Netzwerkrichtlinien

StorageGRID software

NetApp
July 23, 2026

Inhalt

Netzwerkrichtlinien

Netzwerkrichtlinien für StorageGRID

Diese Richtlinien bieten Informationen zur StorageGRID Architektur und zu Netzwerktopologien sowie zu den Anforderungen an die Netzwerkkonfiguration und -bereitstellung.

Über diese Anweisungen

Diese Richtlinien liefern Informationen, mit denen die StorageGRID Netzwerkinfrastruktur vor der Bereitstellung und Konfiguration von StorageGRID Knoten erstellt werden kann. Diese Richtlinien tragen dazu bei, sicherzustellen, dass die Kommunikation zwischen allen Knoten im Grid sowie zwischen dem Grid und externen Clients und Diensten möglich ist.

Externe Clients und externe Dienste müssen eine Verbindung zu StorageGRID Netzwerken herstellen, um Funktionen wie die folgenden auszuführen:

- Objektdaten speichern und abrufen
- E-Mail-Benachrichtigungen empfangen
- Zugriff auf die StorageGRID Managementoberfläche (Grid Manager und Tenant Manager)
- Auf die Auditfreigabe zugreifen (optional)
- Dienstleistungen wie die folgenden werden bereitgestellt:
  - Network Time Protocol (NTP)
  - Domain Name System (DNS)
  - Schlüsselverwaltungsserver (KMS)

StorageGRID Netzwerkarchitektur muss entsprechend konfiguriert werden, um den Datenverkehr für diese Funktionen und mehr zu bewältigen.

Bevor Sie beginnen

Die Konfiguration der Netzwerkinfrastruktur eines StorageGRID Systems erfordert umfassende Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerkrouting und Firewalls.

Bevor Sie das Netzwerk konfigurieren, ist es hilfreich, sich mit der StorageGRID Architektur vertraut zu machen, wie in "Informationen zu StorageGRID" beschrieben.

Nachdem Sie festgelegt haben, welche StorageGRID Netzwerke Sie verwenden möchten und wie diese Netzwerke konfiguriert werden, können die StorageGRID Knoten gemäß den entsprechenden Anweisungen installiert und konfiguriert werden.

Appliance Knoten installieren

- "Gerätehardware installieren"

Softwarebasierte Knoten

- "StorageGRID auf softwarebasierten Knoten installieren"

StorageGRID Software konfigurieren und verwalten

- "StorageGRID verwalten"
- "Versionshinweise". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

StorageGRID Netzwerktypen

Die Grid-Knoten eines StorageGRID Systems verarbeiten Grid-Traffic, Admin-Traffic und Client-Traffic. Die Netzwerkkonfiguration muss entsprechend angepasst werden, um diese drei Arten von Traffic zu verwalten und Kontrolle sowie Sicherheit zu gewährleisten.

Verkehrsarten

Verkehrsart	Beschreibung	Netzwerktyp
Grid-Verkehr	Der interne StorageGRID Datenverkehr, der zwischen allen Knoten im Grid übertragen wird. Alle Grid-Knoten müssen über dieses Netzwerk mit allen anderen Grid-Knoten kommunizieren können.	Grid-Netzwerk (erforderlich)
Administratorverkehr	Der Datenverkehr, der für Systemadministration und Wartung verwendet wird.	Admin-Netzwerk (optional), VLAN Netzwerk (optional)
Client-Datenverkehr	Der gesamte Datenverkehr zwischen externen Clientanwendungen und dem Grid, einschließlich aller Objektspeicheranforderungen von S3-Clients.	Client-Netzwerk (optional), VLAN Netzwerk (optional)

Die Netzwerkkonfiguration ist auf folgende Weise möglich:

- Nur im Grid Network
- Grid und Admin Netzwerke
- Grid und Client Netzwerke
- Grid, Admin und Client Netzwerke

Das Grid Network ist obligatorisch und kann den gesamten Grid-Datenverkehr verwalten. Das Admin Network und das Client Network können bei der Installation einbezogen oder später hinzugefügt werden, um sich an geänderte Anforderungen anzupassen. Obwohl das Admin Network und das Client Network optional sind, kann das Grid Network isoliert und gesichert werden, wenn diese Netzwerke für die Abwicklung des administrativen und des Client-Datenverkehrs verwendet werden.

Interne Ports sind nur über das Grid-Netzwerk erreichbar. Externe Ports sind von allen Netzwerktypen aus erreichbar. Diese Flexibilität bietet vielfältige Möglichkeiten für die Planung einer StorageGRID Bereitstellung und die Einrichtung externer IP- und Portfilter in Switches und Firewalls. Siehe "interne Grid-Knoten-Kommunikation" und "externe Kommunikation".

Netzwerkschnittstellen

StorageGRID Knoten sind über die folgenden spezifischen Schnittstellen mit den jeweiligen Netzwerken verbunden:

Netzwerk	Schnittstellenname
Grid-Netzwerk (erforderlich)	eth0
Admin-Netzwerk (optional)	eth1
Client-Netzwerk (optional)	eth2

Weitere Informationen zur Zuordnung virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie unter "StorageGRID auf softwarebasierten Knoten installieren".

Geräteknoten

- "SG6160 Storage Appliance"
- "SGF6112 Storage Appliance"
- "SG6000 Storage Appliance"
- "SG5800 Storage Appliance"
- "SG5700 Storage Appliance"
- "SG110 und SG1100 Services Appliances"
- "SG100 und SG1000 Services Appliances"

Netzwerkinformationen für jeden Knoten

Für jedes Netzwerk, das Sie auf einem Knoten aktivieren, ist Folgendes zu konfigurieren:

- IP-Adresse
- Subnetzmaske
- Gateway-IP-Adresse

Sie können für jedes der drei Netzwerke auf jedem Grid-Knoten nur eine IP-Adresse/Maske/Gateway-Kombination konfigurieren. Wenn für ein Netzwerk kein Gateway konfiguriert werden soll, ist die IP-Adresse als Gateway-Adresse zu verwenden.

Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (HA-Gruppen) bieten die Möglichkeit, virtuelle IP-Adressen (VIP-Adressen) zur Grid- oder Client-Netzwerkschnittstelle hinzuzufügen. Weitere Informationen finden sich unter "Hochverfügbarkeitsgruppen verwalten".

Grid-Netzwerk

Das Grid Network ist erforderlich. Es wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das Grid Network stellt die Konnektivität zwischen allen Knoten im Grid über alle Standorte und Subnetze hinweg bereit. Alle Knoten im Grid Network müssen mit allen anderen Knoten kommunizieren können. Das Grid Network kann aus mehreren Subnetzen bestehen. Netzwerke mit kritischen Grid-Diensten, wie NTP, können ebenfalls als Grid-Subnetze hinzugefügt werden.

StorageGRID unterstützt keine Netzwerkadressübersetzung (NAT) zwischen Knoten.

Das Grid-Netzwerk kann für den gesamten Admin-Datenverkehr und den gesamten Client-Datenverkehr verwendet werden, selbst wenn das Admin-Netzwerk und das Client-Netzwerk konfiguriert sind. Das Grid-Netzwerk-Gateway ist das Standardgateway des Knotens, es sei denn, für den Knoten ist das Client-Netzwerk konfiguriert.

> Bei der Konfiguration des Grid-Netzwerks muss sichergestellt werden, dass das Netzwerk vor nicht vertrauenswürdigen Clients wie solchen im offenen Internet geschützt ist.

Beachten Sie die folgenden Anforderungen und Details für das Grid Network Gateway:

- Das Grid Network Gateway muss konfiguriert werden, wenn mehrere Grid-Subnetze vorhanden sind.
- Das Grid Network Gateway ist das Standard-Gateway des Knotens, bis die Grid-Konfiguration abgeschlossen ist.
- Für alle Knoten werden automatisch statische Routen zu allen in der globalen Grid Network Subnet List konfigurierten Subnetzen generiert.
- Wenn ein Client-Netzwerk hinzugefügt wird, wechselt das Standardgateway nach Abschluss der Grid-Konfiguration vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway.

${post_edited_translations.segment}

Das Admin Network ist optional. Wenn es konfiguriert ist, kann es für Systemadministration und Wartungsdatenverkehr verwendet werden. Das Admin Network ist typischerweise ein privates Netzwerk und muss nicht zwischen den Knoten routbar sein.

Sie können auswählen, auf welchen Grid-Knoten das Admin-Netzwerk aktiviert sein soll.

Bei Verwendung des Admin Network muss der administrative und Wartungsdatenverkehr nicht über das Grid Network geleitet werden. Typische Anwendungsfälle des Admin Network sind die folgenden:

- Zugriff auf die Benutzeroberflächen von Grid Manager und Tenant Manager.
- Zugriff auf kritische Dienste wie NTP-Server, DNS-Server, externe Schlüsselverwaltungsserver (KMS) und Lightweight Directory Access Protocol (LDAP)-Server.
- Zugriff auf die Überwachungsprotokolle auf den Admin Nodes.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support.

Das Admin Network wird niemals für internen Grid-Datenverkehr verwendet. Ein Admin Network Gateway ist vorhanden und ermöglicht dem Admin Network die Kommunikation mit mehreren externen Subnetzen. Das Admin Network Gateway wird jedoch niemals als Standard-Gateway des Knotens verwendet.

Beachten Sie die folgenden Anforderungen und Details für das Admin Network Gateway:

- Das Admin Network Gateway ist erforderlich, wenn Verbindungen von außerhalb des Admin Network Subnetzes hergestellt werden oder wenn mehrere Admin Network Subnetze konfiguriert sind.
- Statische Routen werden für jedes Subnetz erstellt, das in der Admin-Netzwerk-Subnetzliste des Knotens konfiguriert ist.

Client-Netzwerk

Das Clientnetzwerk ist optional. Wenn es konfiguriert ist, wird es verwendet, um Clientanwendungen wie S3 den Zugriff auf Grid-Dienste bereitzustellen. Wenn StorageGRID-Daten für eine externe Ressource (zum Beispiel einen Cloud Storage Pool oder den StorageGRID CloudMirror Replikationsdienst) zugänglich gemacht

werden sollen, kann diese externe Ressource ebenfalls das Clientnetzwerk verwenden. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Clientnetzwerk-Gateway erreichbar ist.

Sie können auswählen, für welche Grid-Knoten das Client-Netzwerk aktiviert sein soll. Nicht alle Knoten müssen sich im selben Client-Netzwerk befinden, und die Knoten kommunizieren niemals über das Client-Netzwerk miteinander. Das Client-Netzwerk wird erst nach Abschluss der Grid-Installation betriebsbereit.

Zur Erhöhung der Sicherheit kann festgelegt werden, dass die Client Network-Schnittstelle eines Knotens als nicht vertrauenswürdig gilt, sodass das Client Network restriktiver hinsichtlich der zulässigen Verbindungen ist. Wenn die Client Network-Schnittstelle eines Knotens als nicht vertrauenswürdig eingestuft ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie beispielsweise von CloudMirror-Replikation verwendet werden, akzeptiert jedoch eingehende Verbindungen nur auf Ports, die explizit als Load Balancer-Endpunkte konfiguriert wurden. Siehe "Firewall-Steuerung verwalten" und "Load Balancer-Endpunkte konfigurieren".

Wenn ein Client Network verwendet wird, muss der Client-Datenverkehr nicht über das Grid Network laufen. Grid Network-Datenverkehr kann auf ein sicheres, nicht routbares Netzwerk getrennt werden. Die folgenden Knotentypen werden häufig mit einem Client Network konfiguriert:

- Gateway Nodes, da diese Nodes Zugriff auf den StorageGRID Load Balancer Service und S3-Clientzugriff auf das Grid bieten.
- Speicherknoten, da diese Knoten den Zugriff auf das S3-Protokoll und auf Cloud-Speicherpools sowie den CloudMirror Replikationsdienst ermöglichen.
- Admin-Knoten, damit Mandantenbenutzer eine Verbindung zum Tenant Manager herstellen können, ohne das Admin-Netzwerk nutzen zu müssen.

Beachten Sie Folgendes für das Client Network Gateway:

- Das Client Network Gateway ist erforderlich, wenn das Client Network konfiguriert ist.
- Das Client Network Gateway wird zur Standardroute für den Grid-Knoten, sobald die Grid-Konfiguration abgeschlossen ist.

Optionale VLAN Netzwerke

Bei Bedarf können optional virtuelle LAN (VLAN) Netzwerke für Client-Datenverkehr und für bestimmte Arten von Administrator-Datenverkehr verwendet werden. Grid-Datenverkehr kann jedoch keine VLAN-Schnittstelle verwenden. Der interne StorageGRID Datenverkehr zwischen den Knoten muss immer das Grid-Netzwerk auf eth0 verwenden.

Um die Verwendung von VLANs zu unterstützen, muss eine oder mehrere Schnittstellen eines Knotens als Trunk-Schnittstellen am Switch konfiguriert werden. Die Grid Network-Schnittstelle (eth0) oder die Client Network-Schnittstelle (eth2) kann als Trunk konfiguriert werden, oder dem Knoten können Trunk-Schnittstellen hinzugefügt werden.

Wenn eth0 als Trunk konfiguriert ist, fließt der Grid Network-Datenverkehr über die nativ-Schnittstelle des Trunks, wie am Switch konfiguriert. Analog dazu verwendet das Client Network, wenn eth2 als Trunk konfiguriert ist und das Client Network ebenfalls auf demselben Knoten konfiguriert ist, das native VLAN des Trunk-Ports, wie am Switch konfiguriert.

Über VLAN-Netzwerke wird ausschließlich eingehender Administrator-Datenverkehr unterstützt, beispielsweise für SSH, Grid Manager oder Tenant Manager. Ausgehender Datenverkehr, beispielsweise für NTP, DNS, LDAP, KMS und Cloud Storage Pools, wird über VLAN-Netzwerke nicht unterstützt.

VLAN-Schnittstellen können nur zu Admin-Knoten und Gateway-Knoten hinzugefügt werden. Eine VLAN-Schnittstelle kann nicht für den Client- oder Administratorzugriff auf Storage Nodes verwendet werden.

Siehe "${post_edited_translations.segment}" Anweisungen und Richtlinien.

VLAN-Schnittstellen werden nur in HA-Gruppen verwendet und erhalten VIP-Adressen auf dem aktiven Knoten. Siehe "Hochverfügbarkeitsgruppen verwalten" für Anweisungen und Richtlinien.

Beispiele für Netzwerktopologien

Grid-Netzwerktopologie für StorageGRID

Die einfachste Netzwerktopologie wird erstellt, indem nur das Grid-Netzwerk konfiguriert wird.

Bei der Konfiguration des Grid-Netzwerks werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle jedes Grid-Knotens festgelegt.

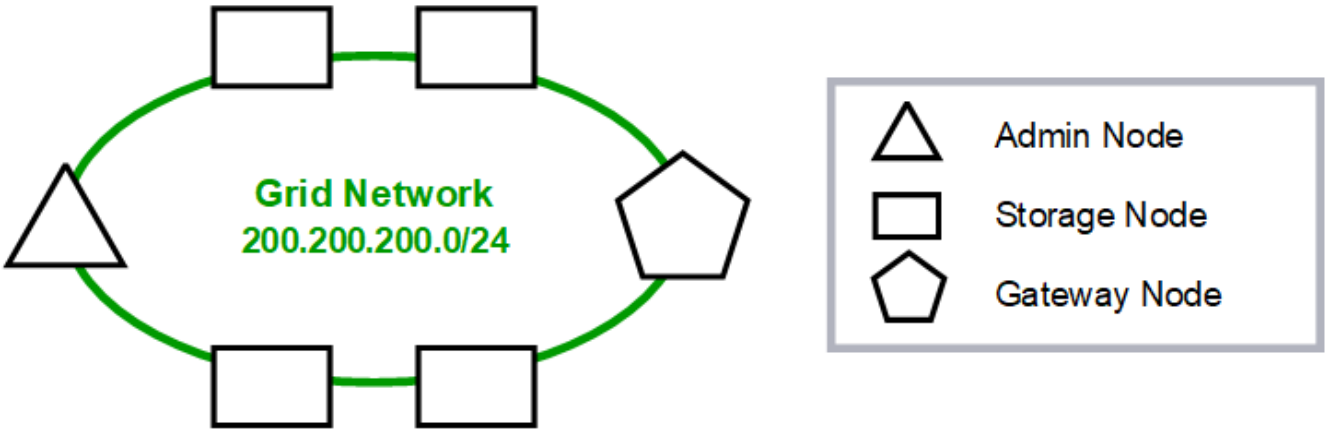
Während der Konfiguration müssen Sie alle Grid Network Subnetze zur Grid Network Subnetzliste (GNSL) hinzufügen. Diese Liste enthält alle Subnetze aller Standorte und kann auch externe Subnetze umfassen, die Zugriff auf wichtige Dienste wie NTP, DNS oder LDAP ermöglichen.

Bei der Installation wendet die Grid-Netzwerk-Schnittstelle statische Routen für alle Subnetze im GNSL an und legt die Standardroute des Knotens auf das Grid Network Gateway fest, sofern eines konfiguriert ist. Das GNSL ist nicht erforderlich, wenn kein Client Network vorhanden ist und das Grid Network Gateway die Standardroute des Knotens ist. Host-Routen zu allen anderen Knoten im Grid werden ebenfalls generiert.

In diesem Beispiel nutzt der gesamte Datenverkehr dasselbe Netzwerk, einschließlich des Datenverkehrs im Zusammenhang mit S3-Clientanfragen sowie administrativen und Wartungsfunktionen.

Diese Topologie eignet sich für Einzelstandortbereitstellungen, die nicht extern verfügbar sind, für Proof-of-Concept- oder Testbereitstellungen oder wenn ein Load Balancer eines Drittanbieters als Clientzugriffsgrenze fungiert. Das Grid-Netzwerk sollte nach Möglichkeit ausschließlich für internen Datenverkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk verfügen über zusätzliche Firewall-Beschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Nutzung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, bietet jedoch weniger Schutzebenen.

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

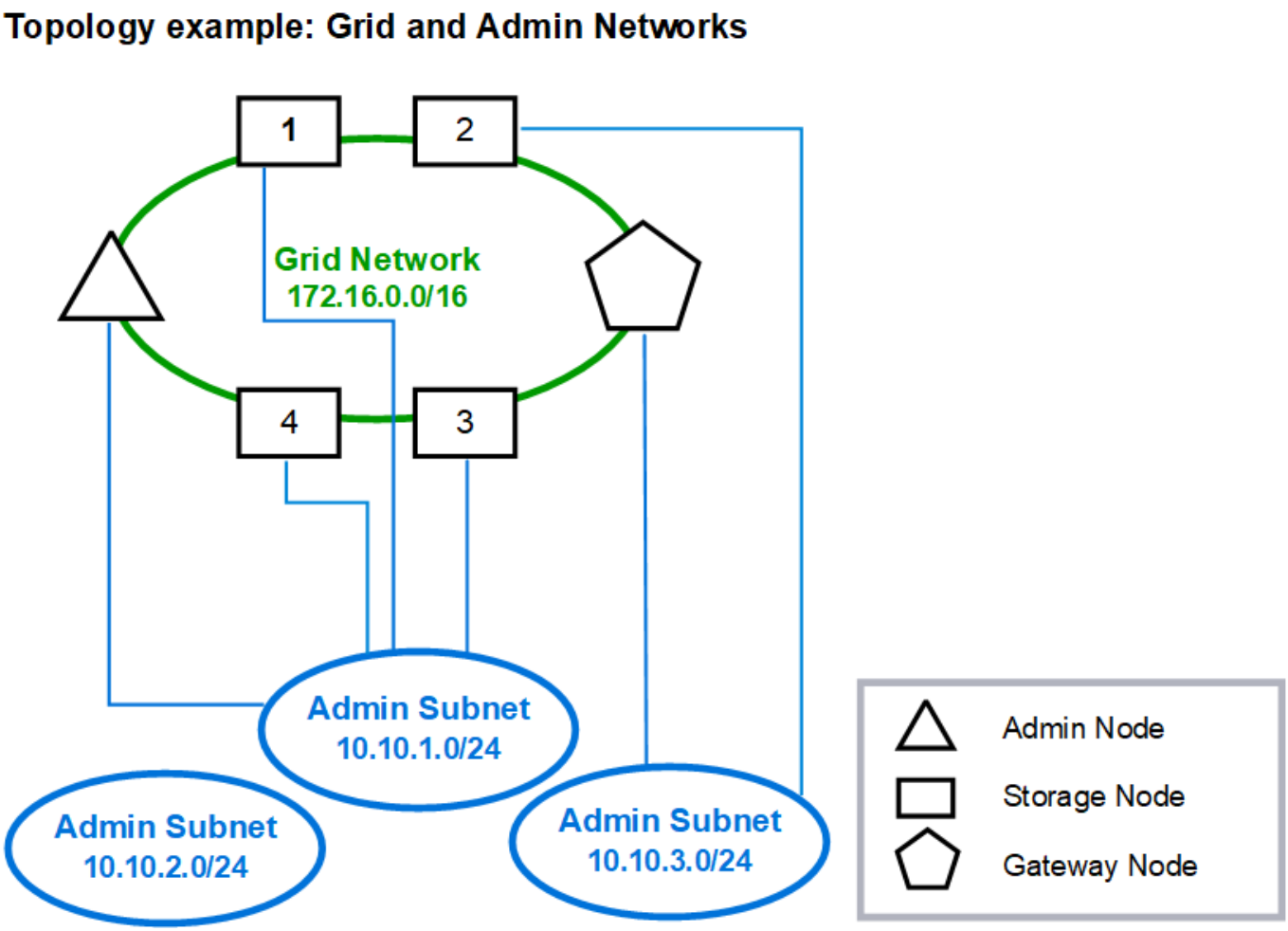
Admin-Netzwerktopologie für StorageGRID

Die Verwendung eines Admin Network ist optional. Eine Möglichkeit, ein Admin Network und ein Grid Network zu nutzen, besteht darin, für jeden Node ein routbares Grid Network und ein begrenztes Admin Network zu konfigurieren.

Bei der Konfiguration des Admin Network werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth1-Schnittstelle jedes Grid-Node festgelegt.

Das Admin Network kann für jeden Node einzigartig sein und aus mehreren Subnetzen bestehen. Jeder Node kann mit einer Admin External Subnet List (AESL) konfiguriert werden. Die AESL listet die Subnetze auf, die über das Admin Network für jeden Node erreichbar sind. Die AESL muss außerdem die Subnetze aller Services enthalten, auf die das Grid über das Admin Network zugreift, wie NTP, DNS, KMS und LDAP. Statische Routen werden für jedes Subnetz in der AESL angewendet.

In diesem Beispiel wird das Grid Network für den Datenverkehr im Zusammenhang mit S3-Clientanfragen und der Objektverwaltung verwendet, während das Admin Network für administrative Funktionen genutzt wird.



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Client-Netzwerktopologie für StorageGRID

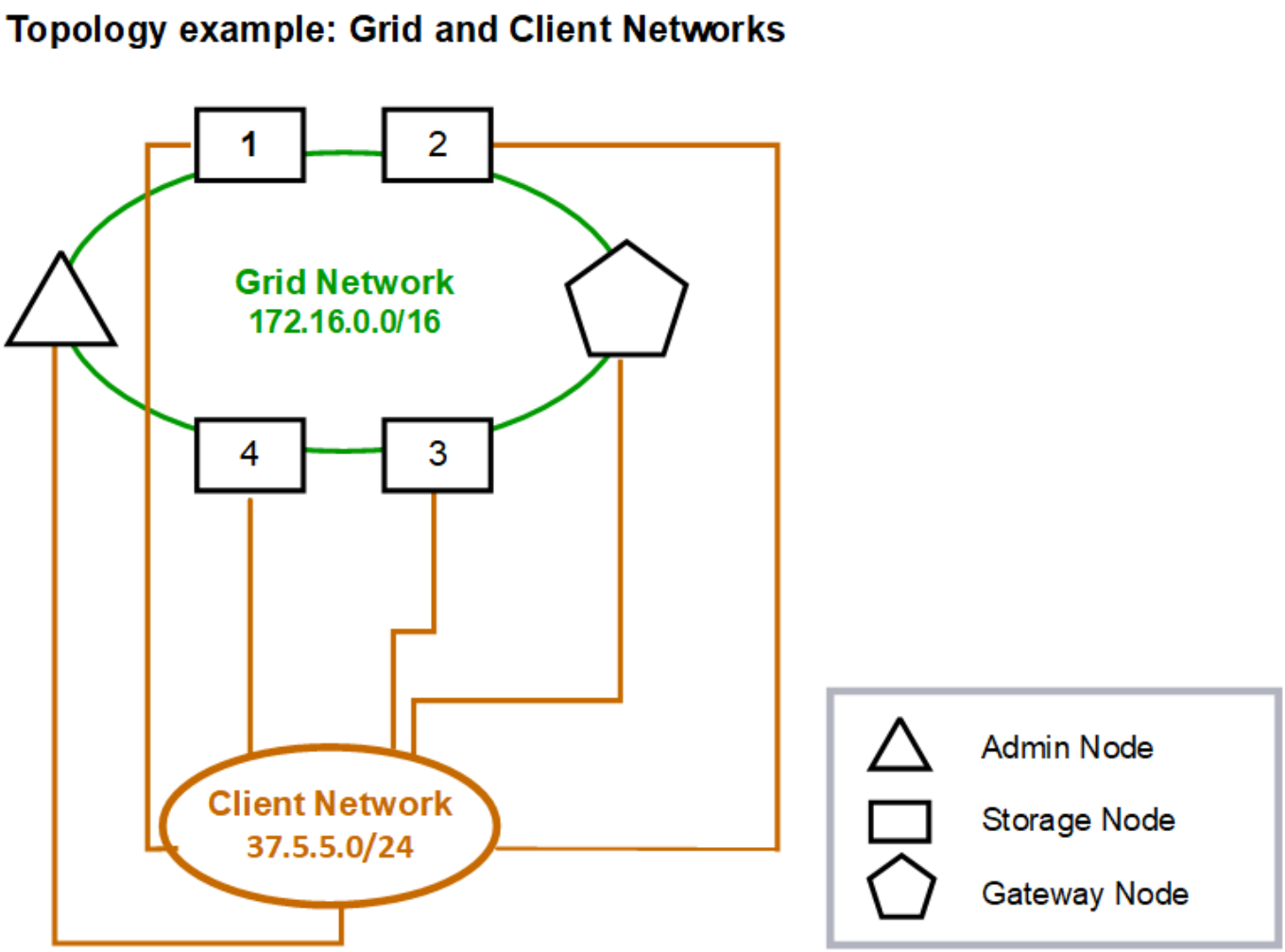
Die Einrichtung eines Client-Netzwerks ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerkverkehr (zum Beispiel S3) vom internen Grid-Verkehr getrennt werden, was das Grid-Netzwerk sicherer macht. Administrativer Datenverkehr kann entweder über das Client- oder das Grid-Netzwerk erfolgen, wenn das Admin-Netzwerk nicht konfiguriert ist.

Bei der Konfiguration des Client Network werden die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle des konfigurierten Node festgelegt. Das Client Network eines jeden Node kann unabhängig vom Client Network eines anderen Node sein.

Wenn während der Installation ein Clientnetzwerk für einen Knoten konfiguriert wird, wechselt das Standardgateway des Knotens nach Abschluss der Installation vom Grid Network Gateway zum Client Network Gateway. Wenn ein Clientnetzwerk später hinzugefügt wird, wechselt das Standardgateway des Knotens auf die gleiche Weise.

In diesem Beispiel wird das Client Network für S3-Client-Anfragen und für administrative Funktionen

verwendet, während das Grid Network für interne Objektmanagement-Operationen vorgesehen ist.



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

Verwandte Informationen

"Netzwerkkonfiguration des Node ändern"

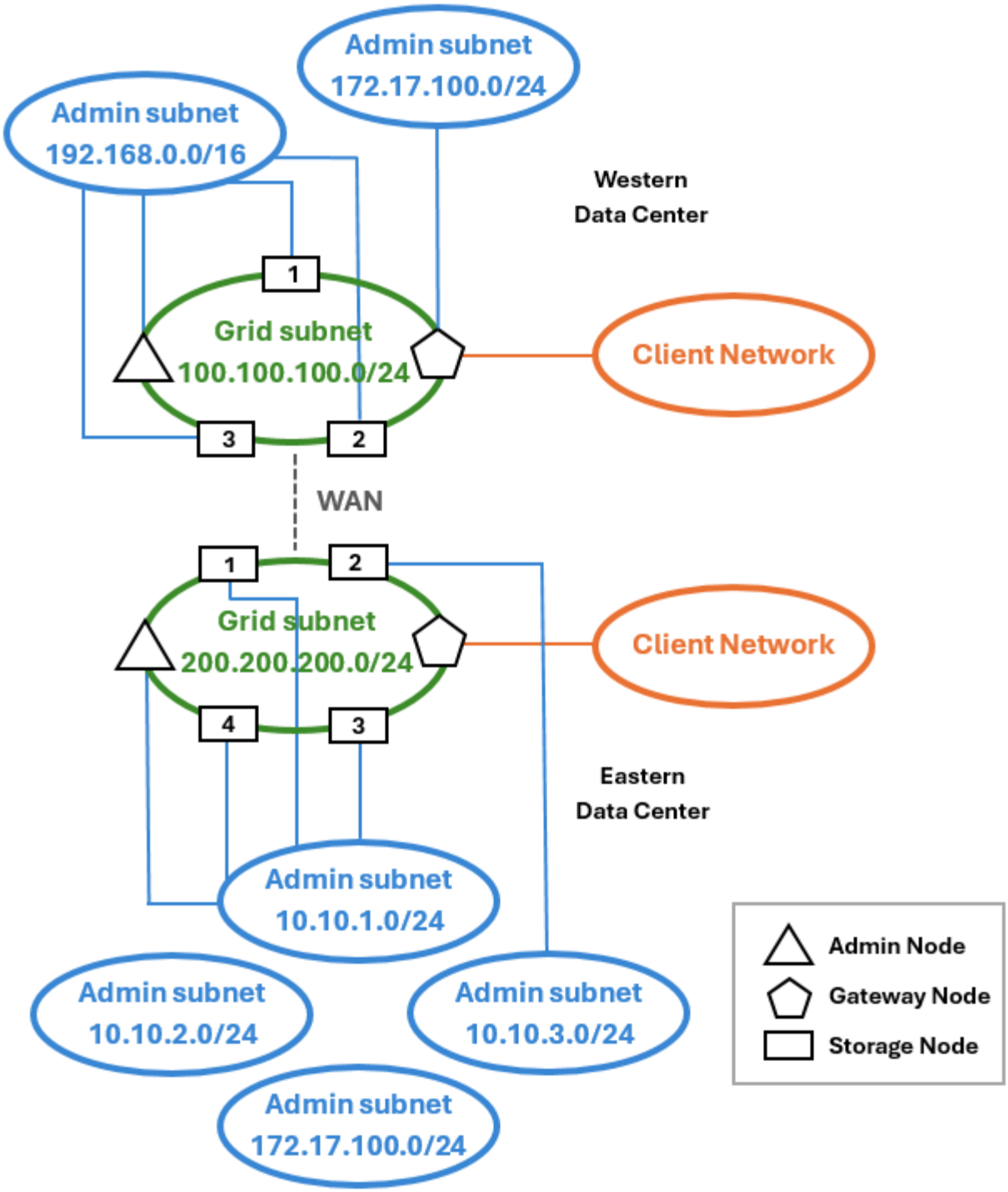
Netzwerktopologie für alle drei StorageGRID Netzwerke

Sie können alle drei Netzwerke zu einer Netzwerktopologie konfigurieren, die aus einem privaten Grid Network, abgegrenzten standortspezifischen Admin Networks und offenen Client Networks besteht. Die Verwendung von Load Balancer Endpunkten und nicht vertrauenswürdigen Client Networks kann bei Bedarf zusätzliche Sicherheit bieten.

In diesem Beispiel:

- Das Grid Network wird für Netzwerkverkehr im Zusammenhang mit internen Objektverwaltungsoperationen verwendet.
- Das Admin Network wird für Datenverkehr im Zusammenhang mit administrativen Funktionen verwendet.
- Das Client-Netzwerk wird für den Datenverkehr im Zusammenhang mit S3-Client-Anfragen verwendet.

Topologiebeispiel: Grid, Admin und Client Netzwerke



Netzwerkanforderungen für StorageGRID

Es ist zu überprüfen, ob die aktuelle Netzwerkinfrastruktur und -konfiguration das geplante StorageGRID Netzwerkdesign unterstützen kann.

Allgemeine Netzwerkanforderungen

Alle StorageGRID Bereitstellungen müssen die folgenden Verbindungen unterstützen können.

Diese Verbindungen können über das Grid, Admin oder Client Netzwerk oder über Kombinationen dieser Netzwerke erfolgen, wie in den Beispielen zur Netzwerktopologie dargestellt.

- **Verwaltungsverbindungen**: Eingehende Verbindungen von einem Administrator zum Knoten, üblicherweise über SSH. Webbrowser-Zugriff auf den Grid Manager, den Tenant Manager und den StorageGRID Appliance Installer.
- **NTP-Serververbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.

  Mindestens ein NTP-Server muss vom primären Admin-Knoten erreichbar sein.
- **DNS-Server-Verbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory Serververbindungen**: Ausgehende TCP-Verbindung vom Identity Service auf Storage Nodes.
- **AutoSupport**: Ausgehende TCP-Verbindung von den Admin-Nodes zu entweder `support.netapp.com` oder einem vom Kunden konfigurierten Proxy.
- **Externer Schlüsselverwaltungsserver**: Ausgehende TCP-Verbindung von jedem Appliance-Knoten mit aktivierter Knotenverschlüsselung.
- Eingehende TCP-Verbindungen von S3 Clients.
- Ausgehende Anfragen von StorageGRID Plattformdiensten wie CloudMirror Replikation oder von Cloud Storage Pools.

Kann StorageGRID keinen der bereitgestellten NTP- oder DNS-Server über die Standard-Routingregeln erreichen, wird automatisch versucht, über alle Netzwerke (Grid, Admin und Client) Kontakt aufzunehmen, sofern die IP-Adressen der DNS- und NTP-Server angegeben sind. Sind die NTP- oder DNS-Server über ein Netzwerk erreichbar, erstellt StorageGRID automatisch zusätzliche Routingregeln, damit dieses Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.

Obwohl Sie diese automatisch ermittelten Hostrouten nutzen können, sollte im Allgemeinen die manuelle Konfiguration der DNS- und NTP-Routen erfolgen, um die Konnektivität sicherzustellen, falls die automatische Ermittlung fehlschlägt.

Wenn Sie die optionalen Admin- und Clientnetzwerke während der Bereitstellung noch nicht konfigurieren möchten, können Sie diese Netzwerke konfigurieren, wenn Sie die Grid-Knoten während der Konfigurationsschritte genehmigen. Zusätzlich können Sie diese Netzwerke nach der Installation mit dem Tool „IP ändern“ konfigurieren (siehe "IP-Adressen konfigurieren").

Über VLAN-Schnittstellen werden ausschließlich S3-Client-Verbindungen sowie SSH-, Grid Manager- und Tenant Manager-Administrationsverbindungen unterstützt. Ausgehende Verbindungen, wie zu NTP-, DNS-, LDAP-, AutoSupport und KMS-Servern, müssen direkt über die Client-, Admin- oder Grid-Netzwerkschnittstellen erfolgen. Wenn die Schnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, fließt dieser Datenverkehr über das native VLAN der Schnittstelle, wie am Switch konfiguriert.

Weitverkehrsnetze (WANs) für mehrere Standorte

Bei der Konfiguration eines StorageGRID Systems mit mehreren Standorten muss die WAN-Verbindung zwischen den Standorten eine Mindestbandbreite von 25 Mbit/s in jeder Richtung aufweisen, bevor der Client-Datenverkehr berücksichtigt wird. Datenreplikation oder Erasure Coding zwischen Standorten, Knoten- oder Standorterweiterung, Knotenwiederherstellung und andere Vorgänge oder Konfigurationen erfordern zusätzliche Bandbreite.

Die tatsächlichen Mindestanforderungen an die WAN-Bandbreite hängen von der Clientaktivität und dem ILM-

Schutzschema ab. Für Unterstützung bei der Abschätzung der Mindestanforderungen an die WAN-Bandbreite steht Ihr NetApp Professional Services Berater zur Verfügung.

Verbindungen für Admin Nodes und Gateway Nodes

Admin Nodes müssen stets vor nicht vertrauenswürdigen Clients, wie zum Beispiel solchen aus dem offenen Internet, geschützt werden. Es muss sichergestellt sein, dass kein nicht vertrauenswürdiger Client auf einen Admin Node im Grid Network, im Admin Network oder im Client Network zugreifen kann.

Admin Nodes und Gateway Nodes, die zu Hochverfügbarkeitsgruppen hinzugefügt werden sollen, müssen mit einer statischen IP-Adresse konfiguriert sein. Weitere Informationen finden sich unter "Hochverfügbarkeitsgruppen verwalten".

Verwendung von Netzwerkadressübersetzung (NAT)

Keine Netzwerkadressübersetzung (NAT) im Grid Network zwischen Grid-Knoten oder zwischen StorageGRID Sites verwenden. Wenn private IPv4-Adressen für das Grid Network verwendet werden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routbar sein. Falls erforderlich, kann jedoch NAT zwischen externen Clients und Grid-Knoten eingesetzt werden, beispielsweise um einer Gateway Node eine öffentliche IP-Adresse bereitzustellen. Die Verwendung von NAT zur Überbrückung eines öffentliches Netzwerk Segments wird nur unterstützt, wenn eine Tunneling-Anwendung eingesetzt wird, die für alle Knoten im Grid transparent ist, das heißt, die Grid-Knoten benötigen keine Kenntnis öffentlicher IP-Adressen.

Netzwerkspezifische Anforderungen für StorageGRID

Die Anforderungen für jeden StorageGRID Netzwerktyp sind zu beachten.

Netzwerk Gateways und Router

- Falls festgelegt, muss sich das Gateway für ein bestimmtes Netzwerk innerhalb des jeweiligen Subnetzes befinden.
- Wenn Sie eine Schnittstelle mit statischer Adressierung konfigurieren, muss eine andere Gateway-Adresse als 0.0.0.0 angegeben werden.
- Wenn kein Gateway vorhanden ist, gilt es als Best Practice, die Gateway-Adresse auf die IP-Adresse der Netzwerkschnittstelle zu setzen.

Subnetze

> Jedes Netzwerk muss mit einem eigenen Subnetz verbunden sein, das sich mit keinem anderen Netzwerk auf dem Knoten überschneidet.

Die folgenden Einschränkungen werden vom Grid Manager während der Bereitstellung durchgesetzt. Sie sind hier zur Unterstützung der Netzwerkplanung vor der Bereitstellung aufgeführt.

- Die Subnetzmaske für eine Netzwerk-IP-Adresse darf nicht 255.255.255.254 oder 255.255.255.255 (/31 oder /32 in CIDR-Notation) sein.
- Das durch eine Netzwerkschnittstellen-IP-Adresse und Subnetzmaske (CIDR) definierte Subnetz darf sich nicht mit dem Subnetz einer anderen auf demselben Knoten konfigurierten Schnittstelle überschneiden.
- Für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines beliebigen Knotens sollten keine Subnetze verwendet werden, die die folgenden IPv4-Adressen enthalten:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4

  Beispielsweise sollten die folgenden Subnetzbereiche nicht für das Grid Network, das Admin Network oder das Client Network eines beliebigen Knotens verwendet werden:

  - 192.168.130.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.130.101 und 192.168.130.102 enthält
  - 192.168.131.0/24, da dieser Subnetzbereich die IP-Adressen 192.168.131.101 und 192.168.131.102 enthält
  - 198.51.100.0/24, da dieser Subnetzbereich die IP-Adressen 198.51.100.2 und 198.51.100.4 enthält

- Das Grid Network Subnetz für jeden Knoten muss in die GNSL aufgenommen werden.
- Das Admin Network-Subnetz darf sich nicht mit dem Grid Network-Subnetz, dem Client Network-Subnetz oder einem Subnetz im GNSL überschneiden.
- Die Subnetze im AESL dürfen sich nicht mit Subnetzen im GNSL überschneiden.
- Das Client Network-Subnetz darf sich nicht mit dem Grid Network-Subnetz, dem Admin Network-Subnetz, einem beliebigen Subnetz im GNSL oder einem beliebigen Subnetz im AESL überschneiden.

Grid-Netzwerk

- Zur Implementierungszeit muss jeder Grid-Knoten an das Grid Network angeschlossen sein und mit dem primären Admin Node über die Netzwerkkonfiguration kommunizieren können, die bei der Bereitstellung des Knotens angegeben wird.
- Während des normalen Grid-Betriebs muss jeder Grid-Knoten in der Lage sein, über das Grid-Netzwerk mit allen anderen Grid-Knoten zu kommunizieren.

> ⓘ Das Grid-Netzwerk muss zwischen jedem Knoten direkt routingfähig sein. Network Address Translation (NAT) zwischen Knoten wird nicht unterstützt.

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, werden diese der Grid-Netzwerk-Subnetzliste (GNSL) hinzugefügt. Statische Routen werden auf allen Knoten für jedes Subnetz in der GNSL erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das native Trunk-VLAN dasjenige sein, das für den Grid-Netzwerkdatenverkehr verwendet wird. Alle Grid-Knoten müssen über das native Trunk-VLAN erreichbar sein.

${post_edited_translations.segment}

Das Admin-Netzwerk ist optional. Wenn ein Admin-Netzwerk konfiguriert werden soll, gelten die folgenden Anforderungen und Richtlinien.

Typische Anwendungsfälle des Admin Network sind Management-Verbindungen, AutoSupport, KMS und Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, sofern diese Verbindungen nicht über das Grid Network oder das Client Network bereitgestellt werden.

> Das Admin Network und AESL können für jeden Node einzigartig sein, solange die gewünschten Netzwerkdienste und Clients erreichbar sind.

> Sie müssen mindestens ein Subnetz im Admin Network definieren, um eingehende Verbindungen von externen Subnetzen zu ermöglichen. Statische Routen werden automatisch auf jedem Node für jedes Subnetz in der AESL generiert.

Client-Netzwerk

Das Clientnetzwerk ist optional. Bei der Konfiguration eines Clientnetzwerks sind die folgenden Punkte zu beachten.

- Das Client Network ist für die Unterstützung des Datenverkehrs von S3-Clients ausgelegt. Wenn konfiguriert, wird das Client Network Gateway zum Standardgateway des Knotens.
- Wenn Sie ein Client Network verwenden, kann StorageGRID vor feindlichen Angriffen geschützt werden, indem eingehender Client-Datenverkehr nur an explizit konfigurierten Load Balancer-Endpunkten akzeptiert wird. Siehe "Load Balancer-Endpunkte konfigurieren".
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, sollte berücksichtigt werden, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn konfiguriert, fließt der Client-Netzwerkdatenverkehr über das im Switch konfigurierte native VLAN des Trunks.

Verwandte Informationen

"Netzwerkkonfiguration des Node ändern"

Bereitstellungsspezifische Netzwerküberlegungen

Netzwerkkonfiguration für StorageGRID Linux-Bereitstellungen

Das StorageGRID System läuft aus Gründen der Effizienz, Zuverlässigkeit und Sicherheit unter Linux als Sammlung von Container-Engines. Eine container-engine-bezogene Netzwerkkonfiguration ist in einem StorageGRID System nicht erforderlich.

Für die Container-Netzwerkschnittstelle sollte ein Gerät ohne Bonding, wie ein VLAN oder ein virtuelles Ethernet-Paar (veth), verwendet werden. Dieses Gerät ist in der Knotenkonfigurationsdatei als Netzwerkschnittstelle anzugeben.

> Bond- oder Bridge-Geräte sollten nicht direkt als Container-Netzwerkschnittstelle verwendet werden. Dies könnte den Start des Knotens aufgrund eines Kernel-Problems bei der Verwendung von macvlan mit Bond- und Bridge-Geräten im Container-Namespace verhindern.

Siehe "Installationsanleitung".

Host-Netzwerkkonfiguration für Container Engine-Bereitstellungen

Vor Beginn der StorageGRID Implementierung auf einer Container-Engine-Plattform ist festzulegen, welche Netzwerke (Grid, Admin, Client) von den einzelnen Knoten verwendet werden. Es ist sicherzustellen, dass die Netzwerkschnittstelle jedes Knotens auf der korrekten virtuellen oder physischen Host-Schnittstelle konfiguriert ist und dass jedes Netzwerk über ausreichende Bandbreite verfügt.

Physische Hosts

Wenn Sie physische Hosts zur Unterstützung von Grid-Knoten verwenden:

- Alle Hosts sollten für jede Knotenschnittstelle dieselbe Host-Schnittstelle verwenden. Diese Strategie vereinfacht die Host-Konfiguration und ermöglicht zukünftige Knotenmigrationen.
- Eine IP-Adresse für den physischen Host selbst erhalten.

> Eine physische Schnittstelle des Hosts kann vom Host selbst und von einem oder mehreren auf dem Host laufenden Knoten verwendet werden. Alle dem Host oder den Knoten über diese Schnittstelle zugewiesenen IP-Adressen müssen eindeutig sein. Der Host und der Knoten können keine IP-Adressen gemeinsam nutzen.

- Die erforderlichen Ports zum Host müssen geöffnet werden.
- Wenn VLAN-Schnittstellen in StorageGRID verwendet werden sollen, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die den Zugriff auf die gewünschten VLANs ermöglichen. Diese Schnittstellen können dem Node-Container als eth0, eth2 oder als zusätzliche Schnittstellen zugewiesen werden. Zum Hinzufügen von Trunk- oder Access-Schnittstellen siehe Folgendes:
  - **Linux (vor der Installation des Node)**: "Knotenkonfigurationsdateien erstellen"
  - **Linux (nach der Installation des Nodes)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"

> „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Installation. Eine Liste der unterstützten Versionen befindet sich unter "NetApp Interoperabilitätsmatrix Tool (IMT)".

Empfehlungen zur Mindestbandbreite

Die folgende Tabelle enthält die empfohlenen Mindestbandbreiten für das LAN für jeden StorageGRID-Knotentyp und jeden Netzwerktyp. Jeder physische oder virtuelle Host muss mit ausreichender Netzwerkbandbreite ausgestattet werden, um die aggregierten Mindestbandbreitenanforderungen für die Gesamtzahl und den Typ der StorageGRID-Knoten zu erfüllen, die auf diesem Host betrieben werden sollen.

Knotentyp	**Netzwerktyp**		
	Grid	Administrator	Client
	Minimale LAN Bandbreite	Administrator	10 Gbit/s
1 Gbit/s	1 Gbit/s	Gateway	10 Gbit/s

Knotentyp	Netzwerktyp		
1 Gbit/s	10 Gbit/s	Storage	10 Gbit/s
1 Gbit/s	10 Gbit/s	Archiv	10 Gbit/s

Diese Tabelle enthält keine SAN Bandbreite, die für den Zugriff auf gemeinsam genutzten Speicher erforderlich ist. Bei gemeinsam genutztem Speicher, auf den über Ethernet (iSCSI oder FCoE) zugegriffen wird, sollten auf jedem Host separate physische Schnittstellen bereitgestellt werden, um ausreichende SAN Bandbreite zu gewährleisten. Um einen Engpass zu vermeiden, sollte die SAN Bandbreite eines Hosts in etwa der aggregierten Storage Node Netzwerkbandbreite aller auf diesem Host ausgeführten Storage Nodes entsprechen.

Anhand der Tabelle lässt sich die Mindestanzahl der auf jedem Host bereitzustellenden Netzwerkschnittstellen ermitteln, basierend auf der Anzahl und Art der StorageGRID Knoten, die auf diesem Host ausgeführt werden sollen.

Beispielsweise kann ein Admin Node, ein Gateway Node und ein Storage Node auf einem einzigen Host betrieben werden:

- Das Grid- und das Admin-Netzwerk werden auf dem Admin-Knoten verbunden (erfordert 10 + 1 = 11 Gbit/s)
- Das Grid- und das Client-Netzwerk am Gateway-Knoten verbinden (erfordert 10 + 10 = 20 Gbit/s)
- Das Grid Network am Storage Node verbinden (erfordert 10 Gbit/s)

In diesem Szenario ist eine Mindestbandbreite von 11 + 20 + 10 = 41 Gbit/s an Netzwerkbandbreite bereitzustellen, was durch zwei 40 Gbit/s-Schnittstellen oder fünf 10 Gbit/s-Schnittstellen erfüllt werden könnte, die gegebenenfalls zu Trunks zusammengefasst und dann von den drei oder mehr VLANs gemeinsam genutzt werden, welche die Grid-, Admin- und Client-Subnetze enthalten, die lokal im physischen Rechenzentrum liegen, in dem sich der Host befindet.

Einige empfohlene Methoden zur Konfiguration der physischen und Netzwerkressourcen auf den Hosts Ihres StorageGRID Clusters zur Vorbereitung Ihrer StorageGRID Bereitstellung sind unter "Das Hostnetzwerk konfigurieren" zu finden.

Netzwerk und Ports für Plattformdienste und Cloud Storage Pools

Wenn Sie StorageGRID Plattformdienste oder Cloud Storage Pools verwenden möchten, müssen Grid-Netzwerkfunktionen und Firewalls so konfiguriert werden, dass die Zielendpunkte erreichbar sind.

Vernetzung für Plattformdienste

Wie in "Plattformdienste für Mandanten verwalten" und "Plattformdienste verwalten" beschrieben, umfassen Plattformdienste externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bereitstellen.

Plattformdienste benötigen Zugriff von Speicherknoten, die den StorageGRID ADC Service hosten, auf die externen Dienstendpunkte. Beispiele für die Bereitstellung dieses Zugriffs sind:

- Auf den Speicherknoten mit ADC-Diensten werden eindeutige Admin-Netzwerke mit AESL-Einträgen

konfiguriert, die zu den Zielendpunkten routen.

- Die vom Clientnetzwerk bereitgestellte Standardroute kann verwendet werden. Bei Nutzung der Standardroute besteht die Möglichkeit, mit "Funktion „Untrusted Client Network“" eingehende Verbindungen einzuschränken.

Netzwerk für Cloud Storage Pools

Cloud Storage Pools erfordern ebenfalls Zugriff von den Storage Nodes auf die von dem verwendeten externen Dienst bereitgestellten Endpunkte, wie etwa Amazon S3 Glacier oder Microsoft Azure Blob storage. Weitere Informationen sind unter "Was ist ein Cloud Storage Pool" zu finden.

Ports für Plattformdienste und Cloud Storage Pools

Standardmäßig verwenden Plattformdienste und Cloud Storage Pool-Kommunikation die folgenden Ports:

- **80**: Für Endpunkt-URIs, die mit `http`
- **443**: Für Endpunkt-URIs, die mit `https`

Beim Erstellen oder Bearbeiten des Endpunkts kann ein anderer Port angegeben werden. Siehe "Netzwerkport-Referenz".

Wenn Sie einen nicht transparenten Proxyserver verwenden, muss auch "Speicher-Proxy-Einstellungen konfigurieren" zugelassen werden, damit Nachrichten an externe Endpunkte wie einen Endpunkt im Internet gesendet werden können.

VLANs, Plattformdienste und Cloud Storage Pools

VLAN-Netzwerke können nicht für Plattformdienste oder Cloud Storage Pools verwendet werden. Die Zielendpunkte müssen über das Grid, Admin oder Client Network erreichbar sein.

Netzwerkkonfiguration für StorageGRID Appliance-Nodes

Sie können die Netzwerkports auf StorageGRID Appliances so konfigurieren, dass die Port-Bond-Modi verwendet werden, die Ihren Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

Die 10/25-GbE Ports der StorageGRID Appliances können im Fixed oder Aggregate Bond-Modus für Verbindungen zum Grid-Netzwerk und Client-Netzwerk konfiguriert werden.

Die 1-GbE Admin Network Ports können für Verbindungen zum Admin Network im Independent- oder Active-Backup-Modus konfiguriert werden.

Informationen zu den Port-Bonding-Modi Ihres Geräts:

- "Port-Bond-Modi (SG6160)"
- "Port-Bond-Modi (SGF6112)"
- "Port-Bonding-Modi (SG6000-CN Controller)"
- "Port-Bond-Modi (SG5800 Controller)"
- "Port-Bond-Modi (E5700SG Controller)"
- "Port-Bond-Modi (SG110 und SG1100)"

- "Port-Bond-Modi (SG100 und SG1000)"

Netzwerkinstallation und Bereitstellung für StorageGRID

Sie müssen verstehen, wie das Grid Network sowie die optionalen Admin und Client Networks während der Knotenbereitstellung und Grid-Konfiguration verwendet werden.

Erstmalige Bereitstellung eines Knotens

Bei der erstmaligen Bereitstellung eines Knotens muss der Knoten mit dem Grid Network verbunden werden, und es muss sichergestellt sein, dass er Zugriff auf den primären Admin Node hat. Wenn das Grid Network isoliert ist, kann das Admin Network auf dem primären Admin Node für Konfigurations- und Installationszugriffe von außerhalb des Grid Network konfiguriert werden.

Ein Grid-Netzwerk mit konfiguriertem Gateway wird während der Bereitstellung zum Standardgateway für einen Knoten. Das Standardgateway ermöglicht Grid-Knoten in separaten Subnetzen die Kommunikation mit dem primären Admin-Knoten, bevor das Grid konfiguriert wurde.

Falls erforderlich, können auch Subnetze, die NTP-Server enthalten oder Zugriff auf den Grid Manager oder die API benötigen, als Grid Subnetze konfiguriert werden.

Automatische Knotenregistrierung beim primären Admin Node

Nach der Bereitstellung registrieren sich die Knoten über das Grid-Netzwerk beim primären Admin Node. Anschließend kann der Grid Manager, das `configure-storagegrid.py` Python-Skript oder die Installation API verwendet werden, um das Grid zu konfigurieren und die registrierten Knoten zu genehmigen. Während der Grid-Konfiguration können mehrere Grid-Subnetze konfiguriert werden. Statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway werden auf jedem Knoten erstellt, wenn die Grid-Konfiguration abgeschlossen ist.

Deaktivierung des Admin-Netzwerks oder des Client-Netzwerks

Wenn Sie das Admin Network oder das Client Network deaktivieren möchten, kann die Konfiguration während des Knotengenehmigungsprozesses entfernt werden, oder das Change IP Tool kann nach Abschluss der Installation verwendet werden (siehe "IP-Adressen konfigurieren").

Richtlinien nach der Installation für StorageGRID

Nach Abschluss der Bereitstellung und Konfiguration der Grid-Knoten gelten diese Richtlinien für die DHCP-Adressierung und Änderungen der Netzwerkkonfiguration.

- Wenn DHCP zur Zuweisung von IP-Adressen verwendet wurde, sollte für jede IP-Adresse in den verwendeten Netzwerken eine DHCP-Reservierung konfiguriert werden.

  DHCP kann nur während der Bereitstellungsphase eingerichtet werden. DHCP kann während der Konfiguration nicht eingerichtet werden.

  Die Knoten werden neu gestartet, wenn die Grid-Netzwerkkonfiguration per DHCP geändert wird, was zu Ausfällen führen kann, wenn eine DHCP-Änderung mehrere Knoten gleichzeitig betrifft.

- Die Verfahren zum Ändern der IP-Adresse sind erforderlich, wenn IP-Adressen, Subnetzmasken und Standardgateways für einen Grid-Knoten geändert werden sollen. Siehe "IP-Adressen konfigurieren".
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin Node und zu anderen Grid-Nodes verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen kann es erforderlich sein, diese Verbindungen erneut herzustellen.

Netzwerkport-Referenz

Interne Grid-Knotenkommunikation für StorageGRID

Die StorageGRID interne Firewall erlaubt eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. Verbindungen werden auch an Ports akzeptiert, die von Load-Balancer-Endpunkten definiert sind.

> NetApp empfiehlt, den Internet Control Message Protocol (ICMP)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Die Zulassung von ICMP-Datenverkehr kann die Failover-Leistung verbessern, wenn ein Grid-Knoten nicht erreichbar ist.

Zusätzlich zu ICMP und den in der Tabelle aufgeführten Ports verwendet StorageGRID das Virtual Router Redundancy Protocol (VRRP). VRRP ist ein Internetprotokoll, das die IP-Protokollnummer 112 verwendet. StorageGRID verwendet VRRP ausschließlich im Unicast-Modus. VRRP ist nur erforderlich, wenn "Hochverfügbarkeitsgruppen" konfiguriert sind.

Richtlinien für Linux-basierte Knoten

Falls die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können Ports während der Implementierungszeit mithilfe eines Bereitstellungskonfigurationsparameters neu zugeordnet werden. Weitere Informationen zur Portneuzuordnung und zu Bereitstellungskonfigurationsparametern sind unter "StorageGRID auf softwarebasierten Knoten installieren" zu finden.

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf Bare-Metal-Hosts entfernen".

Richtlinien für VMware basierte Knoten

Die folgenden Ports sind nur zu konfigurieren, wenn Firewall-Beschränkungen definiert werden müssen, die außerhalb des VMware-Netzwerks liegen.

Falls die Netzwerkrichtlinien Ihres Unternehmens den Zugriff auf einen dieser Ports einschränken, können Ports bei der Bereitstellung von Knoten mithilfe des VMware vSphere Web Clients oder durch eine Konfigurationsdatei-Einstellung bei der Automatisierung der Grid-Knoten-Bereitstellung neu zugeordnet werden. Weitere Informationen zur Port-Neuzuordnung und zu den Bereitstellungskonfigurationsparametern enthält die Anleitung für "Installation von StorageGRID auf VMware".

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf Bare-Metal-Hosts entfernen".

Richtlinien für Geräteknoten

Falls die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können die Ports mithilfe des StorageGRID Appliance Installers neu zugeordnet werden. Siehe "Optional: Netzwerkports für das Appliance neu zuordnen".

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf StorageGRID Appliances entfernen".

StorageGRID interne Ports

Port	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsarbeiten muss der primäre Admin-Knoten über SSH auf Port 22 mit allen anderen Knoten kommunizieren können. Das Zulassen von SSH-Datenverkehr von anderen Knoten ist optional.
80	TCP	Appliances	Primärer Admin-Knoten	Wird von StorageGRID Appliances verwendet, um mit dem primären Admin-Node zu kommunizieren und die Installation zu starten.
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mithilfe von NTP mit jedem anderen Knoten.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um den Status während der Installation und anderer Wartungsverfahren an den primären Admin Node zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Storage Nodes.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstattung, Auditierung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Nodes	NMS-Serviceberichte und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Nodes	Interner Datenverkehr des AMS Service.

Port	TCP oder UDP	Aus	Zu	Details
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Nodes	Interner Datenverkehr des Load Balancer.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Konfigurationsmanagement interner Datenverkehr.
1511	TCP	Alle Knoten	Speicherknoten	Interner Metadatenverkehr.
5353	UDP	Alle Knoten	Alle Knoten	Bietet den Multicast-DNS-Dienst (mDNS), der für vollständige Grid-IP-Änderungen und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
7001	TCP	Speicherknoten	Speicherknoten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, sonstige Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Knoten	Geräteknoten	Interner Datenverkehr im Zusammenhang mit dem Wartungsmodusverfahren.
9042	TCP	Speicherknoten	Speicherknoten	Cassandra Client-Port.
9999	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsverfahren, Kennzahlen und Netzwerkaktualisierungen.
10226	TCP	Speicherknoten	Primärer Admin-Knoten	Wird von StorageGRID Appliances für das Weiterleiten von AutoSupport-Paketen vom E-Series SANtricity System Manager an den primären Admin-Node verwendet.

Port	TCP oder UDP	Aus	Zu	Details
10342	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
18000	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr des Kontodienstes.
18001	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Storage-Nodes	Speicherknoten	Interner API-Datenverkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr der Plattform-Services.
18017	TCP	Admin-/Storage-Nodes	Speicherknoten	Interner Datenverkehr des Data Mover Dienstes für Cloud Storage Pools.
18019	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin-/Storage-Nodes	Speicherknoten	S3-bezogener interner Datenverkehr.
18086	TCP	Alle Knoten	Speicherknoten	Interner Datenverkehr im Zusammenhang mit dem LDR Service.
18200	TCP	Admin-/Storage-Nodes	Speicherknoten	Zusätzliche Statistiken zu Client-Anfragen.
19000	TCP	Admin-/Storage-Nodes	Speicherknoten mit ADC	Interner Datenverkehr des Keystone-Dienstes.

Verwandte Informationen

"${post_edited_translations.segment}"

Externe Kommunikation für StorageGRID

Clients müssen mit Grid-Knoten kommunizieren, um Inhalte zu erfassen und abzurufen. Die verwendeten Ports hängen von den gewählten Objektspeicherprotokollen ab. Diese Ports müssen für den Client erreichbar sein.

Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, ist Folgendes möglich:

- Verwenden Sie "Load Balancer Endpunkte", um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ports sollten beim Bereitstellen von Knoten neu zugeordnet werden. Load-Balancer-Endpunkte sollten jedoch nicht neu zugeordnet werden. Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten sind verfügbar:

> Die Unterstützung für Port-Remapping ist veraltet und wird in einer zukünftigen Version entfernt. Zum Entfernen umgeleiteter Ports siehe "Port-Remaps auf StorageGRID Appliances entfernen" oder "Port-Remaps auf Bare-Metal-Hosts entfernen".

- "Port-Remap-Schlüssel für StorageGRID auf Red Hat Enterprise Linux"
- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für das Appliance neu zuordnen"

Ports für externe Kommunikation

Die folgende Tabelle zeigt die Ports, die für den Datenverkehr in die Knoten verwendet werden.

> Diese Liste enthält keine Ports, die möglicherweise als "Load Balancer Endpunkte" konfiguriert sind.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service Laptop	Alle Knoten	Für Prozeduren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional kann Port 2022 anstelle von 22 verwendet werden. **Hinweis**: Dieser Port ist nur erforderlich, wenn der SSH-Zugriff für bestimmte Wartungsarbeiten aktiviert werden muss.
25	TCP	SMTP	Admin-Nodes	E-Mail Server	Wird für Benachrichtigungen und E-Mail-basierte AutoSupport verwendet. Die Standardporteinstellung von 25 kann auf der Seite „E-Mail-Server“ überschrieben werden.
53	TCP/ UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
67	UDP	DHCP	Alle Knoten	DHCP-Service	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient Dienst wird für statisch konfigurierte Grids nicht ausgeführt.
68	UDP	DHCP	DHCP-Service	Alle Knoten	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient Dienst wird nicht für Grids ausgeführt, die statische IP-Adressen verwenden.
80	TCP	HTTP	Browser	Admin-Nodes	Port 80 leitet für die Benutzeroberfläche des Admin Node auf Port 443 um.
80	TCP	HTTP	Browser	Appliances	Port 80 wird auf Port 8443 für den StorageGRID Appliance Installer umgeleitet.
80	TCP	HTTP	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTP verwenden. Mandanten können die Standard-HTTP-Port-Einstellung 80 beim Erstellen eines Endpunkts überschreiben.
80	TCP	HTTP	Speicherknoten	AWS	Cloud Storage Pools-Anfragen, die an AWS-Ziele gesendet werden, die HTTP verwenden. Grid-Administratoren können die standardmäßige HTTP-Port-Einstellung 80 beim Konfigurieren eines Cloud Storage Pools überschreiben.
123	UDP	NTP	Primäre NTP Knoten	Externes NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Knoten synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
161	TCP/ UDP	SNMP	SNMP Client	Alle Knoten	Wird für SNMP-Abfragen verwendet. Alle Knoten liefern grundlegende Informationen; Admin Nodes liefern zusätzlich Warnmeldungen. Standardmäßig wird bei entsprechender Konfiguration UDP-Port 161 verwendet. **Hinweis:** Dieser Port ist nur erforderlich und wird auf der Knotenfirewall nur geöffnet, wenn SNMP konfiguriert ist. Wenn die Verwendung von SNMP vorgesehen ist, können alternative Ports konfiguriert werden. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID sind bei Ihrem NetApp Account Representative erhältlich.
162	TCP/ UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps verwenden standardmäßig den UDP-Port 162. **Hinweis:** Dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn die Verwendung von SNMP vorgesehen ist, können alternative Ports konfiguriert werden. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID sind bei Ihrem NetApp Account Representative erhältlich.
389	TCP/ UDP	LDAP	Speicherknoten mit ADC	Active Directory/LDAP	Wird für die Verbindung mit einem Active Directory oder LDAP-Server für die Identitätsföderation verwendet.
443	TCP	HTTPS	Browser	Admin-Nodes	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen. **Hinweis**: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Firewall-Steuerung konfigurieren" zur Konfiguration privilegierter IP-Adressen.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
443	TCP	HTTPS	Admin-Nodes	Active Directory	Wird von Administratorknoten verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist.
443	TCP	HTTPS	Speicherknoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTPS verwenden. Mandanten können die Standardeinstellung für den HTTP-Port 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speicherknoten	AWS	Cloud Storage Pools-Anfragen, die an AWS-Ziele gesendet werden, die HTTPS verwenden. Grid-Administratoren können die standardmäßige HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud Storage Pools überschreiben.
5353	UDP	mDNS	Alle Knoten	Alle Knoten	Bietet den Multicast-DNS-Dienst (mDNS), der für vollständige Grid-IP-Änderungen und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
5696	TCP	KMIP	Appliance	KMS	Key Management Interoperability Protocol (KMIP) externer Datenverkehr von Appliances, die für die Knotenverschlüsselung konfiguriert sind, zum Key Management Server (KMS), es sei denn, auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer ist ein anderer Port angegeben.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
8443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann zur Trennung der Grid Manager und Tenant Manager Kommunikation verwendet werden. **Hinweis**: Wenn die Grid Manager-Ports 443 oder 8443 geschlossen werden, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Firewall-Steuerung konfigurieren" zur Konfiguration privilegierter IP-Adressen.
8443	TCP	HTTPS	Browser	Appliances	Wird von Webbrowsern und Management-API-Clients verwendet, um auf den StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 wird auf Port 8443 für den StorageGRID Appliance Installer umgeleitet.
9022	TCP	SSH	Service Laptop	Appliances	Gewährt Zugriff auf StorageGRID Appliances im Vorkonfigurationsmodus für Support- und Fehlerbehebung. Dieser Port muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
9091	TCP	HTTPS	Externer Grafana Dienst	Admin-Nodes	Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.
9092	TCP	Kafka	Speicherknoten mit ADC	Kafka Cluster	Wird für Plattformdienstnachrichten verwendet, die an einen Kafka-Cluster gesendet werden. Mandanten können die Standardeinstellung für den Kafka-Port 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Grid Manager und Tenant Manager Kommunikation zu trennen.

Port	TCP oder UDP	Protokoll	Aus	Zu	Details
18082	TCP	HTTPS	S3 Clients	Speicherknoten	S3-Client-Datenverkehr direkt zu Storage Nodes (HTTPS).
18084	TCP	HTTP	S3 Clients	Speicherknoten	S3-Client-Datenverkehr direkt zu Speicherknoten (HTTP).
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die gridübergreifende Replikation	Admin Nodes und Gateway Nodes im Ziel-Grid für die gridübergreifende Replikation	Dieser Portbereich ist für Grid-Federation-Verbindungen reserviert. Beide Grids einer Verbindung nutzen denselben Port.