Informationen zu StorageGRID 11.5

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Informationen zu StorageGRID 11.5 1
Was ist neu in StorageGRID 11.5 1
Funktionen entfernt oder veraltet 10
Änderungen an der Grid-Management-API 13
Änderungen an der Mandantenmanagement-API 14

Informationen zu StorageGRID 11.5

Bevor Sie ein Upgrade starten, lesen Sie diesen Abschnitt, um mehr über die neuen Funktionen und Verbesserungen in StorageGRID 11.5 zu erfahren. Sie können ermitteln, ob Funktionen veraltet bzw. entfernt wurden, und erfahren Sie mehr über die Änderungen an StorageGRID APIs.

- "Die Neuheiten in StorageGRID 11.5"
- "Funktionen entfernt oder veraltet"
- "Änderungen an der Grid-Management-API"
- "Änderungen an der Mandantenmanagement-API"

Was ist neu in StorageGRID 11.5

StorageGRID 11.5 führt S3 Object Lock ein, unterstützt die KMIP-Verschlüsselung von Daten, Verbesserungen der Benutzerfreundlichkeit beim ILM, eine neu konzipierte Mandanten-Manager-Benutzeroberfläche, Unterstützung für die Stilllegung eines StorageGRID Standorts und ein Verfahren für Appliance-Node-Klone.

S3 Objektsperre für konforme Daten

Die S3-Objektsperre in StorageGRID 11.5 ist eine Objektschutzlösung, die äquivalent zur S3-Objektsperre in Amazon Simple Storage Service (Amazon S3) ist. Sie können die globale S3-Objektsperre für ein StorageGRID-System aktivieren, damit S3-Mandantenkonten Buckets erstellen können, wobei S3-Objektsperre aktiviert ist. Der Mandant kann dann mithilfe einer S3-Client-Applikation optional Aufbewahrungseinstellungen und Einstellungen für die Aufbewahrung gemäß den gesetzlichen Bestimmungen in diesen Buckets festlegen.

Mit der S3 Object Lock können Mandantenbenutzer Vorschriften einhalten, nach denen bestimmte Objekte für eine bestimmte Zeit oder für eine bestimmte Dauer aufbewahrt werden müssen.

Weitere Informationen .

- "Objektmanagement mit ILM"
- "S3 verwenden"
- "Verwenden Sie ein Mandantenkonto"

VERSCHLÜSSELUNGSMANAGEMENT NACH KM

Im Grid Manager kann ein oder mehrere externe KMS (Key Management Server) konfiguriert werden, um StorageGRID Services und Storage Appliances Verschlüsselungen zu übermitteln. Jeder KMS- oder KMS-Cluster verwendet das KMIP (Key Management Interoperability Protocol), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen. Nachdem die Appliance-Volumes verschlüsselt sind, können Sie erst auf sämtliche Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

> Wenn Sie die Verschlüsselungsschlüsselverwaltung verwenden möchten, müssen Sie die Einstellung **Node Encryption** für die Appliance mit dem Installationsprogramm von StorageGRID Appliance aktivieren, bevor Sie die Appliance zum Grid hinzufügen.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen der Benutzerfreundlichkeit beim Information Lifecycle Management (ILM)

- Sie können jetzt die Gesamtkapazität eines Speicherpools einschließlich des belegten und freien Speicherplatzes anzeigen. Sie können auch sehen, welche Nodes in einem Storage-Pool enthalten sind und welche ILM-Regeln und Erasure Coding-Profile den Storage-Pool verwenden.
- Sie können jetzt ILM-Regeln entwerfen, die für mehr als ein Mandantenkonto gelten.
- Wenn Sie eine ILM-Regel für das Erasure Coding erstellen, werden Sie nun daran erinnert, den erweiterten Filter für Objektgröße (MB) auf größer als 0.2 zu setzen, um sicherzustellen, dass sehr kleine Objekte nicht gelöscht werden.
- Die ILM-Richtlinienschnittstelle stellt nun sicher, dass die Standard-ILM-Regel immer für Objekte verwendet wird, die nicht mit einer anderen Regel übereinstimmen. Ab StorageGRID 11.5 kann die Standardregel keine grundlegenden oder erweiterten Filter verwenden und wird automatisch als letzte Regel in der Richtlinie platziert.

> Wenn Ihre aktuelle ILM-Richtlinie den neuen Anforderungen nicht entspricht, können Sie sie nach einem Upgrade auf StorageGRID 11.5 weiterhin verwenden. Wenn Sie jedoch nach dem Upgrade versuchen, eine nicht konforme Richtlinie zu klonen, werden Sie aufgefordert, eine Standardregel auszuwählen, die keine Filter enthält, und Sie müssen die Standardregel am Ende der Richtlinie platzieren.

- Der Speicherpool Alle Speicherknoten auf Lager ist standardmäßig nicht mehr ausgewählt, wenn Sie eine neue ILM-Regel oder ein neues Erasure Coding-Profil erstellen. Außerdem können Sie jetzt den Speicherpool Alle Speicherknoten entfernen, solange er in keiner Regel verwendet wird.

> Die Verwendung des Speicherpools für alle Speicherknoten wird nicht empfohlen, da dieser Speicherpool alle Standorte enthält. Mehrere Kopien eines Objekts können auf demselben Standort platziert werden, wenn Sie diesen Storage-Pool mit einem StorageGRID System verwenden, das mehr als einen Standort umfasst.

- Sie können nun die Regel „Vorrat 2 Kopien erstellen“ entfernen (die den Speicherpool „Alle Speicherknoten“ verwendet), solange sie nicht in einer aktiven oder vorgeschlagenen Richtlinie verwendet wird.
- In einem Cloud-Storage-Pool gespeicherte Objekte können jetzt sofort gelöscht werden (synchrones Löschen).

Weitere Informationen .

- "Objektmanagement mit ILM"

Verbesserungen am Grid Manager

- Auf der Seite „neu gestaltete Mandantenkonten“ können Sie die Nutzung des Mandantenkontos einfacher anzeigen. Die Zusammenfassungstabelle für Mandanten enthält jetzt Spalten für genutzten Speicherplatz, Kontingentnutzung, Kontingente und Objektanzahl. Ein neuer **Details anzeigen** Button greift auf eine Übersicht der einzelnen Mandanten sowie Details zu den S3 Buckets oder Swift Containern des Kontos zu. Außerdem können Sie jetzt zwei exportieren `.csv` Dateien zur Mandantennutzung: Eine mit Nutzungswerten für alle Mandanten und eine mit Details zu den Buckets oder Containern eines Mandanten.

Im Zusammenhang mit dieser Änderung wurden drei neue Prometheus-Kennzahlen hinzugefügt, um die Nutzung von Mandantenkonten nachzuverfolgen:

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`

- Im neuen Feld **Zugriffsmodus** auf der Seite Admin Groups (**Configuration** > **Access Control**) können Sie festlegen, ob die Verwaltungsberechtigungen für die Gruppe schreibgeschützt (Standard) oder schreibgeschützt sind. Benutzer, die zu einer Gruppe mit Lese-/Schreibzugriff gehören, können Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API ausführen. Benutzer, die zu einer Gruppe mit schreibgeschütztem Zugriffsmodus gehören, können nur die für die Gruppe ausgewählten Einstellungen und Funktionen anzeigen.

  > Wenn Sie ein Upgrade auf StorageGRID 11.5 durchführen, ist die Option „Lese-/Schreibzugriff“ für alle vorhandenen Admin-Gruppen ausgewählt.

- Die Benutzeroberfläche von AutoSupport wurde neu gestaltet. Sie können nun ereignisgesteuerte, vom Benutzer ausgelöste und wöchentliche AutoSupport Meldungen über eine einzige Seite im Grid Manager konfigurieren. Sie können auch ein zusätzliches Ziel für AutoSupport Meldungen konfigurieren.

  > Wenn AutoSupport nicht aktiviert wurde, wird jetzt im Grid ManagerDashboard eine Erinnerungsmeldung angezeigt.

- Wenn Sie das Diagramm **verwendete Speicherelemente - Objektdaten** auf der Seite Knoten anzeigen, sehen Sie jetzt Schätzungen für die Menge der replizierten Objektdaten und die Menge der mit Löschungscode gekennzeichneten Daten im Raster, am Standort oder Storage Node (**Nodes** > ***Grid/site/Storage Node*** > **Storage**).
- Die Menüoptionen im Grid Manager wurden neu organisiert, um Optionen einfacher zu finden. Zum Beispiel wurde ein neues Untermenü **Network Settings** zum Menü **Configuration** hinzugefügt und Optionen in den Menüs **Wartung** und **Support** sind nun alphabetisch aufgelistet.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen am Tenant Manager

- Das Erscheinungsbild und die Organisation der Tenant Manager-Benutzeroberfläche wurden komplett neu gestaltet, um die Benutzerfreundlichkeit zu verbessern.
- Das neue Mandanten-Manager-Dashboard bietet einen allgemeinen Überblick über jedes Konto: Es bietet Bucket-Details und zeigt die Anzahl der Buckets oder Container, Gruppen, Benutzer und Endpunkte der Plattform-Services (falls konfiguriert) an.

Weitere Informationen .

- "Verwenden Sie ein Mandantenkonto"

Client-Zertifikate für Prometheus Kennzahlenexport

Sie können nun Clientzertifikate (**Konfiguration** > **Zugriffskontrolle** > **Clientzertifikate**) hochladen oder generieren, die für einen sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank verwendet werden können. Sie können beispielsweise Clientzertifikate verwenden, wenn Sie StorageGRID

extern mit Grafana überwachen müssen.

Weitere Informationen .

- "StorageGRID verwalten"

Verbesserungen für den Load Balancer

- Beim Umgang mit Routinganfragen an einem Standort führt der Load Balancer-Service nun ein Load-aware-Routing durch: Er berücksichtigt die CPU-Verfügbarkeit der Storage Nodes am selben Standort. In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer Service befindet.

> Die CPU-Bekanntheit wird erst aktiviert, wenn mindestens zwei Drittel der Storage-Nodes an einem Standort auf StorageGRID 11.5 aktualisiert wurden und CPU-Statistiken gemeldet wurden.

- Für zusätzliche Sicherheit können Sie nun für jeden Load Balancer-Endpunkt einen Bindungsmodus festlegen. Mit Endpoint Pinning können Sie die Zugänglichkeit jedes Endpunkts auf bestimmte Hochverfügbarkeitsgruppen oder Node-Schnittstellen beschränken.

Weitere Informationen .

- "StorageGRID verwalten"

Änderungen an Objektmetadaten

- **Neue Metrik für den tatsächlich reservierten Speicherplatz**: Um Ihnen zu helfen, die Auslastung von Objektmetadaten auf jedem Speicherknoten zu verstehen und zu überwachen, wird eine neue Prometheus-Metrik auf der Speichernutzung - Objektmetadaten für einen Speicherknoten (**Knoten** > ***Speicherknoten*** > **Speicher**) angezeigt.

```
storagegrid_storage_utilization_metadata_reserved
```

  Die Metrik **tatsächlich reservierter Speicherplatz** gibt an, wie viel Speicherplatz StorageGRID für Objektmetadaten auf einem bestimmten Speicherknoten reserviert hat.

- **Bei Installationen mit größeren Speicherknoten erhöht sich der Metadatenspeicherplatz**: Bei StorageGRID-Systemen mit Speicherknoten mit mindestens 128 GB RAM wurde die Einstellung systemweiter reservierter reservierter Speicherplatz erhöht:

  - **8 TB für Neuinstallationen**: Wenn Sie ein neues StorageGRID 11.5 System installieren und jeder Speicherknoten im Raster 128 GB oder mehr RAM hat, wird die Einstellung für systemweiten reservierten Speicherplatz auf 8 TB anstatt 3 TB gesetzt.
  - **4 TB für Upgrades**: Wenn Sie auf StorageGRID 11.5 aktualisieren und jeder Speicherknoten an einem Standort 128 GB oder mehr RAM hat, ist die Einstellung für systemweiten reservierten Speicherplatz auf 4 TB anstatt 3 TB gesetzt.

    Die neuen Werte für die Einstellung „Metadatenreservierter Speicherplatz“ erhöhen den zulässigen Metadatenspeicherplatz für diese größeren Storage-Nodes auf bis zu 2.64 TB und stellen sicher, dass für zukünftige Hardware- und Softwareversionen ausreichend Metadatenspeicherplatz reserviert ist.

Wenn Ihre Speicherknoten genügend RAM und genügend Speicherplatz auf dem Datenträger 0 haben, können Sie den Einstellungen für reservierten Metadatenspeicherplatz nach dem Upgrade manuell auf 8 TB erhöhen. Die Reservierung von zusätzlichem Metadaten-Speicherplatz nach dem StorageGRID 11.5 Upgrade vereinfacht zukünftige Hardware- und Software-Upgrades.

"Erhöhen der Einstellung für reservierten Speicherplatz für Metadaten"

+

Wenn Ihr StorageGRID System mehr als 2.64 TB Metadaten auf jedem Storage-Node speichert (oder voraussichtlich gespeichert werden), kann der zulässige Metadatenspeicherplatz in einigen Fällen erhöht werden. Wenn jeweils Ihre Storage-Nodes freien Speicherplatz auf dem Storage-Volume 0 und mehr als 128 GB RAM zur Verfügung haben, wenden Sie sich an Ihren NetApp Ansprechpartner. NetApp überprüft ggf. die Anforderungen und erhöht den zulässigen Metadatenspeicherplatz für jeden Storage-Node.

- **Automatische Bereinigung gelöschter Metadaten**: Wenn 20% oder mehr der auf einem Speicherknoten gespeicherten Metadaten entfernt werden können (weil die entsprechenden Objekte gelöscht wurden), kann StorageGRID nun eine automatische Data-Compaction auf diesem Speicherknoten durchführen. Dieser Hintergrundprozess wird nur ausgeführt, wenn die Belastung des Systems niedrig ist – also wenn CPU, Speicherplatz und Arbeitsspeicher verfügbar sind. Bei dem neuen Data-Compaction-Prozess werden Metadaten für gelöschte Objekte schneller entfernt als in früheren Versionen. Zudem wird Speicherplatz für neue zu speichernde Objekte verfügbar.

Weitere Informationen .

- "StorageGRID verwalten"

Änderungen an der Unterstützung für die S3-REST-API

- Sie können jetzt die S3-REST-API verwenden, um anzugeben S3-Objektsperre Einstellungen:
  - Verwenden Sie zum Erstellen eines Buckets mit aktivierter S3-Objektsperre eine PUT-Bucket-Anforderung beim `x-amz-bucket-object-lock-enabled` Kopfzeile.
  - Um festzustellen, ob die S3-Objektsperre für einen Bucket aktiviert ist, verwenden Sie eine Konfigurationsanforderung FÜR GET Object Lock.
  - Wenn Sie eine Objektversion zu einem Bucket hinzufügen, bei dem die S3-Objektsperre aktiviert ist, verwenden Sie die folgenden Anfrageböpfe, um die Einstellungen für Aufbewahrung und Aufbewahrung der gesetzlichen Aufbewahrungspflichten festzulegen: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`.
- ES können nun mehrere Objekte in einem versionierten Bucket GELÖSCHT werden.
- Sie können nun Bucket-Verschlüsselungsanfragen PER PUT, GET und DELETE verwenden, um die Verschlüsselung für einen vorhandenen S3-Bucket zu managen.
- Es wurde eine kleine Änderung an einem Feldnamen für den vorgenommen `Expiration` Parameter. Dieser Parameter wird in der Antwort auf EINE PUT-Objekt-, HEAD-Objekt- oder GET-Objekt-Anforderung enthalten, wenn eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt angewendet wird. Das Feld, das angibt, welche Ablaufregel übereinstimmen wurde, wurde zuvor benannt `rule_id`. Dieses Feld wurde in umbenannt `rule-id` Das muss auch auf die AWS-Implementierung abgestimmt sein.
- Standardmäßig versucht die Anforderung GET Storage Usage durch starke globale Konsistenz, den von

einem Mandantenkonto verwendeten Storage und seine Buckets abzurufen. Wenn keine „stabile globale“ Konsistenz erreicht werden kann, versucht StorageGRID, die Nutzungsdaten mithilfe der starken Standortkonsistenz abzurufen.

- Der `Content-MD5` Die Anforderungsüberschrift wird jetzt korrekt unterstützt.

Weitere Informationen .

- "S3 verwenden"

Die maximale Größe für CloudMirror-Objekte wurde auf 5 TB erhöht

Die maximale Größe für Objekte, die vom CloudMirror-Replizierungsservice auf einen Ziel-Bucket repliziert werden können, wurde auf 5 TB erhöht. Dies ist die von StorageGRID unterstützte maximale Objektgröße.

Weitere Informationen .

- "S3 verwenden"
- "Verwenden Sie Swift"

Neue Warnmeldungen hinzugefügt

Für StorageGRID 11.5 wurden die folgenden neuen Warnmeldungen hinzugefügt:

- Fehler bei der BMC-Kommunikation des Geräts
- Fibre-Channel-Fehler des Geräts erkannt
- Fehler des Fibre-Channel-HBA-Ports des Geräts
- Geräte-LACP-Port fehlt
- Cassandra Auto-Kompaktor-Fehler
- Cassandra Auto-Kompaktor-Kennzahlen veraltet
- Cassandra-Kompensation überlastet
- Die Festplatten-I/O ist sehr langsam
- ABLAUF DES KMS-CA-Zertifikats
- ABLAUF DES KMS-Clientzertifikats
- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KM ist nicht konfiguriert
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- Ablauf DES KMS-Serverzertifikats
- Wenig freier Speicherplatz für den Speicherpool
- Node-Netzwerkannahme-Frame-Fehler
- Die Speicherkonnektivität der Services-Appliance ist herabgesetzt
- Storage-Konnektivität der Storage-Appliance ist herabgesetzt (zuvor unter dem Namen „Storage-Konnektivität der Appliance“ beeinträchtigt)

- Hohe Kontingentnutzung für Mandanten
- Unerwarteter Node-Neustart

Weitere Informationen .

- "Monitor Fehlerbehebung"

TCP-Unterstützung für SNMP-Traps

Sie können nun als Protokoll für SNMP-Trap-Ziele das Transmission Control Protocol (TCP) auswählen. Zuvor wurde nur das Protokoll (User Datagram Protocol) (UDP) unterstützt.

Weitere Informationen .

- "Monitor Fehlerbehebung"

Installation und Netzwerkverbesserungen

- **MAC-Adressenklonierung**: Sie können jetzt MAC-Adressenklonierung verwenden, um die Sicherheit bestimmter Umgebungen zu erhöhen. Mit dem Klonen VON MAC-Adressen können Sie eine dedizierte virtuelle NIC für das Grid-Netzwerk, das Admin-Netzwerk und das Client-Netzwerk verwenden. Wenn der Docker Container die MAC-Adresse der dedizierten NIC auf dem Host nutzen soll, können Sie keine Kompromissmodus-Netzwerkkonfigurationen verwenden. Die Node-Konfigurationsdatei für Linux-basierte (Bare Metal-)Nodes wurde um drei neue Klon-Schlüssel für MAC-Adressen erweitert.
- **Automatische Ermittlung von DNS- und NTP-Hostrouten**: Zuvor gab es Einschränkungen, mit welchem Netzwerk Ihre NTP- und DNS-Server verbunden werden mussten, wie z.B. die Anforderung, dass Sie nicht alle Ihre NTP- und DNS-Server im Client-Netzwerk haben konnten. Diese Einschränkungen werden nun entfernt.

Weitere Informationen .

- "Installieren Sie Red hat Enterprise Linux oder CentOS"
- "Installieren Sie Ubuntu oder Debian"

Unterstützung für das Ausbalancieren von EC-Daten (Erasure Coding) nach der Storage-Node-Erweiterung

Das EC-Ausgleichverfahren ist ein neues Befehlszeilenskript, das nach dem Hinzufügen neuer Storage-Nodes erforderlich sein kann. Bei der Durchführung des Verfahrens verteilt StorageGRID nach dem Erasure-Coding-Verfahren Fragmente auf die vorhandenen und neu erweiterten Storage-Nodes an einem Standort neu.

> Sie sollten das EC-Ausgleichverfahren nur in begrenzten Fällen durchführen. Wenn Sie beispielsweise nicht die empfohlene Anzahl von Speicherknoten zu einer Erweiterung hinzufügen können, können Sie das EC-Ausgleichverfahren verwenden, um zusätzliche Objekte mit Löschungscode zu speichern.

Weitere Informationen .

- "Erweitern Sie Ihr Raster"

Neue und überarbeitete Wartungsabläufe

- **Deaktivierung der Website**: Sie können nun eine funktionsfähige Website aus Ihrem StorageGRID-System entfernen. Durch die Stilllegung einer verbundenen Website wird ein operativer Standort entfernt und Daten beibehalten. Der neue Decommission Site Wizard führt Sie durch den Prozess (**Wartung** >

Dekommission > **Decommission Site**).

- **Appliance Node Cloning**: Sie können jetzt einen vorhandenen Appliance-Knoten klonen, um den Knoten auf ein neues Appliance-Modell zu aktualisieren. Beispielsweise können Sie einen Appliance Node mit geringerer Kapazität in einer Appliance mit höherer Kapazität klonen. Sie können auch einen Appliance-Knoten klonen, um neue Funktionen zu implementieren, wie z. B. die neue **Node Encryption**-Einstellung, die für die KMS-Verschlüsselung erforderlich ist.
- **Möglichkeit, die Provisioning-Passphrase zu ändern**: Sie können jetzt die Provisioning-Passphrase (**Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter**) ändern. Die Passphrase ist für Recovery-, Erweiterungs- und Wartungsvorgänge erforderlich.
- **Erweitertes SSH-Passwortverhalten**: Um die Sicherheit von StorageGRID-Geräten zu erhöhen, wird das SSH-Passwort nicht mehr geändert, wenn Sie eine Appliance in den Wartungsmodus versetzen. Darüber hinaus werden beim Upgrade eines Node auf StorageGRID 11.5 neue SSH-Host-Zertifikate und Hostschlüssel generiert.

> Wenn Sie SSH zum Anmelden bei einem Node nach dem Upgrade auf StorageGRID 11.5 verwenden, wird die Warnung ausgegeben, dass sich der Host-Schlüssel geändert hat. Dieses Verhalten wird erwartet, und Sie können den neuen Schlüssel sicher genehmigen.

Weitere Informationen .

- "Verwalten Sie erholen"

Änderungen an StorageGRID Appliances

- **Direkter Zugriff auf SANtricity System Manager für Storage Appliances**: Sie können jetzt vom StorageGRID Appliance Installer und über den Grid Manager auf die Benutzeroberfläche des E-Series SANtricity System Managers zugreifen. Mit diesen neuen Methoden kann auf SANtricity System Manager zugegriffen werden, ohne den Management-Port der Appliance zu verwenden. Benutzer, die vom Grid Manager aus auf SANtricity System Manager zugreifen müssen, müssen über die neue Administrator-Berechtigung für Speichergeräte verfügen.
- **Knotenverschlüsselung**: Als Teil der neuen KMS-Verschlüsselungsfunktion wurde dem StorageGRID-Appliance-Installer eine neue **Node-Verschlüsselung**-Einstellung hinzugefügt. Wenn Sie zum Schutz von Appliance-Daten das Verschlüsselungskeymanagement verwenden möchten, müssen Sie diese Einstellung während der Hardware-Konfigurationsphase der Appliance-Installation aktivieren.
- **UDP-Port-Konnektivität**: Sie können jetzt die Netzwerkverbindung eines StorageGRID-Geräts auf UDP-Ports testen, wie sie für einen externen NFS- oder DNS-Server verwendet werden. Wählen Sie im Installationsprogramm der StorageGRID-Appliance die Option **Netzwerke konfigurieren** > **Port Connectivity Test (nmap)** aus.
- **Automatisierte Installation und Konfiguration**: Dem StorageGRID Appliance Installer wurde eine neue Seite zum Hochladen der JSON-Konfiguration hinzugefügt (**Erweitert** > **Appliance-Konfiguration aktualisieren**). Auf dieser Seite können Sie eine Datei verwenden, um mehrere Geräte in großen Grids zu konfigurieren. Darüber hinaus der `configure-sga.py` Python-Skript wurde aktualisiert, um den Fähigkeiten des StorageGRID-Appliance-Installationsprogramms gerecht zu werden.

Weitere Informationen .

- "SG100 SG1000 Services-Appliances"
- "SG6000 Storage-Appliances"
- "SG5700 Storage-Appliances"
- "SG5600 Storage Appliances"

Änderungen an Audit-Meldungen

- **Automatische Bereinigung von überschreibten Objekten**: Zuvor wurden Objekte, die überschrieben wurden, in bestimmten Fällen nicht von der Festplatte entfernt, was zu einem zusätzlichen Platzbedarf führte. Diese überschreibbaren Objekte, die für Benutzer nicht zugänglich sind, werden jetzt automatisch entfernt, um Speicherplatz zu sparen. Weitere Informationen finden Sie in der LKCU-Überwachungsmeldung.
- **Neue Audit-Codes für S3 Object Lock**: Die SPUT-Audit-Nachricht wurde um vier neue Audit-Codes ergänzt S3-Objektsperre Anfragezeilen:
  - LKEN: Objektsperre aktiviert
  - LKLH: Objektsperre Legal Hold
  - LKMD: Objektsperrmodus
  - LKRU: Objektsperre bis Datum beibehalten
- **Neue Felder für letzte geänderte Zeit und Vorherige Objektgröße**: Sie können jetzt verfolgen, wann ein Objekt überschrieben wurde, sowie die ursprüngliche Objektgröße.
  - Das Feld MTME (letzte geänderte Zeit) wurde den folgenden Audit-Meldungen hinzugefügt:
    - SDEL (S3 DELETE)
    - SPUT (S3 PUT)
    - WDEL (Swift LÖSCHEN)
    - WPUT (Swift PUT)
  - Das Feld CSIZ (Vorherige Objektgröße) wurde der OVWR-Meldung (Objekt-Überschreiben) hinzugefügt.

Weitere Informationen .

- "Prüfung von Audit-Protokollen"

Neue nms.requestlog-Datei

Eine neue Protokolldatei, `/var/local/log/nms.requestlog`, Wird auf allen Admin-Knoten gepflegt. Diese Datei enthält Informationen über ausgehende Verbindungen von der Management-API zu internen StorageGRID-Diensten.

Weitere Informationen .

- "Monitor Fehlerbehebung"

Änderungen in der StorageGRID-Dokumentation

- Damit die Netzwerkinformationen und -Anforderungen leichter zu finden sind und klarzustellen ist, dass die Informationen auch für StorageGRID-Appliance-Knoten gelten, wurde die Netzwerkdokumentation von den softwarebasierten Installationshandbüchern (RedHat Enterprise Linux/CentOS, Ubuntu/Debian und VMware) in einen neuen Netzwerkleitfaden verschoben.

  "Netzwerkrichtlinien"

- Um die Suche nach ILM-bezogenen Anweisungen und Beispielen zu erleichtern, wurde die Dokumentation für das Management von Objekten mit Information Lifecycle Management vom *Administrator Guide* in einen neuen ILM-Leitfaden verschoben.

"Objektmanagement mit ILM"

- Ein neuer FabricPool Leitfaden bietet einen Überblick über die Konfiguration von StorageGRID als NetApp FabricPool Cloud Tier und beschreibt die Best Practices für die Konfiguration von ILM-Optionen und anderen StorageGRID-Optionen für einen FabricPool-Workload.

  "Konfigurieren Sie StorageGRID für FabricPool"

- Sie können jetzt auf mehrere Anleitungsvideos vom Grid Manager zugreifen. Die aktuellen Videos enthalten Anweisungen zum Management von Warnmeldungen, benutzerdefinierten Warnmeldungen, ILM-Regeln und ILM-Richtlinien.

Funktionen entfernt oder veraltet

Einige Funktionen wurden in StorageGRID 11.5 entfernt oder veraltet. Sie müssen diese Elemente überprüfen, um zu verstehen, ob Sie Clientanwendungen aktualisieren oder Ihre Konfiguration ändern müssen, bevor Sie ein Upgrade durchführen.

Schwache Konsistenzkontrolle entfernt

Die schwache Konsistenzkontrolle wurde für StorageGRID 11.5 entfernt. Nach dem Upgrade gelten folgende Verhaltensweisen:

- Anfragen zur Festlegung einer schwachen Konsistenz für einen S3-Bucket oder Swift-Container sind erfolgreich. Die Konsistenzstufe steht jedoch tatsächlich zur Verfügung.
- Vorhandene Buckets und Container, die eine schwache Konsistenz verwenden, werden im Hintergrund aktualisiert, um die verfügbare Konsistenz zu nutzen.
- Anforderungen, die einen schwachen Header zur Consistency-Control haben, verwenden tatsächlich verfügbare Konsistenz, falls zutreffend.

Die verfügbare Consistency Control verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet jedoch nur eventuelle Konsistenz für DEN KOPFBETRIEB. Die verfügbare Consistency Control bietet eine höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Speicherknoten nicht verfügbar sind.

Alarm für den Zustand des Rasters ist veraltet

Der `/grid/health/topology` Die API, die auf aktive *Alarme* von Nodes überprüft, ist veraltet. An ihrem Platz ein neues `/grid/node-health` endpunkt wurde hinzugefügt. Diese API gibt den aktuellen Status jedes Knotens zurück, indem sie auf aktive „*Alerts*“ auf Knoten überprüft.

Compliance-Funktion veraltet

Die S3-Objektsperrfunktion in StorageGRID 11.5 ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die neue S3-Objektsperrfunktion den Amazon S3-Anforderungen entspricht, depretiert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „`` Legacy-Compliance“ bezeichnet wird.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die neue globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch aktiviert. Mandantenbenutzer können keine neuen Buckets erstellen, für die Compliance in StorageGRID aktiviert ist. Mandantenbenutzer können jedoch nach Bedarf vorhandene, konforme Buckets weiterhin verwenden und managen.

Im Mandanten-Manager wird ein Shield-Symbol angezeigt  Zeigt einen veralteten, konformen Bucket an. Auch für ältere, konforme Buckets ist ein Hold-Abzeichen vorhanden  Um anzugeben, dass der Bucket unter einer gesetzlichen Aufbewahrungspflichten steht.

"KB: Wie verwaltet man ältere, konforme Buckets in StorageGRID 11.5"

"Objektmanagement mit ILM"

Warnung „`s 3 mehrtei. zu klein`“ entfernt

Die Warnung **S3 mehrtei. zu klein** wurde entfernt. Zuvor wurde diese Warnmeldung ausgelöst, wenn ein S3-Client einen mehrteiligen Upload mit Teilen durchführen wollte, die die Größenlimits für Amazon S3 nicht erfüllen. Nach dem Upgrade auf StorageGRID 11.5 werden alle Anforderungen für mehrteilige Uploads, die die folgenden Größenlimits nicht erfüllen, fehlschlagen:

- Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5,242,880 Byte) und 5 gib (5,368,709,120 Byte) liegen.
- Der letzte Teil kann kleiner als 5 MiB (5,242,880 Byte) sein.
- Im Allgemeinen sollten die Teilemaße so groß wie möglich sein. Verwenden Sie z. B. für ein Objekt mit 100 gib die Teilenummer 5 gib. Da jedes Teil als einzigartiges Objekt betrachtet wird, verringert der StorageGRID-Metadaten-Overhead durch große Teilgrößen.
- Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.

Warnmeldungen „Appliance-Verbindung im Grid-Netzwerk deaktiviert“ entfernt

Die folgenden Meldungen wurden entfernt. Wenn das Grid-Netzwerk ausgefallen ist, sind die Metriken, die diese Warnmeldungen auslösen würden, nicht verfügbar:

- Services-Appliance-Verbindung im Grid-Netzwerk deaktiviert
- Verbindung der Storage Appliance im Grid-Netzwerk deaktiviert

Unterstützung für vollständig qualifizierte Domain Name aus SNMP-Konfiguration entfernt

Wenn Sie einen SNMP-Server im Baseboard Management Controller (BMC) für SG6000, SG100 oder SG1000 konfigurieren, müssen Sie jetzt eine IP-Adresse anstelle eines vollständig qualifizierten Domänennamens angeben. Wenn zuvor ein vollständig qualifizierter Domänenname konfiguriert war, ändern Sie ihn in eine IP-Adresse, bevor Sie ein Upgrade auf StorageGRID 11.5 durchführen.

Alte Attribute entfernt

Die folgenden älteren Attribute wurden entfernt. Bei Bedarf werden die äquivalenten Informationen zu den Prometheus Kennzahlen bereitgestellt:

Altes Attribut	Äquivalenter Prometheus-Wert
BREC	storagegrid_Service_Network_received_Byte
BTRA	storagegrid_Service_Network_transmited_Byte

Altes Attribut	Äquivalenter Prometheus-Wert
CQST	storagegrid_Metadatenabfragen_average_Latency_Millisekunden
HAIS	storagegrid_http_Sessions_Incoming_versuchte
HCCS	storagegrid_http_Sessions_Incoming_derzeit_etabliertes
HEIS	storagegrid_http_Sessions_INCOMING_FAILED
HISC	storagegrid_http_Sessions_Incoming_successful
LHAC	*None*
NREC	*None*
NTSO (ausgewähltes Zeitquelloffset)	storagegrid_ntp_Chooed_time_source_Offset_Millisekunden
NTRA	*None*
SLOD	storagegrid_Service_Load
SMEM	storagegrid_Service_Memory_Usage_Byte
SUTM	storagegrid_Service_cpu_Sekunden
SVUT	storagegrid_Service_Uptime_Sekunden
TRBS (empfangene Bits pro Sekunde)	*None*
TRXB	storagegrid_Network_received_Byte
TTBS (Bits insgesamt pro Sekunde übertragen)	*None*
TTXB	storagegrid_Network_transmited_Byte

Es wurden auch folgende Änderungen vorgenommen:

- Der `network_received_bytes` Und `network_transmitted_bytes` Die Kennzahlen von Prometheus wurden von den Messwerten zu Zählern geändert, da die Werte dieser Kennzahlen nur noch zunehmen. Wenn Sie diese Metriken derzeit in Prometheus-Abfragen verwenden, sollten Sie mit dem beginnen `increase()` Funktion in der Abfrage.
- Die Tabelle „Netzwerkressourcen“ wurde aus der Registerkarte „Ressourcen“ für StorageGRID-Services entfernt. (Wählen Sie **Support** > **Tools** > **Grid Topology** und dann ***Node*** > ***Service*** > **Ressourcen**.)

- Die Seite HTTP-Sitzungen wurde für Speicherknoten entfernt. Bisher konnten Sie auf diese Seite zugreifen, indem Sie **Support** > **Tools** > **Grid Topology** und dann ***Storage Node*** > **LDR** > **HTTP** wählen.
- Der HCCS-Alarm (Currently Creved Incoming Sessions) wurde entfernt.
- Der NTSO-Alarm (ausgewählter Zeitquelle Offset) wurde entfernt.

Änderungen an der Grid-Management-API

StorageGRID 11.5 verwendet Version 3 der Grid Management API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.

> Sie können weiterhin Version 1 und Version 2 der Management-API mit StorageGRID 11.5 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.5 können die veralteten v1- und v2-APIs mit dem deaktiviert werden `PUT /grid/config/management` API:

Abschnitt „Neue Clientzertifikate“

Der neue Abschnitt, `/grid/client-certificates`, Ermöglicht es Ihnen, Client-Zertifikate zu konfigurieren, um sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank bereitzustellen. Sie können StorageGRID beispielsweise extern mit Grafana überwachen.

Ältere Compliance-Endpunkte werden in den Abschnitt mit der neuen s3-Objektsperre verschoben

Mit der Einführung der StorageGRID S3-Objektsperre wurden die APIs, mit denen die bisherigen Compliance-Einstellungen für das Grid verwaltet werden, in einen neuen Abschnitt der Swagger-Benutzeroberfläche verschoben. Der Abschnitt **s3-Object-Lock** enthält die beiden `/grid/compliance-global` API-Endpunkte, die jetzt die globale S3-Objektsperre steuern. Die Endpunkt-URIs bleiben unverändert, um die Kompatibilität mit vorhandenen Anwendungen zu gewährleisten.

Swift-admin-Passwort-Konten Endpunkt entfernt

Der folgende API-Endpunkt für Konten, der in StorageGRID 10.4 veraltet war, wurde jetzt entfernt:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

Abschnitt „Neue Grid-Passwörter“

Der Abschnitt * Grid-passwords* ermöglicht die Verwaltung von Grid-Kennwörtern. Der Abschnitt enthält zwei Abschnitte `/grid/change-provisioning-passphrase` API-Endpunkte: Mit den Endpunkten können Benutzer die Passphrase für die StorageGRID-Bereitstellung ändern und den Status der Änderung der Passphrase abrufen.

SpeicherAdmin-Berechtigung zur Gruppen-API hinzugefügt

Der `/grid/groups` API enthält jetzt die Berechtigung „Storage Admin“.

Neuer Parameter für die Storage-Verwendung-API

Der `GET /grid/accounts/{id}/usage` API hat jetzt eine `strictConsistency` Parameter. Um beim Abrufen von Speichernutzungsdaten über Speicherknoten eine stabile globale Konsistenz durchzusetzen, setzen Sie diesen Parameter auf `true`. Wenn dieser Parameter auf festgelegt ist `false` (Standard), StorageGRID versucht, Nutzungsdaten mit einer starken globalen Konsistenz abzurufen, kehrt aber zurück zu starker Standortkonsistenz, wenn starke globale Konsistenz nicht erreicht werden kann.

Neue Node Health API

Eine neue `/grid/node-health` endpunkt wurde hinzugefügt. Diese API gibt den aktuellen Status jedes Node zurück, indem sie auf den Nodes auf aktive „*Alerts*“ überprüft. Der `/grid/health/topology` Die API, die auf aktive *Alarme* von Nodes überprüft, ist veraltet.

Ändern Sie in „ApplianceWatch StorageShelvesPowerSupplyDegraded“ Warnregel-ID

Die Warnregel-ID „ApplianceWatch StorageShelvesPowerSupplyDegraded“ wurde in „ApplianceWatch StorageShelvesDegraded“ umbenannt, um das tatsächliche Verhalten der Warnmeldung besser widerzuspiegeln.

Verwandte Informationen

"StorageGRID verwalten"

Änderungen an der Mandantenmanagement-API

StorageGRID 11.5 verwendet Version 3 der Mandantenmanagement-API. Version 3 depretiert Version 2; jedoch werden Version 1 und Version 2 weiterhin unterstützt.

> Sie können weiterhin Version 1 und Version 2 der Management-API mit StorageGRID 11.5 verwenden. Die Unterstützung für diese Versionen der API wird jedoch in einem zukünftigen Release von StorageGRID entfernt. Nach dem Upgrade auf StorageGRID 11.5 können die veralteten v1- und v2-APIs mit dem deaktiviert werden `PUT /grid/config/management` API:

Neuer Parameter für die Mandanten-Storage-Nutzung-API

Der `GET /org/usage` API hat jetzt eine `strictConsistency` Parameter. Um beim Abrufen von Speichernutzungsdaten über Speicherknoten eine stabile globale Konsistenz durchzusetzen, setzen Sie diesen Parameter auf `true`. Wenn dieser Parameter auf festgelegt ist `false` (Standard), StorageGRID versucht, Nutzungsdaten mit einer starken globalen Konsistenz abzurufen, kehrt aber zurück zu starker Standortkonsistenz, wenn starke globale Konsistenz nicht erreicht werden kann.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie ein Mandantenkonto"