# Erweitertes System konfigurieren

StorageGRID

NetApp
October 03, 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 ausführen, die Sie in Ihrer Erweiterung hinzufügen. Einige Aufgaben können optional sein, je nachdem, welche Optionen bei der Installation und Verwaltung des Systems ausgewählt wurden, und wie Sie die während der Erweiterung hinzugefügten Grid-Nodes konfigurieren möchten.

**Schritte**

1. Wenn Sie einen Speicherknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus:
   a. Überprüfen Sie die in Ihren ILM-Regeln verwendeten Speicherpools, um sicherzustellen, dass der neue Speicher verwendet wird. Siehe Objektmanagement mit ILM.
      - Wenn Sie einen Standort hinzufügen, erstellen Sie einen Speicherpool für den Standort und aktualisieren Sie ILM-Regeln, um den neuen Speicherpool zu verwenden.
      - Wenn Sie einem vorhandenen Standort einen Speicherknoten hinzugefügt haben, bestätigen Sie, dass der neue Node die richtige Speicherklasse verwendet.

      > Standardmäßig wird der Speicherklasse Alle Speicherknoten ein neuer Speicherknoten zugewiesen und zu Speicherpools hinzugefügt, die diese Klasse für den Standort verwenden. Wenn ein neuer Knoten eine benutzerdefinierte Speicherklasse verwenden soll, müssen Sie diesen manuell der benutzerdefinierten Klasse zuweisen (**ILM Speicherstufen**).

   b. Vergewissern Sie sich, dass der Speicherknoten Objekte erfasst. Siehe Vergewissern Sie sich, dass der Speicherknoten aktiv ist.
   c. Ausgleich von Daten mit Verfahren zur Einhaltung von Datenkonsistenz (nur wenn die empfohlene Anzahl von Storage-Nodes nicht hinzugefügt werden konnte) SieheAusgleich von Daten, die im Erasure Coding ausgeführt werden, nach dem Hinzufügen von Storage-Nodes.
2. Wenn Sie einen Gateway-Node hinzugefügt haben, führen Sie die folgende Konfigurationsaufgabe aus:
   - Wenn Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) für Client-Verbindungen verwendet werden, fügen Sie optional den Gateway-Node einer HA-Gruppe hinzu. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe StorageGRID verwalten.
3. Wenn Sie einen Admin-Node hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus:
   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 dieses Vertrauen der Vertrauensbasis erstellen. SieheKonfigurieren 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 **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen** aus, um die Liste der vorhandenen HA-Gruppen zu überprüfen und den neuen Knoten hinzuzufügen. Siehe StorageGRID verwalten.

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.

f. Konfigurieren Sie optional den Zugriff auf das System für Audit-Zwecke über eine NFS- oder CIFS-Dateifreigabe. Siehe StorageGRID verwalten.

> ⓘ Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

g. Ändern Sie optional den bevorzugten Absender für Benachrichtigungen. Sie können den Erweiterungs-Admin-Knoten zum bevorzugten Absender machen. Andernfalls sendet ein vorhandener als bevorzugter Absender konfigurierter Admin-Node weiterhin Benachrichtigungen, einschließlich AutoSupport-Nachrichten, SNMP-Benachrichtigungen, Alarm-E-Mails und Alarm-E-Mails (Legacy-System). Siehe StorageGRID verwalten.

4. Wenn Sie einen Archivknoten hinzugefügt haben, führen Sie die folgenden Konfigurationsaufgaben aus.

   a. Konfigurieren Sie die Verbindung des Archiv-Knotens mit dem angestrebten externen Archiv-Storage-System. Wenn Sie die Erweiterung abgeschlossen haben, befinden sich Archiv-Knoten in einem Alarmzustand, bis Sie die Verbindungsinformationen über die Komponente **ARC Ziel** konfigurieren. Siehe StorageGRID verwalten.

   b. Aktualisieren Sie die ILM-Richtlinie, um Objektdaten über den neuen Archivierungs-Node zu archivieren. Siehe Objektmanagement mit ILM.

   c. Konfigurieren Sie benutzerdefinierte Alarme für die Attribute, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten von Archiv-Nodes verwendet werden. Siehe StorageGRID verwalten.

5. Um zu prüfen, 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 Network UnTrusted Client Network**.

   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 StorageGRID verwalten.

6. Konfigurieren Sie das Domain Name System (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.

   Eine Best Practice besteht in der netzweiten DNS-Server-Liste, die einige DNS-Server enthält, auf die von jedem Standort aus lokal zugegriffen werden kann. Wenn Sie gerade einen neuen Standort hinzugefügt haben, fügen Sie der Grid-weiten DNS-Konfiguration neue DNS-Server für den Standort hinzu.

Geben Sie zwei bis sechs IPv4-Adressen für DNS-Server an. Wählen Sie DNS-Server aus, auf die jeder Standort lokal zugreifen kann, wenn das Netzwerk landet. Damit soll sichergestellt werden, dass ein islanded-Standort weiterhin Zugriff auf den DNS-Dienst hat. Nach der Konfiguration der DNS-Serverliste für das gesamte Grid können Sie die DNS-Serverliste für jeden Knoten weiter anpassen. Weitere Informationen finden Sie unter Ändern der DNS-Konfiguration für einen einzelnen Grid-Node..

7. Wenn Sie einen neuen Standort hinzugefügt haben, vergewissern Sie sich, dass auf die NTP-Server (Network Time Protocol) von diesem Standort aus zugegriffen werden kann. Siehe Konfigurieren Sie NTP-Server.

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.

# 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 bei Grid Manager an Unterstützter Webbrowser.
2. Wählen Sie **NODES *Erweiterungs-Storage-Node* Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm **verwendete Speicherung - Objektdaten**, um den Wert für **verwendet** anzuzeigen. Dies ist die Menge des insgesamt nutzbaren Speicherplatzes, 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.

**Was Sie benötigen**

- 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
- Alarmverlauf
- Historische Attributdaten, die in den Diagrammen und Textberichten verwendet werden, die auf der Seite **SUPPORT Tools Grid Topology** verfügbar sind

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 im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   b. Führen Sie den folgenden Befehl aus: `recover-access-points`
   c. Geben Sie die Provisionierungs-Passphrase ein.
   d. Beenden SIE DEN MI-Dienst: `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 im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   b. Beenden SIE DEN MI-Dienst: `service mi stop`
   c. Beenden Sie den Management API-Service: `service mgmt-api stop`
   d. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`
   e. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

f. Kopieren Sie die Datenbank vom Quell-Admin-Knoten auf den Erweiterungs-Admin-Knoten: `/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. Geben Sie Ein:`ssh-add -D`

3. Starten Sie die Dienste auf dem primären Admin-Knoten 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.

**Was Sie benötigen**

- 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
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 im aufgeführte Passwort ein `Passwords.txt` Datei:

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

iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

b. Stoppen Sie den Prometheus Service: `service prometheus stop`

c. Fügen Sie den SSH-privaten Schlüssel zum SSH-Agenten hinzu. Geben Sie Ein:`ssh-add`

d. Geben Sie das SSH-Zugriffspasswort ein, das im aufgeführt ist `Passwords.txt` Datei:

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.

**Was Sie benötigen**

- 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.

Siehe Konfigurieren von Überwachungsmeldungen und Protokollzielen Entsprechende Details.

**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 im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Stoppen Sie den AMS-Dienst, um zu verhindern, dass eine neue Datei erstellt wird: `service ams stop`
3. Benennen Sie den um `audit.log` Datei um sicherzustellen, dass die Datei auf dem Erweiterungs-Admin-Knoten nicht überschrieben wird, in den Sie sie kopieren:

   ```
   cd /var/local/audit/export
   ls -l
   mv audit.log new_name.txt
   ```

4. Kopieren Sie alle Audit-Log-Dateien in den Erweiterungs-Admin-Node:

   ```
   scp -p * IP_address:/var/local/audit/export
   ```

5. Wenn Sie zur Eingabe der Passphrase für aufgefordert werden `/root/.ssh/id_rsa`Geben Sie das SSH-Zugriffskennwort für den primären Admin-Node ein, der im aufgeführt ist `Passwords.txt` Datei:
6. Stellen Sie das Original wieder her `audit.log` Datei:

   ```
   mv new_name.txt audit.log
   ```

7. AMS-Dienst starten:

   ```
   service ams start
   ```

8. Melden Sie sich vom Server ab:

   ```
   exit
   ```

9. 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 im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

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

```
cd /var/local/audit/export
chown ams-user:bycast *
```

11. Melden Sie sich vom Server ab:

```
exit
```

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

In einigen Fällen müssen Sie möglicherweise nach dem Hinzufügen neuer Storage-Nodes einen Ausgleich für Daten schaffen, die mit Erasure Coding versehen sind.

**Was Sie benötigen**

- Sie haben die Erweiterungsschritte zum Hinzufügen der neuen Speicherknoten abgeschlossen.
- Sie haben die geprüft Überlegungen zur Lastverteilung bei Daten, die mit Erasure Coding versehen sind.

> Führen Sie diesen Vorgang nur aus, wenn die Warnung **Low Object Storage** für einen oder mehrere Speicherknoten an einem Standort ausgelöst wurde und Sie die empfohlene Anzahl neuer Speicherknoten nicht hinzufügen konnten.

- 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:

**Über diese Aufgabe**

Wenn das EC-Ausgleichverfahren ausgeführt wird, ist die Performance von ILM-Vorgängen sowie S3- und Swift-Client-Operationen wahrscheinlich beeinträchtigt. Aus diesem Grund sollten Sie dieses Verfahren nur in begrenzten Fällen durchführen.

> 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.

S3- und Swift-API-Operationen zum Hochladen von Objekten (oder Objektteilen) können während des EC-Ausgleichs fehlschlagen, wenn sie mehr als 24 Stunden benötigen. Langfristige PUT-Vorgänge funktionieren nicht, wenn die anwendbare ILM-Regel eine strenge oder ausgewogene Platzierung bei der Aufnahme verwendet. Der folgende Fehler wird gemeldet:

```
500 Internal Server Error
```

**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. Halten Sie den Mauszeiger über das Diagramm „verwendete Daten – Objektdaten“, um die aktuelle Menge der replizierten Daten und mit Erasure Coding versehenen Daten auf dem Storage-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 im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Geben Sie den folgenden Befehl ein:

   ```
   rebalance-data start --site "site-name"
   ```

   Für "*site-name*"`Geben Sie den ersten Standort an, an dem Sie neue Speicherknoten oder Knoten hinzugefügt haben. Umschließen `site-name` In Angeboten.

   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
     ```

     Für `*job-id*`Geben Sie die ID an, die beim Start 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
```

- Um die geschätzte Zeit bis zum Abschluss und den Prozentsatz für den Abschluss des aktuellen Jobs anzuzeigen, wählen Sie **SUPPORT Tools Metrics**. Wählen Sie dann im Abschnitt Grafana die Option **EC Übersicht** aus. Sehen Sie sich die Dashboards **Grid EC Job Estimated Time to Completion** und **Grid EC Job prozentual Completed** an.

6. Führen Sie weitere Schritte aus, basierend auf dem zurückgegebenen Status:
   - Wenn der Status lautet `In progress`, Der EC-Ausgleichsoperation läuft noch. Sie sollten das Verfahren regelmäßig überwachen, bis es abgeschlossen ist.
   - Wenn der Status lautet `Failure`, Führen Sie die Fehlerschritte.
   - Wenn der Status lautet `Success`, Führen Sie die Erfolg.
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 ein EC-Ausgleichverfahren beenden, verbleiben alle bereits verschobenen Datenfragmente am neuen Standort. Daten werden nicht zurück an den ursprünglichen Speicherort verschoben.

9. Wenn der Status des EC-Ausgleichs lautet `Failure`, Folgen Sie folgenden Schritten:
   a. Vergewissern Sie sich, dass alle Speicherknoten am Standort mit dem Raster verbunden sind.
   b. Überprüfen Sie, ob Warnmeldungen vorliegen, die sich auf diese Speicherknoten auswirken könnten, und beheben Sie sie.

      Informationen zu bestimmten Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung.

   c. Starten Sie das EC-Ausgleichverfahren neu:
      `rebalance-data start --job-id job-id`
   d. Wenn der Status des EC-Ausgleichs noch immer ist `Failure`, Wenden Sie sich an den technischen Support.
10. Wenn der Status des EC-Ausgleichs-Verfahrens lautet `Success`, Optional Prüfen von Objekt-Storage Um die aktualisierten Details für die Site anzuzeigen.

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

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