-Knoten aus:

a. Melden Sie sich beim Erweiterungs-Admin-Knoten an:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

iii. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`

iv. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

b. Halten Sie den MI-Dienst an: `service mi stop`

c. Stoppen Sie den Management-API-Service: `service mgmt-api stop`

d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Eingabe:`ssh-add`

e. Geben Sie das in der Datei aufgeführte SSH-Zugriffspasswort ein `Passwords.txt`.

f. Kopieren Sie die Datenbank vom Quell-Admin-Node auf den Erweiterungs-Admin-Node: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die MI-Datenbank auf dem Erweiterungs-Admin-Node überschreiben möchten.

Die Datenbank und ihre historischen Daten werden auf den Erweiterungs-Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den Erweiterungs-Admin-Knoten.

h. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Eingabe:`ssh-add -D`

3. Starten Sie die Dienste auf dem primären Admin-Node neu: `service servermanager start`

Kopieren Sie die Prometheus-Kennzahlen

Nach dem Hinzufügen eines neuen Admin-Knotens können Sie optional die historischen Metriken kopieren, die von Prometheus vom primären Admin-Node erhalten wurden, zum neuen Admin-Node. Durch das Kopieren der Metriken wird sichergestellt, dass historische Metriken zwischen Admin-Nodes konsistent sind.

Bevor Sie beginnen

- Der neue Admin-Node wird installiert und ausgeführt.
- Sie haben die `Passwords.txt` Datei.
- Sie haben die Provisionierungs-Passphrase.

Über diese Aufgabe

Wenn Sie einen Admin-Knoten hinzufügen, erstellt der Software-Installationsprozess eine neue Prometheus-Datenbank. Sie können die historischen Kennzahlen zwischen den Knoten konsistent halten, indem Sie die

Prometheus-Datenbank vom primären Admin-Node (den_Source Admin-Node_) auf den neuen Admin-Node kopieren.

> Das Kopieren der Prometheus-Datenbank dauert möglicherweise ein Stunde oder länger. Einige Grid Manager-Funktionen sind nicht verfügbar, während Dienste auf dem Quell-Admin-Node angehalten werden.

Schritte

1. Melden Sie sich beim Quell-Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
2. Beenden Sie vom Quell-Admin-Node den Prometheus-Service: `service prometheus stop`
3. Führen Sie auf dem neuen Admin-Knoten die folgenden Schritte aus:
   a. Melden Sie sich beim neuen Admin-Knoten an:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
      iii. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
      iv. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   b. Stoppen Sie den Prometheus-Service: `service prometheus stop`
   c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Eingabe:`ssh-add`
   d. Geben Sie das in der Datei aufgeführte SSH-Zugriffspasswort ein `Passwords.txt`.
   e. Kopieren Sie die Prometheus-Datenbank vom Quell-Admin-Node auf den neuen Admin-Node: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um zu bestätigen, dass Sie die neue Prometheus-Datenbank auf dem neuen Admin-Knoten zerstören möchten.

      Die ursprüngliche Prometheus-Datenbank und ihre historischen Daten werden auf den neuen Admin-Knoten kopiert. Wenn der Kopiervorgang abgeschlossen ist, startet das Skript den neuen Admin-Knoten. Der folgende Status wird angezeigt:

```
Database cloned, starting services
```

   a. Wenn Sie keinen passwortlosen Zugriff auf andere Server mehr benötigen, entfernen Sie den privaten Schlüssel vom SSH-Agent. Geben Sie Ein:

```
ssh-add -D
```

4. Starten Sie den Prometheus-Service auf dem Quell-Admin-Node neu.

```
service prometheus start
```

Prüfprotokolle kopieren

Wenn Sie einen neuen Admin-Node durch ein Erweiterungsverfahren hinzufügen, protokolliert sein AMS-Service nur Ereignisse und Aktionen, die nach dem Beitritt zum System auftreten. Nach Bedarf können Sie Audit-Protokolle von einem zuvor installierten Admin-Node auf den neuen Erweiterungs-Admin-Node kopieren, sodass er mit dem Rest des StorageGRID Systems synchronisiert ist.

Bevor Sie beginnen

- Sie haben die erforderlichen Erweiterungsschritte zum Hinzufügen eines Admin-Knotens abgeschlossen.
- Sie haben die `Passwords.txt` Datei.

Über diese Aufgabe

Um historische Audit-Meldungen auf einem neuen Admin-Knoten verfügbar zu machen, müssen Sie die Audit-Log-Dateien manuell von einem vorhandenen Admin-Knoten in den Erweiterungs-Admin-Knoten kopieren.

> Standardmäßig werden Audit-Informationen an das Audit-Protokoll auf Admin-Knoten gesendet. Sie können diese Schritte überspringen, wenn eine der folgenden Maßnahmen zutrifft:
>
> - Sie haben einen externen Syslog-Server konfiguriert und Audit-Protokolle werden jetzt an den Syslog-Server anstatt an Admin-Knoten gesendet.
> - Sie haben ausdrücklich angegeben, dass Audit-Meldungen nur auf den lokalen Knoten gespeichert werden sollten, die sie generiert haben.
>
> Weitere Informationen finden Sie unter "Konfigurieren von Überwachungsmeldungen und Protokollzielen" .

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@_primary_Admin_Node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.
2. Beenden Sie den AMS-Dienst, um zu verhindern, dass er eine neue Datei erstellt: `service ams stop`
3. Navigieren Sie zum Verzeichnis für den Audit-Export:

   ```
   cd /var/local/log
   ```

4. Benennen Sie die Quelldatei `audit.log` um, um sicherzustellen, dass die Datei auf dem Erweiterungsadministratorknoten, in den Sie kopieren, nicht überschrieben wird:

```
ls -l
mv audit.log _new_name_.txt
```

5. Kopieren Sie alle Audit-Log-Dateien in den Zielspeicherort auf dem Erweiterungs-Admin-Node:

   `scp -p * IP_address:/var/local/log`

6. Wenn Sie zur Eingabe der Passphrase für aufgefordert `/root/.ssh/id_rsa` werden, geben Sie das SSH-Zugriffspasswort für den in der Datei aufgeführten primären Admin-Knoten ein `Passwords.txt`.
7. Originaldatei wiederherstellen `audit.log`:

   `mv new_name.txt audit.log`

8. AMS-Dienst starten:

   `service ams start`

9. Melden Sie sich vom Server ab:

   `exit`

10. Melden Sie sich beim Erweiterungs-Admin-Knoten an:
    a. Geben Sie den folgenden Befehl ein: `ssh admin@expansion_Admin_Node_IP`
    b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
    c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
    d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

    Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

11. Benutzer- und Gruppeneinstellungen für die Audit-Log-Dateien aktualisieren:

    ```
    cd /var/local/log

    chown ams-user:bycast *
    ```

12. Melden Sie sich vom Server ab:

    `exit`

Ausgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes

Nach dem Hinzufügen von Storage Nodes können Sie das Ausgleichen von Fragmenten, die mit Erasure Coding (EC) codiert wurden, mithilfe der vorhandenen und neuen Storage Nodes verteilen.

Bevor Sie beginnen

- Sie haben die Erweiterungsschritte zum Hinzufügen der neuen Speicherknoten abgeschlossen.
- Sie haben die überprüft"Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind".
- Sie wissen, dass replizierte Objektdaten bei diesem Verfahren nicht verschoben werden und dass beim EC-Ausgleichverfahren die replizierte Datennutzung auf jedem Storage Node nicht berücksichtigt wird, wenn festgestellt wird, wo Daten mit Erasure Coding verschoben werden.
- Sie haben die `Passwords.txt` Datei.

Was passiert, wenn dieses Verfahren ausgeführt wird

Beachten Sie vor dem Starten des Verfahrens Folgendes:

- Das EC-Ausgleichverfahren startet nicht, wenn ein oder mehrere Volumes offline (unmounted) sind oder online (gemountet) sind, sondern sich in einem Fehlerzustand befinden.
- Das EG-Ausgleichverfahren reserviert vorübergehend einen großen Speicher. Storage-Warnmeldungen werden möglicherweise ausgelöst, aber nach Abschluss des Ausgleichs werden sie gelöst. Wenn nicht genügend Speicherplatz für die Reservierung vorhanden ist, schlägt das EC-Ausgleichverfahren fehl. Speicherreservierungen werden freigegeben, wenn der EC-Ausgleichvorgang abgeschlossen ist, unabhängig davon, ob der Vorgang fehlgeschlagen oder erfolgreich war.
- Wenn ein Volume offline geschaltet wird, während der EC-Neuausgleich ausgeführt wird, wird der Neuausgleich beendet. Alle bereits verschobenen Datenfragmente bleiben an ihren neuen Speicherorten und es gehen keine Daten verloren.

  Sie können den Vorgang erneut ausführen, nachdem alle Volumes wieder online sind.

- Wenn das EC-Ausgleichverfahren ausgeführt wird, kann die Performance von ILM-Vorgängen und S3 Client-Operationen beeinträchtigt werden.

  > ⓘ S3-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Ausgleichs fehlschlagen, wenn ihr Abschluss mehr als 24 Stunden erfordert. PUT-Vorgänge mit langer Dauer schlagen fehl, wenn die geltende ILM-Regel eine ausgewogene oder strikte Platzierung bei der Aufnahme verwendet. Der folgende Fehler wird gemeldet: `500 Internal Server Error`.

- Bei diesem Verfahren haben alle Knoten eine Speicherkapazitätsgrenze von 80 %. Knoten, die diese Grenze überschreiten, aber immer noch unterhalb der Zieldatenpartition gespeichert werden, werden von folgenden Elementen ausgeschlossen:
  - Der Wert für die Unwucht des Standorts
  - Alle Bedingungen für den Abschluss eines Jobs

  > ⓘ Die Zieldatenpartition wird berechnet, indem die Gesamtdaten für einen Standort durch die Anzahl der Knoten dividiert werden.

- **Bedingungen für die Fertigstellung des Jobs**. Das EC-Ausgleichverfahren gilt als abgeschlossen, wenn eine der folgenden Bedingungen erfüllt ist:
  - Es können keine Daten mit Erasure Coded verschoben werden.
  - Die Daten in allen Knoten liegen innerhalb einer Abweichung von 5% von der Zieldatenpartition.
  - Das Verfahren läuft seit 30 Tagen.

Schritte

1. Überprüfen Sie die aktuellen Objekt-Storage-Details für den Standort, den Sie ausgleichen möchten.
   a. Wählen Sie **KNOTEN**.
   b. Wählen Sie den ersten Speicherknoten am Standort aus.
   c. Wählen Sie die Registerkarte **Storage** aus.
   d. Bewegen Sie den Mauszeiger über das Diagramm Speicher verwendet – Objektdaten, um die aktuelle Menge replizierter Daten und mit Löschungscodes versehene Daten auf dem Speicher-Node anzuzeigen.
   e. Wiederholen Sie diese Schritte, um die anderen Speicherknoten am Standort anzuzeigen.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

      Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.
3. Starten Sie den Vorgang:

   `reBalance-Data Start --site "*site-Name*"

   Geben Sie für „*site-Name*“ den ersten Standort an, an dem Sie einen oder mehrere neue Storage-Nodes hinzugefügt haben. In Angebote einschließen `site-name`.

   Der EC-Ausgleichvorgang startet, und eine Job-ID wird zurückgegeben.
4. Kopieren Sie die Job-ID.
5. Überwachen Sie den Status des EC-Ausgleichs.
   - So zeigen Sie den Status eines einzelnen EC-Ausgleichs an:

     `rebalance-data status --job-id job-id`

     Geben Sie für *`job-id`* die ID an, die beim Starten des Verfahrens zurückgegeben wurde.
   - So zeigen Sie den Status des aktuellen EC-Ausgleichs und aller zuvor abgeschlossenen Verfahren an:

     `rebalance-data status`

   > Hilfe zum Befehl zum Ausgleich von Daten erhalten:
   >
   > `rebalance-data --help`
6. Führen Sie weitere Schritte aus, basierend auf dem zurückgegebenen Status:
   - Wenn `State` dies der Fall ist `In progress`, wird der EC-Ausgleichsoperation noch ausgeführt. Sie sollten das Verfahren regelmäßig überwachen, bis es abgeschlossen ist.

     Verwenden Sie den `Site Imbalance` Wert, um zu beurteilen, wie unausgewogen Daten aus dem

Löschcode in den Storage-Nodes am Standort verwendet werden. Dieser Wert kann zwischen 1.0 und 0 liegen, wobei 0 bedeutet, dass die Datennutzung für das Erasure Coding vollständig auf alle Storage-Nodes am Standort verteilt ist.

Der EC-Neuausgleich-Job gilt als abgeschlossen und wird angehalten, wenn sich die Daten in allen Knoten innerhalb einer Abweichung von 5 % von der Zieldatenpartition befinden.

- Wenn `State` ist `Success`, optionalPrüfen von Objekt-Storage, um die aktualisierten Details für die Website anzuzeigen.

  Daten mit Erasure-Coding-Verfahren sollten nun besser auf die Storage-Nodes am Standort abgestimmt sein.

- Wenn `State` `Failure`:

  i. Vergewissern Sie sich, dass alle Speicherknoten am Standort mit dem Raster verbunden sind.

  ii. Überprüfen Sie, ob Warnmeldungen vorliegen, die sich auf diese Speicherknoten auswirken könnten, und beheben Sie sie.

  iii. Starten Sie das EC-Neuausgleich-Verfahren neu:

  ```
  rebalance-data start --job-id job-id
  ```

  iv. Den Status anzeigen Des neuen Verfahrens. Falls `State` noch vorhanden `Failure`, wenden Sie sich an den technischen Support.

7. Wenn das EC-Ausgleichverfahren zu viel Last generiert (beispielsweise sind Ingest-Operationen betroffen), unterbrechen Sie den Vorgang.

   ```
   rebalance-data pause --job-id job-id
   ```

8. Wenn Sie das EC-Ausgleichverfahren beenden müssen (z. B. um ein StorageGRID-Software-Upgrade durchzuführen), geben Sie Folgendes ein:

   ```
   rebalance-data terminate --job-id job-id
   ```

   Wenn Sie eine EC-Neuverteilung beenden, bleiben alle Datenfragmente, die bereits verschoben wurden, an ihren neuen Speicherorten. Daten werden nicht zurück an den ursprünglichen Speicherort verschoben.

9. Wenn Sie Erasure Coding an mehreren Standorten verwenden, führen Sie dieses Verfahren für alle anderen betroffenen Standorte aus.