TR-4626: Load Balancer

How to enable StorageGRID in your environment

NetApp
October 09, 2024

Inhalt

TR-4626: Load Balancer . . . 1
Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID . . . 1
Erfahren Sie, wie Sie SSL-Zertifikate für HTTPS in StorageGRID implementieren . . . 3
Konfigurieren Sie den Load Balancer eines vertrauenswürdigen Drittanbieters in StorageGRID . . . 4
Informieren Sie sich über Load Balancer für lokale Traffic Manager . . . 4
Lernen Sie einige Anwendungsfälle für StorageGRID Konfigurationen kennen . . . 8
SSL-Verbindung in StorageGRID validieren . . . 11
Informationen zu den globalen Lastausgleichsanforderungen für StorageGRID . . . 11

TR-4626: Load Balancer

Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID

Erfahren Sie mehr über die Rolle eines Drittanbieters und globaler Load Balancer in einem Objektspeicher-System wie StorageGRID.

Allgemeine Hinweise für die Implementierung von NetApp® StorageGRID® mit Load Balancern von Drittanbietern.

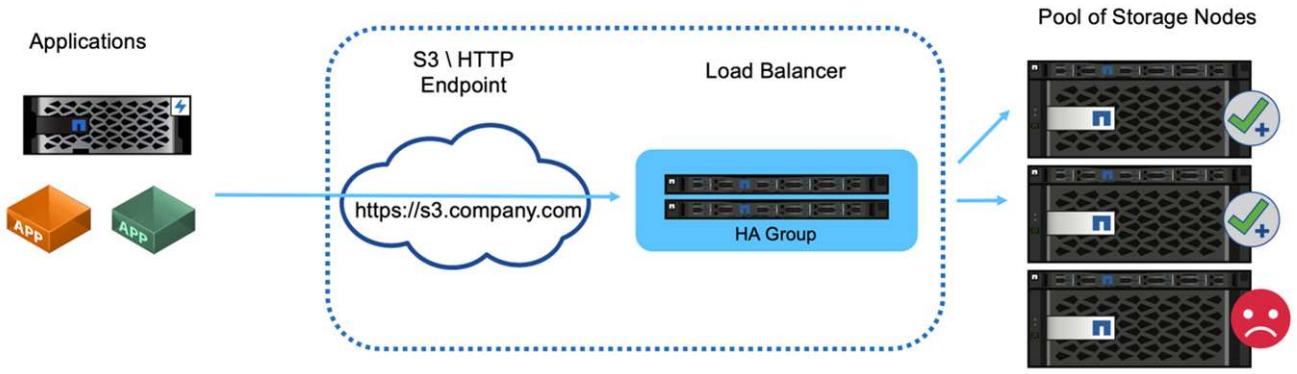
Objekt-Storage ist gleichbedeutend mit dem Begriff Cloud-Storage. Wie Sie erwarten würden, adressieren Applikationen, die Cloud-Storage nutzen, diesen Storage über eine URL. Unter dieser einfachen URL StorageGRID lässt sich die Kapazität, Performance und Langlebigkeit auf einen einzelnen Standort oder über geografisch verteilte Standorte skalieren. Die Komponente, die diese Einfachheit ermöglicht, ist ein Load Balancer.

Dieses Dokument dient dazu, StorageGRID Kunden über Load Balancer-Optionen zu informieren und allgemeine Hinweise zur Konfiguration von Load Balancern anderer Anbieter zu geben.

Grundlagen der Lastverteilung

Load Balancer sind eine wesentliche Komponente von Objekt-Storage-Systemen der Enterprise-Klasse wie StorageGRID. StorageGRID besteht aus mehreren Storage-Nodes, von denen jeder den gesamten S3-Namensraum (Simple Storage Service) für eine bestimmte StorageGRID Instanz darstellen kann. Load Balancer erzeugen einen hochverfügbaren Endpunkt, hinter dem StorageGRID Nodes platziert werden können. StorageGRID ist einzigartig unter S3-kompatiblen Objektspeichersystemen, da es einen eigenen Load Balancer anbietet, aber auch Load Balancer von Drittanbietern oder Mehrzweck-Systemen wie F5, Citrix NetScaler, HA Proxy, NGINX usw. unterstützt.

In der folgenden Abbildung wird der Beispiel-URL/ Fully Qualified Domain Name (FQDN) „s3.company.com" verwendet. Der Load Balancer erstellt eine virtuelle IP (VIP), die über DNS in den FQDN aufgelöst wird und leitet dann alle Anforderungen von Anwendungen an einen Pool von StorageGRID-Knoten weiter. Der Load Balancer führt eine Integritätsprüfung für jeden Node durch und stellt nur Verbindungen zu funktionstüchtigen Nodes her.



Die Abbildung zeigt den von StorageGRID bereitgestellten Load Balancer, das Konzept ist jedoch dasselbe bei Load Balancern von Drittanbietern. Anwendungen richten eine HTTP-Sitzung mithilfe der VIP auf dem Load Balancer ein und der Datenverkehr wird über den Load Balancer zu den Speicher-Nodes geleitet. Standardmäßig wird der gesamte Datenverkehr von der Anwendung zum Load Balancer und vom Load

Balancer zum Speicher-Node über HTTPS verschlüsselt. HTTP ist eine unterstützte Option.

Lokale und globale Load Balancer

Es gibt zwei Arten von Load Balancern:

- * Local Traffic Manager (LTM)*. Verteilt Verbindungen über einen Node-Pool an einem einzelnen Standort.
- **Global Service Load Balancer (GSLB)**. Verteilt Verbindungen über mehrere Standorte und sorgt so für einen effektiven Lastenausgleich bei LTM-Load-Balancern. Stellen Sie sich ein GSLB als intelligenten DNS-Server vor. Wenn ein Client eine StorageGRID-Endpunkt-URL anfordert, löst die GSLB sie auf Grundlage der Verfügbarkeit oder anderer Faktoren in die VIP eines LTM auf (z. B. welche Website kann eine niedrigere Latenz für die Anwendung bereitstellen). Es ist zwar immer ein LTM erforderlich, abhängig von der Anzahl der StorageGRID-Standorte und Ihren Applikationsanforderungen ist jedoch ein GSLB optional.

Load Balancer für StorageGRID-Gateway-Nodes im Vergleich zum Load Balancer eines Drittanbieters

StorageGRID ist einzigartig unter S3-kompatiblen Objekt-Storage-Anbietern und bietet einen nativen Load Balancer als speziell entwickelte Appliance, VM oder Container. Der von StorageGRID bereitgestellte Load Balancer wird auch als Gateway-Node bezeichnet.

Für Kunden, die noch keinen Load Balancer wie F5, Citrix usw. besitzen, kann die Implementierung eines Load Balancers eines Drittanbieters sehr komplex sein. Der StorageGRID Load Balancer vereinfacht den Load Balancer erheblich.

Der Gateway Node ist ein hochverfügbarer und hochperformanter Load Balancer der Enterprise-Klasse. Kunden können den Gateway Node, den Load Balancer eines Drittanbieters oder sogar beide in einem Grid implementieren. Der Gateway Node ist ein lokaler Traffic-Manager und kein GSLB.

Der StorageGRID Load Balancer bietet folgende Vorteile:

- **Einfachheit**. Automatische Konfiguration von Ressourcen-Pools, Zustandsprüfungen, Patching und Wartung, alle gemanagt durch StorageGRID.
- **Leistung**. Der StorageGRID Load Balancer ist speziell für StorageGRID vorgesehen. Das heißt, Sie konkurrieren nicht mit anderen Anwendungen um Bandbreite.
- **Kosten**. Die Versionen für Virtual Machines (VM) und Container werden ohne zusätzliche Kosten bereitgestellt.
- **Verkehrsklassifizierungen**. Die Funktion zur erweiterten Traffic-Klassifizierung ermöglicht für StorageGRID spezifische QoS-Regeln sowie Workload-Analysen.
- **Zukünftige StorageGRID-spezifische Funktionen**. StorageGRID wird den Load Balancer in künftigen Versionen weiter optimieren und um innovative Funktionen erweitern.

Weitere Informationen zum Bereitstellen des StorageGRID-Gateway-Knotens finden Sie unter "StorageGRID-Dokumentation".

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID Dokumentationszentrum https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID Enablement https://docs.netapp.com/us-en/storagegrid-enable/

- Überlegungen zum Design der StorageGRID f5 Load Balancer https://www.netapp.com/blog/storagegrid-f5-load-balancer-design-considerations/
- Loadbalancer.org—Load NetApp StorageGRID ausgleichen https://www.loadbalancer.org/applications/load-balancing-netapp-storagegrid/
- Kemp – Load Balancing NetApp StorageGRID https://support.kemptechnologies.com/hc/en-us/articles/360045186451-NetApp-StorageGRID

Erfahren Sie, wie Sie SSL-Zertifikate für HTTPS in StorageGRID implementieren

Verstehen Sie die Wichtigkeit und die Schritte zur Implementierung von SSL-Zertifikaten in StorageGRID.

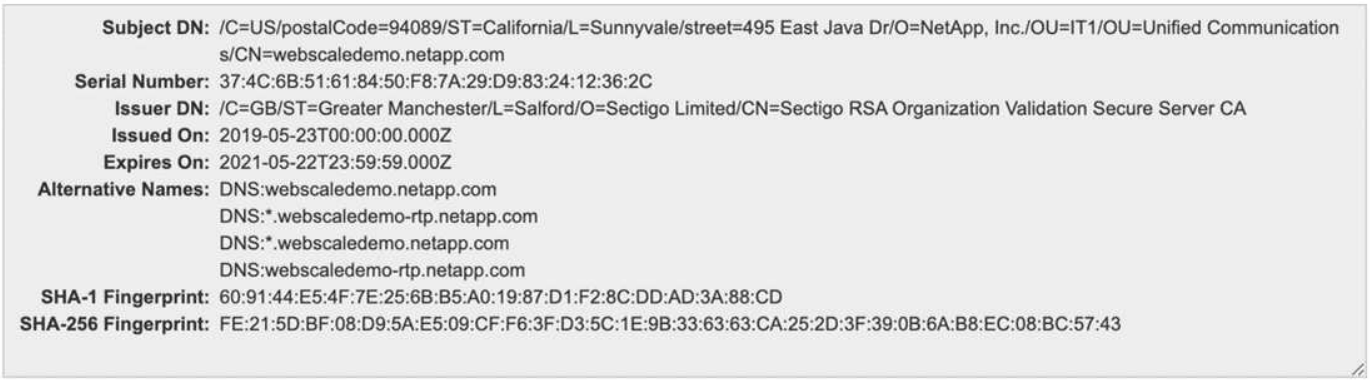
Wenn Sie HTTPS verwenden, müssen Sie über ein SSL-Zertifikat (Secure Sockets Layer) verfügen. Das SSL-Protokoll identifiziert die Clients und Endpunkte und validiert sie als vertrauenswürdig. SSL bietet auch die Verschlüsselung des Datenverkehrs. Das SSL-Zertifikat muss von den Clients vertrauenswürdig sein. Dazu kann das SSL-Zertifikat von einer global vertrauenswürdigen Zertifizierungsstelle (CA) wie DigiCert, einer privaten Zertifizierungsstelle, die in Ihrer Infrastruktur ausgeführt wird, oder einem vom Host generierten selbstsignierten Zertifikat stammen.

Die Verwendung eines global vertrauenswürdigen Zertifizierungsstellenzertifikats ist die bevorzugte Methode, da keine zusätzlichen clientseitigen Aktionen erforderlich sind. Das Zertifikat wird in den Load Balancer oder StorageGRID geladen, und die Clients vertrauen dem Endpunkt und stellen eine Verbindung her.

Für die Verwendung einer privaten Zertifizierungsstelle muss der Stammverzeichnis und alle untergeordneten Zertifikate zum Client hinzugefügt werden. Der Prozess zum Vertrauen auf ein privates CA-Zertifikat kann je nach Client-Betriebssystem und -Anwendungen variieren. Beispielsweise müssen Sie in ONTAP für FabricPool jedes Zertifikat in der Kette einzeln (Stammzertifikat, untergeordnetes Zertifikat, Endpunktzertifikat) auf das ONTAP-Cluster hochladen.

Bei Verwendung eines selbstsignierten Zertifikats muss der Client dem bereitgestellten Zertifikat vertrauen, ohne dass eine Zertifizierungsstelle die Authentizität überprüft. Einige Anwendungen akzeptieren möglicherweise keine selbstsignierten Zertifikate und können die Überprüfung nicht ignorieren.

Die Platzierung des SSL-Zertifikats im StorageGRID-Pfad des Client Load Balancer hängt davon ab, wo Sie die SSL-Terminierung benötigen. Sie können einen Load Balancer als Abschlussendpunkt für den Client konfigurieren und dann erneut verschlüsseln oder mit einem neuen SSL-Zertifikat für den Load Balancer zur StorageGRID-Verbindung verschlüsseln. Sie können auch den Datenverkehr passieren und StorageGRID als Endpunkt für die SSL-Terminierung verwenden. Wenn der Load Balancer der SSL-Abschlussendpunkt ist, wird das Zertifikat auf dem Load Balancer installiert und enthält den Betreffnamen für den DNS-Namen/die DNS-URL sowie alle alternativen URL-/DNS-Namen, für die ein Client für die Verbindung mit dem StorageGRID-Ziel über den Load Balancer konfiguriert ist. einschließlich aller Platzhalternamen. Wenn der Load Balancer für Passthrough konfiguriert ist, muss das SSL-Zertifikat in StorageGRID installiert werden. Auch hier muss das Zertifikat den Subject-Namen für den DNS-Namen/die URL sowie alle alternativen URL-/DNS-Namen enthalten, für die ein Client konfiguriert ist, um über den Load Balancer eine Verbindung zum StorageGRID-Ziel herzustellen, einschließlich aller Platzhalternamen. Einzelne Storage-Node-Namen müssen nicht im Zertifikat enthalten sein, sondern nur die Endpunkt-URLs.



Konfigurieren Sie den Load Balancer eines vertrauenswürdigen Drittanbieters in StorageGRID

Erfahren Sie, wie Sie einen vertrauenswürdigen Drittanbieter-Load Balancer in StorageGRID konfigurieren.

Wenn Sie einen oder mehrere externe Layer-7-Load-Balancer und IP-basierte S3-Bucket oder Gruppenrichtlinien verwenden, muss StorageGRID die IP-Adresse des tatsächlichen Absenders ermitteln. Dies geschieht durch einen Blick auf den X-Forwarded-for (XFF) Header, der vom Load Balancer in die Anfrage eingefügt wird. Da der XFF-Header einfach in Anfragen gespoooofing werden kann, die direkt an die Speicherknoten gesendet werden, muss StorageGRID bestätigen, dass jede Anforderung von einem vertrauenswürdigen Layer 7-Load-Balancer weitergeleitet wird. Wenn StorageGRID der Quelle der Anforderung nicht vertrauen kann, ignoriert er den XFF-Header. Es gibt eine Grid-Management-API, über die eine Liste vertrauenswürdiger externer Load Balancer der Ebene 7 konfiguriert werden kann. Diese neue API ist privat und kann sich bei zukünftigen StorageGRID Versionen ändern. Die aktuellsten Informationen finden Sie im KB-Artikel, "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern".

Informieren Sie sich über Load Balancer für lokale Traffic Manager

Informieren Sie sich über die Richtlinien für den Lastenausgleich von lokalen Traffic-Managern und ermitteln Sie die optimale Konfiguration.

Die folgenden Informationen werden als allgemeine Anleitung für die Konfiguration von Load Balancern von Drittanbietern dargestellt. Ermitteln Sie zusammen mit dem Load Balancer-Administrator die optimale Konfiguration für Ihre Umgebung.

Erstellen Sie eine Ressourcengruppe von Storage-Nodes

Gruppieren Sie StorageGRID-Speicherknoten in einen Ressourcen-Pool oder eine Dienstgruppe (die Terminologie kann sich von bestimmten Load Balancern unterscheiden). StorageGRID-Storage-Nodes stellen die S3-API auf den folgenden Ports zur Verfügung:

- S3 HTTPS: 18082
- S3 HTTP: 18084

Die meisten Kunden entscheiden sich dafür, die APIs auf dem virtuellen Server über die standardmäßigen

HTTPS- und HTTP-Ports (443 und 80) bereitzustellen.

> Für jeden StorageGRID-Standort sind standardmäßig drei Storage-Nodes erforderlich, von denen zwei ordnungsgemäß sein müssen.

Zustandsprüfung

Load Balancer von Drittanbietern erfordern eine Methode, um den Zustand der einzelnen Nodes und ihre Eignung für den Empfang von Traffic zu bestimmen. NetApp empfiehlt zur Durchführung der Integritätsprüfung die HTTP- `OPTIONS` Methode. Der Load Balancer sendet HTTP- `OPTIONS` Anforderungen an jeden einzelnen Speicher-Node und erwartet eine `200` Statusantwort.

Wenn ein Speicher-Node keine Antwort bereitstellt, kann dieser Node keine `200` Speicheranforderungen bearbeiten. Ihre Anwendungs- und Geschäftsanforderungen sollten das Zeitlimit für diese Prüfungen und die Maßnahmen bestimmen, die Ihr Load Balancer ergreift.

Wenn beispielsweise drei von vier Storage-Nodes in Datacenter 1 ausgefallen sind, können Sie den gesamten Datenverkehr an Datacenter 2 leiten.

Das empfohlene Abfrageintervall beträgt einmal pro Sekunde und markiert den Knoten nach drei fehlgeschlagenen Überprüfungen offline.

Beispiel für S3-Integritätsprüfung

Im folgenden Beispiel senden wir `OPTIONS` und überprüfen nach `200 OK`. Wir verwenden `OPTIONS` , da Amazon S3) nicht autorisierte Anfragen unterstützt.

```
curl -X OPTIONS https://10.63.174.75:18082 --verbose --insecure
* Rebuilt URL to: https://10.63.174.75:18082/
*   Trying 10.63.174.75...
* TCP_NODELAY set
* Connected to 10.63.174.75 (10.63.174.75) port 18082 (#0)
* TLS 1.2 connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate: webscale.stl.netapp.com
* Server certificate: NetApp Corp Issuing CA 1
* Server certificate: NetApp Corp Root CA
> OPTIONS / HTTP/1.1
> Host: 10.63.174.75:18082
> User-Agent: curl/7.51.0
> Accept: /
>
< HTTP/1.1 200 OK
< Date: Mon, 22 May 2017 15:17:30 GMT
< Connection: KEEP-ALIVE
< Server: StorageGRID/10.4.0
< x-amz-request-id: 3023514741
```

Zustandsprüfungen für Dateien oder Inhalte

Im Allgemeinen werden von NetApp keine dateibasierten Zustandsprüfungen empfohlen. In der Regel wird eine kleine Datei —`healthcheck.htm`z. B. in einem Bucket mit einer schreibgeschützten Richtlinie erstellt. Diese Datei wird dann vom Load Balancer abgerufen und ausgewertet. Dieser Ansatz hat mehrere Nachteile:

- **Abhängig von einem einzigen Konto.** Wenn das Konto, dem die Datei gehört, deaktiviert ist, schlägt die Integritätsprüfung fehl und es werden keine Speicheranforderungen verarbeitet.
- **Datenschutzregeln.** Das standardmäßige Datensicherungsschema hat einen Ansatz mit zwei Kopien. Wenn in diesem Szenario die beiden Speicherknoten, auf denen die Zustandspeckdatei gehostet wird, nicht verfügbar sind, schlägt die Integritätsprüfung fehl, und Speicheranforderungen werden nicht an funktionstüchtige Speicherknoten gesendet, wodurch das Grid offline geschaltet wird.
- **Audit Log Bloat.** Der Load Balancer ruft die Datei alle X Minuten von jedem Storage-Node ab und erstellt so viele Audit-Log-Einträge.
- **Ressourcenintensiv.** Das Abrufen der Zustandspeckdatei von jedem Node alle paar Sekunden verbraucht Grid- und Netzwerkressourcen.

Wenn eine inhaltsbasierte Zustandsprüfung erforderlich ist, verwenden Sie einen dedizierten Mandanten mit einem dedizierten S3-Bucket.

Persistenz der Sitzung

Sitzungspersistence oder Stickiness bezieht sich auf den Zeitpunkt, zu dem eine bestimmte HTTP-Sitzung bestehen darf. Standardmäßig werden Sitzungen von Storage-Nodes nach 10 Minuten getrennt. Längere Persistenz kann zu besserer Performance führen, da die Applikationen nicht für jede Aktion neu Sitzungen erstellen müssen. Offen zu halten, verbraucht jedoch Ressourcen. Wenn Sie feststellen, dass Ihr Workload von Vorteil ist, können Sie die Persistenz der Sitzung bei einem Load Balancer eines Drittanbieters verringern.

Virtuelle Hosted-Style-Adressierung

Virtual Hosted-Style ist jetzt die Standardmethode für AWS S3. Während StorageGRID und viele Applikationen weiterhin Pfadstil unterstützen, empfiehlt es sich, Unterstützung im Virtual Hosted-Stil zu implementieren. Virtuelle Anforderungen im gehosteten Stil enthalten den Bucket als Teil des Host-Namens.

Gehen Sie wie folgt vor, um Virtual Hosted-Style zu unterstützen:

- Unterstützung von Wildcard-DNS-Suchvorgängen: *.s3.company.com
- Verwenden Sie ein SSL-Zertifikat mit Subject alt-Namen, um Wildcard zu unterstützen: *.s3.company.com einige Kunden haben Sicherheitsbedenken bezüglich der Verwendung von Wildcard-Zertifikaten geäußert. StorageGRID unterstützt wie wichtige Applikationen wie FabricPool weiterhin den Zugriff auf Pfadstil. Allerdings schlagen bestimmte S3-API-Aufrufe fehl oder verhalten sich ohne virtuelle gehostete Unterstützung nicht ordnungsgemäß.

SSL-Terminierung

Die SSL-Terminierung bei Load Balancern von Drittanbietern bietet Sicherheitsvorteile. Wenn der Load Balancer beschädigt ist, wird das Grid unterteilt.

Es gibt drei unterstützte Konfigurationen:

- **SSL-Passthrough.** Das SSL-Zertifikat wird auf StorageGRID als benutzerdefiniertes Serverzertifikat installiert.

- **SSL-Terminierung und Re-Verschlüsselung (empfohlen).** Dies könnte von Vorteil sein, wenn Sie bereits die SSL-Zertifikatsverwaltung auf dem Load Balancer ausführen, anstatt das SSL-Zertifikat auf StorageGRID zu installieren. Diese Konfiguration bietet den zusätzlichen Sicherheitsvorteil, wenn die Angriffsfläche auf den Load Balancer begrenzt wird.
- **SSL-Terminierung mit HTTP.** In dieser Konfiguration wird SSL auf dem Load Balancer des Drittanbieters beendet und die Kommunikation vom Load Balancer zu StorageGRID ist unverschlüsselt, um die Vorteile von SSL-Off-Load zu nutzen (bei SSL-Bibliotheken, die in moderne Prozessoren integriert sind, ist dies nur ein begrenzter Vorteil).

Konfiguration durchlaufen

Wenn Sie den Load Balancer für Passthrough konfigurieren möchten, müssen Sie das Zertifikat auf StorageGRID installieren. Gehen Sie zum Menü:Konfiguration[Serverzertifikate > Object Storage API Service Endpoints Server Certificate].

IP-Sichtbarkeit des Quell-Clients

Mit StorageGRID 11.4 wurde das Konzept eines vertrauenswürdigen Load Balancers eines Drittanbieters eingeführt. Um die Client-Anwendungs-IP an StorageGRID weiterzuleiten, müssen Sie diese Funktion konfigurieren. Weitere Informationen finden Sie unter "So konfigurieren Sie StorageGRID für die Verwendung mit Layer-7-Load-Balancern von Drittanbietern."

So aktivieren Sie den XFF-Header, um die IP-Adresse der Client-Anwendung anzuzeigen:

Schritte

1. Notieren Sie die Client-IP im Überwachungsprotokoll.
2. Verwendung von `aws:SourceIp` S3-Bucket oder Gruppenrichtlinien

Strategien für die Lastverteilung

Die meisten Lastausgleichslösungen bieten mehrere Strategien für den Lastausgleich. Es folgen gängige Strategien:

- * Rundrobin.* Universelle Passform, jedoch mit wenigen Knoten und großen Transfers, die einzelne Knoten verstopfen
- **Geringste Verbindung.** Eignet sich für kleine und gemischte Objekt-Workloads, sodass die Verbindungen auf alle Nodes gleichmäßig verteilt werden.

Die Auswahl des Algorithmus wird mit einer wachsenden Anzahl von Storage-Nodes weniger wichtig.

Datenpfad

Alle Daten fließen über den Lastenausgleich des lokalen Traffic Managers. StorageGRID unterstützt kein direktes Server-Routing (DSR).

Überprüfen der Verteilung der Verbindungen

Um zu überprüfen, ob Ihre Methode die Last gleichmäßig auf die Storage-Nodes verteilt, überprüfen Sie die festgelegten Sitzungen auf jedem Node an einem bestimmten Standort:

- **UI-Methode.** Gehen Sie zum Menü:Support[Kennzahlen > S3-Übersicht > LDR HTTP-Sitzungen]
- **Metrics API.** Verwenden `storagegrid_http_sessions_incoming_currently_established`

Lernen Sie einige Anwendungsfälle für StorageGRID Konfigurationen kennen

Sehen Sie sich einige Anwendungsfälle für StorageGRID-Konfigurationen an, die von Kunden und NetApp IT implementiert wurden.

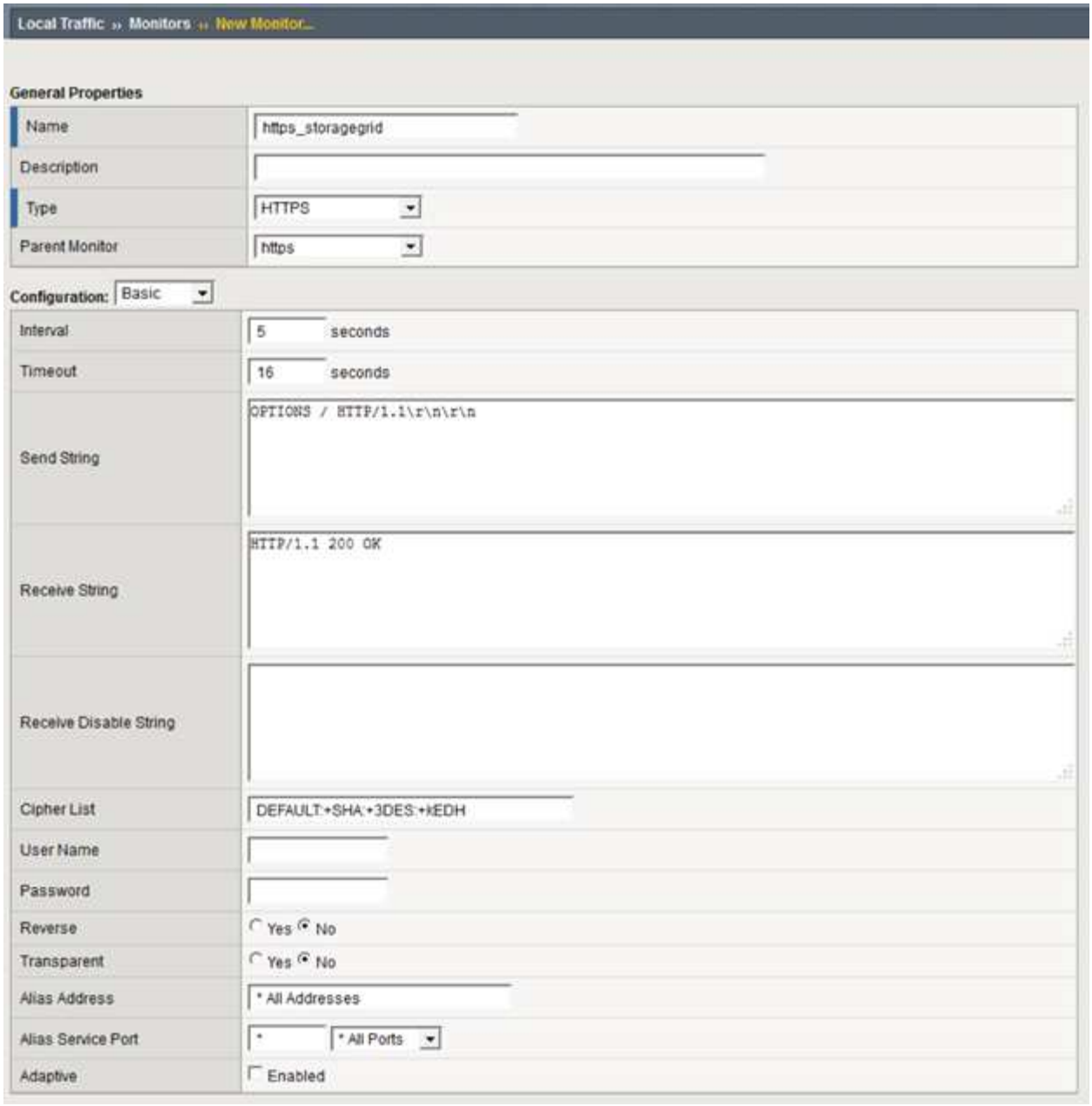
Die folgenden Beispiele veranschaulichen die Konfigurationen, die von StorageGRID Kunden, einschließlich NetApp IT, implementiert wurden.

Systemzustandsüberwachung von F5 BIG-IP Local Traffic Manager für S3 Bucket

Gehen Sie wie folgt vor, um die Integritätsprüfung für den F5 BIG-IP Local Traffic Manager zu konfigurieren:

Schritte

1. Erstellen Sie einen neuen Monitor.
   a. Geben Sie im Feld Typ `HTTPS`.
   b. Konfigurieren Sie das Intervall und die Zeitüberschreitung nach Bedarf.
   c. Geben Sie im Feld Send String \r\n sind Wagenrückläufe ein `OPTIONS / HTTP/1.1\r\n\r\n.` ; verschiedene Versionen der BIG-IP-Software erfordern Null, einen oder zwei Sätze von \r\n Sequenzen. Weitere Informationen finden Sie unter https://support.f5.com/csp/article/K10655.
   d. Geben Sie im Feld Empfangszeichenfolge Folgendes ein: `HTTP/1.1 200 OK`.



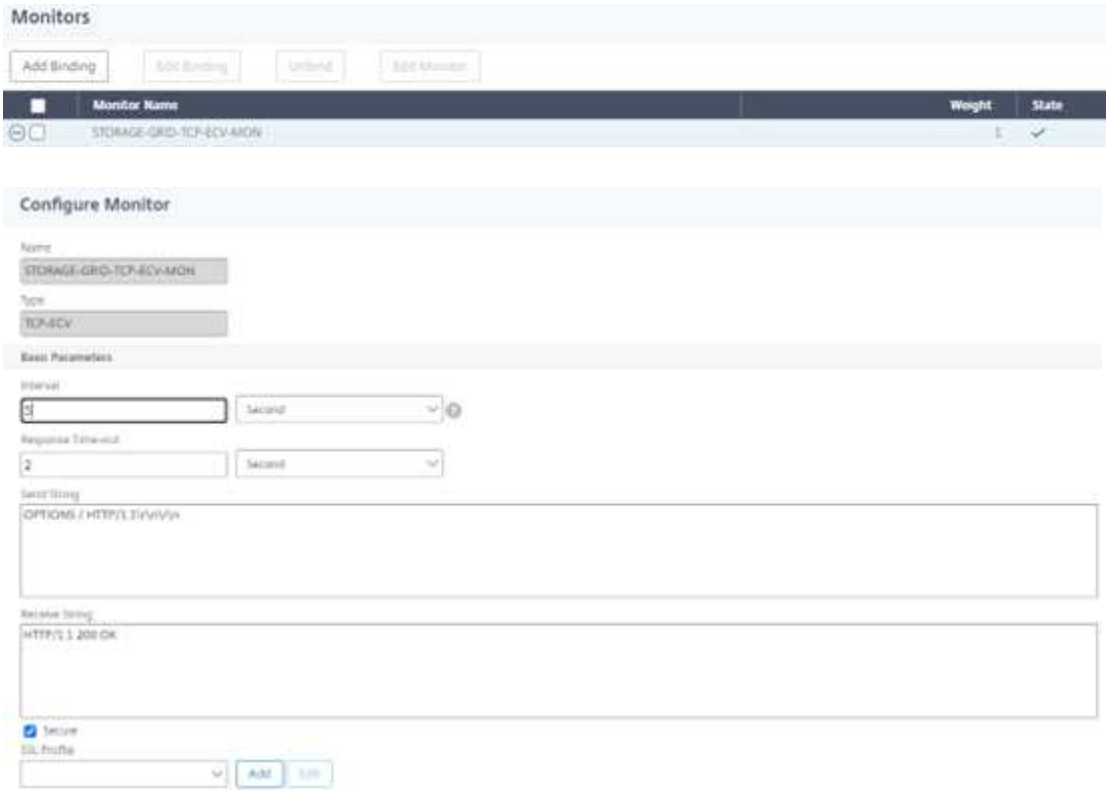
2. Erstellen Sie in Create Pool für jeden erforderlichen Port einen Pool.
   a. Weisen Sie die im vorherigen Schritt erstellte Systemzustandsüberwachung zu.
   b. Wählen Sie eine Lastausgleichsmethode aus.
   c. Wählen Sie Service Port: 18082 (S3).
   d. Nodes hinzufügen.

Citrix NetScaler

Citrix NetScaler erstellt einen virtuellen Server für den Speicherendpunkt und verweist auf StorageGRID-Speicherknoten als Anwendungsserver, die dann in Dienste gruppiert werden.

Verwenden Sie die HTTPS-ECV-Integritätsprüfung, um einen benutzerdefinierten Monitor zu erstellen, der die empfohlene Integritätsprüfung mithilfe der OPTIONSANFRAGE und des Empfangs durchführt `200`. HTTP-ECV ist mit einem Sendestring konfiguriert und validiert eine Empfangszeichenfolge.

Weitere Informationen finden Sie in der Citrix-Dokumentation, "Beispielkonfiguration für HTTP-ECV-Integritätsprüfung".



Loadbalancer.org

Loadbalancer.org hat eigene Integrationstests mit StorageGRID durchgeführt und hat einen umfassenden Konfigurationsleitfaden: https://pdfs.loadbalancer.org/NetApp_StorageGRID_Deployment_Guide.pdf.

Kemp

Kemp hat eigene Integrationstests mit StorageGRID durchgeführt und verfügt über einen umfassenden Konfigurationsleitfaden: https://kemptechnologies.com/solutions/netapp/.

HAProxy

Konfigurieren Sie HAProxy so, dass die OPTIONS-Anfrage verwendet wird, und prüfen Sie auf eine 200-Statusantwort für die Integritätsprüfung in haproxy.cfg. Sie können den Bind-Port am Front-End in einen anderen Port ändern, z. B. 443.

Im Folgenden finden Sie ein Beispiel für die SSL-Terminierung auf HAProxy:

```
frontend s3
       bind *:443 crt /etc/ssl/server.pem ssl
       default_backend s3-serve
rs
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 ssl verify none check inter 3000
       server dc1-s2 10.63.174.72:18082 ssl verify none check inter 3000
       server dc1-s3 10.63.174.73:18082 ssl verify none check inter 3000
```

Im Folgenden ein Beispiel für SSL-Passthrough:

```
frontend s3
       mode tcp
       bind *:443
       default_backend s3-servers
backend s3-servers
       balance leastconn
       option httpchk
       http-check expect status 200
       server dc1-s1 10.63.174.71:18082 check-ssl verify none inter 3000
       server dc1-s2 10.63.174.72:18082 check-ssl verify none inter 3000
       server dc1-s3 10.63.174.73:18082 check-ssl verify none inter 3000
```

Vollständige Beispiele für Konfigurationen für StorageGRID finden Sie unter "Beispiele für die HAProxy-Konfiguration" auf GitHub.

SSL-Verbindung in StorageGRID validieren

Erfahren Sie, wie Sie die SSL-Verbindung in StorageGRID validieren.

Nachdem der Load Balancer konfiguriert ist, sollten Sie die Verbindung mit Tools wie OpenSSL und der AWS CLI validieren. Andere Anwendungen, wie beispielsweise S3 Browser, ignorieren möglicherweise eine fehlerhafte SSL-Konfiguration.

Informationen zu den globalen Lastausgleichsanforderungen für StorageGRID

Informieren Sie sich über die Designüberlegungen und Anforderungen für den globalen Lastausgleich in StorageGRID.

Globaler Lastausgleich erfordert die Integration in DNS, um intelligentes Routing über mehrere StorageGRID-Standorte hinweg zu ermöglichen. Diese Funktion fällt nicht in die StorageGRID-Domäne und muss von einer

Drittanbieterlösung bereitgestellt werden, z. B. den bereits erläuterten Load Balancer-Produkten und/oder einer DNS-Lösung zur Traffic-Kontrolle wie Infoblox. Dieser Lastenausgleich der obersten Ebene bietet intelligentes Routing zum nächsten Zielstandort im Namespace sowie Ausfallerkennung und Umleitung zum nächsten Standort im Namespace. Eine typische GSLB-Implementierung besteht aus dem GSLB der obersten Ebene mit Standortpools mit standortlokalen Load Balancern. Die Standortlastverteiler enthalten Pools der lokalen Speicher-Nodes am Standort. Dies kann eine Kombination aus Load Balancern von Drittanbietern für GSLB-Funktionen und StorageGRID für den lokalen Lastausgleich oder eine Kombination aus Drittanbietern sein. Oder viele der zuvor besprochenen Drittanbieter bieten sowohl GSLB als auch einen standortweiten lokalen Lastausgleich.