Netzwerkrichtlinien

StorageGRID software

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-119/network/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Netzwerkrichtlinien

Netzwerkrichtlinien

Verwenden Sie diese Richtlinien, um mehr über die Architektur und Netzwerktopologien von StorageGRID zu erfahren und die Anforderungen für die Netzwerkkonfiguration und -bereitstellung kennenzulernen.

Zu dieser Anleitung

Diese Richtlinien enthalten Informationen, die Sie zum Erstellen der StorageGRID Netzwerkinfrastruktur verwenden können, bevor Sie StorageGRID -Knoten bereitstellen und konfigurieren. Verwenden Sie diese Richtlinien, um sicherzustellen, dass die Kommunikation zwischen allen Knoten im Grid und zwischen dem Grid und externen Clients und Diensten stattfinden kann.

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

- Speichern und Abrufen von Objektdaten
- Erhalten Sie E-Mail-Benachrichtigungen
- Greifen Sie auf die StorageGRID -Verwaltungsschnittstelle (Grid Manager und Tenant Manager) zu.
- Zugriff auf die Audit-Freigabe (optional)
- Bieten Sie Dienstleistungen an wie:
  - Netzwerkzeitprotokoll (NTP)
  - Domänennamensystem (DNS)
  - Schlüsselverwaltungsserver (KMS)

Das StorageGRID -Netzwerk muss entsprechend konfiguriert werden, um den Datenverkehr für diese und weitere Funktionen zu bewältigen.

Bevor Sie beginnen

Die Netzwerkkonfiguration für ein StorageGRID -System erfordert ein hohes Maß an Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerkrouting und Firewalls.

Machen Sie sich vor der Netzwerkkonfiguration mit der StorageGRID -Architektur vertraut, wie in"Erfahren Sie mehr über StorageGRID" .

Nachdem Sie festgelegt haben, welche StorageGRID -Netzwerke Sie verwenden möchten und wie diese Netzwerke konfiguriert werden, können Sie die StorageGRID -Knoten installieren und konfigurieren, indem Sie den entsprechenden Anweisungen folgen.

Installieren von Appliance-Knoten

- "Installieren der Appliance-Hardware"

Installieren Sie softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

- "Installieren Sie StorageGRID auf VMware"

Konfigurieren und Verwalten der StorageGRID -Software

- "StorageGRID verwalten"
- "Versionshinweise"

StorageGRID -Netzwerktypen

Die Grid-Knoten in einem StorageGRID -System verarbeiten *Grid-Verkehr*, *Admin-Verkehr* und *Client-Verkehr*. Sie müssen das Netzwerk entsprechend konfigurieren, um diese drei Arten von Datenverkehr zu verwalten und Kontrolle und Sicherheit zu gewährleisten.

Verkehrsarten

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

Sie können das Netzwerk auf folgende Arten konfigurieren:

- Nur Grid-Netzwerk
- Grid- und Admin-Netzwerke
- Grid- und Client-Netzwerke
- Grid-, Admin- und Client-Netzwerke

Das Grid-Netzwerk ist obligatorisch und kann den gesamten Grid-Verkehr verwalten. Die Admin- und Client-Netzwerke können zum Zeitpunkt der Installation einbezogen oder später hinzugefügt werden, um sich an geänderte Anforderungen anzupassen. Obwohl das Admin-Netzwerk und das Client-Netzwerk optional sind, kann das Grid-Netzwerk isoliert und sicher gemacht werden, wenn Sie diese Netzwerke zur Abwicklung des Verwaltungs- und Client-Verkehrs verwenden.

Interne Ports sind nur über das Grid-Netzwerk zugänglich. Externe Ports sind von allen Netzwerktypen aus zugänglich. Diese Flexibilität bietet mehrere Optionen für die Gestaltung einer StorageGRID -Bereitstellung und die Einrichtung externer IP- und Portfilter in Switches und Firewalls. Sehen"interne Grid-Knoten-Kommunikation" Und"Externe Kommunikation" .

Netzwerkschnittstellen

StorageGRID -Knoten sind über die folgenden spezifischen Schnittstellen mit jedem Netzwerk verbunden:

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

Einzelheiten zum Zuordnen virtueller oder physischer Ports zu Knotennetzwerkschnittstellen finden Sie in den Installationsanweisungen:

Softwarebasierte Knoten

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"
- "Installieren Sie StorageGRID auf VMware"

Appliance-Knoten

- "SG6160 Speichergerät"
- "SGF6112 Speichergerät"
- "SG6000-Speichergerät"
- "SG5800 Speichergerät"
- "SG5700 Speichergerät"
- "SG110 und SG1100 Servicegeräte"
- "SG100 und SG1000 Servicegeräte"

Netzwerkinformationen für jeden Knoten

Sie müssen für jedes Netzwerk, das Sie auf einem Knoten aktivieren, Folgendes 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 Sie kein Gateway für ein Netzwerk konfigurieren möchten, sollten Sie die IP-Adresse als Gateway-Adresse verwenden.

Hochverfügbarkeitsgruppen

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

Netznetzwerk

Das Grid-Netzwerk ist erforderlich. Es wird für den gesamten internen StorageGRID Verkehr verwendet. Das Grid-Netzwerk bietet Konnektivität zwischen allen Knoten im Grid, über alle Standorte und Subnetze hinweg. Alle Knoten im Grid-Netzwerk müssen mit allen anderen Knoten kommunizieren können. Das Grid-Netzwerk kann aus mehreren Subnetzen bestehen. Netzwerke, die kritische Grid-Dienste wie NTP enthalten, können auch als Grid-Subnetze hinzugefügt werden.

StorageGRID unterstützt keine Netzwerkadressübersetzung (NAT) zwischen Knoten.

Das Grid-Netzwerk kann für den gesamten Admin-Verkehr und den gesamten Client-Verkehr verwendet werden, auch wenn das Admin-Netzwerk und das Client-Netzwerk konfiguriert sind. Das Grid-Netzwerk-Gateway ist das Standard-Gateway des Knotens, sofern für den Knoten nicht das Client-Netzwerk konfiguriert ist.

Beim Konfigurieren des Grid-Netzwerks müssen Sie sicherstellen, dass das Netzwerk vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt ist.

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

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

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Nach der Konfiguration kann es für den Systemadministrations- und Wartungsverkehr verwendet werden. Das Admin-Netzwerk ist normalerweise ein privates Netzwerk und muss nicht zwischen Knoten geroutet werden können.

Sie können auswählen, für welche Grid-Knoten das Admin-Netzwerk aktiviert werden soll.

Wenn Sie das Admin-Netzwerk verwenden, muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk laufen. Typische Verwendungszwecke des Admin-Netzwerks sind unter anderem:

- 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 Prüfprotokolle auf Admin-Knoten.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support.

Das Admin-Netzwerk wird niemals für internen Grid-Verkehr verwendet. Es wird ein Admin-Netzwerk-Gateway bereitgestellt, das dem Admin-Netzwerk die Kommunikation mit mehreren externen Subnetzen ermöglicht. Das Admin-Netzwerk-Gateway wird jedoch nie als Standard-Gateway des Knotens verwendet.

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

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

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn es konfiguriert ist, wird es verwendet, um Clientanwendungen wie S3 Zugriff auf Grid-Dienste zu gewähren. Wenn Sie StorageGRID Daten einer externen Ressource zugänglich machen möchten (z. B. einem Cloud Storage Pool oder dem StorageGRID CloudMirror-Replikationsdienst), kann die externe Ressource auch das Client-Netzwerk verwenden. Grid-Knoten können mit jedem Subnetz kommunizieren, das über das Client-Netzwerk-Gateway erreichbar ist.

Sie können auswählen, auf welchen Grid-Knoten das Client-Netzwerk aktiviert werden soll. Es müssen sich nicht alle Knoten im selben Client-Netzwerk befinden und die Knoten kommunizieren niemals über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst betriebsbereit, wenn die Grid-Installation abgeschlossen ist.

Zur Erhöhung der Sicherheit können Sie festlegen, dass die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, sodass das Client-Netzwerk hinsichtlich der zulässigen Verbindungen restriktiver ist. Wenn die Client-Netzwerkschnittstelle eines Knotens nicht vertrauenswürdig ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie beispielsweise von der CloudMirror-Replikation verwendet werden, akzeptiert jedoch nur eingehende Verbindungen auf Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert wurden. Sehen"Verwalten von Firewall-Steuerelementen" Und"Konfigurieren von Load Balancer-Endpunkten" .

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Verkehr nicht über das Grid-Netzwerk laufen. Der Grid-Netzwerkverkehr kann auf ein sicheres, nicht routingfähiges Netzwerk aufgeteilt werden. Die folgenden Knotentypen werden häufig mit einem Client-Netzwerk konfiguriert:

- Gateway-Knoten, da diese Knoten Zugriff auf den StorageGRID Load Balancer-Dienst und S3-Client-Zugriff auf das Grid bieten.
- Speicherknoten, da diese Knoten Zugriff auf das S3-Protokoll sowie auf Cloud-Speicherpools und den CloudMirror-Replikationsdienst bieten.
- Admin-Knoten, um sicherzustellen, dass Mandantenbenutzer eine Verbindung zum Mandantenmanager herstellen können, ohne das Admin-Netzwerk verwenden zu müssen.

Beachten Sie Folgendes für das Client-Netzwerk-Gateway:

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

Optionale VLAN-Netzwerke

Bei Bedarf können Sie optional virtuelle LAN-Netzwerke (VLAN) für den Client-Verkehr und für einige Arten von Admin-Verkehr verwenden. Grid-Verkehr kann jedoch keine VLAN-Schnittstelle verwenden. Der interne StorageGRID Verkehr zwischen Knoten muss immer das Grid-Netzwerk auf eth0 verwenden.

Um die Verwendung von VLANs zu unterstützen, müssen Sie eine oder mehrere Schnittstellen auf einem Knoten als Trunk-Schnittstellen am Switch konfigurieren. Sie können die Grid-Netzwerkschnittstelle (eth0) oder die Client-Netzwerkschnittstelle (eth2) als Trunk konfigurieren oder dem Knoten Trunk-Schnittstellen hinzufügen.

Wenn eth0 als Trunk konfiguriert ist, fließt der Grid-Netzwerkverkehr über die native Trunk-Schnittstelle, wie auf dem Switch konfiguriert. Wenn eth2 als Trunk konfiguriert ist und das Client-Netzwerk ebenfalls auf demselben Knoten konfiguriert ist, verwendet das Client-Netzwerk das native VLAN des Trunk-Ports, wie es auf dem Switch konfiguriert ist.

Über VLAN-Netzwerke wird nur eingehender Administratorverkehr unterstützt, wie er beispielsweise für SSH-, Grid Manager- oder Tenant Manager-Verkehr verwendet wird. Ausgehender Datenverkehr, wie er beispielsweise für NTP, DNS, LDAP, KMS und Cloud Storage Pools verwendet wird, wird über VLAN-Netzwerke nicht unterstützt.

> VLAN-Schnittstellen können nur zu Admin-Knoten und Gateway-Knoten hinzugefügt werden. Sie können keine VLAN-Schnittstelle für den Client- oder Administratorzugriff auf Speicherknoten verwenden.

Sehen"Konfigurieren von VLAN-Schnittstellen" für Anweisungen und Richtlinien.

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

Beispiele für Netzwerktopologien

Grid-Netzwerktopologie

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

Wenn Sie das Grid-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Knoten fest.

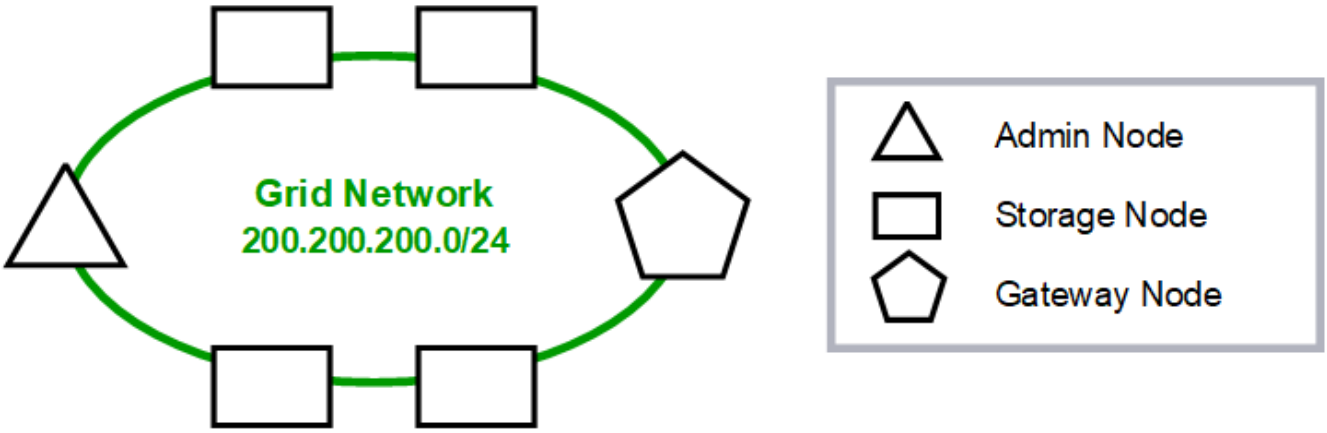
Während der Konfiguration müssen Sie alle Grid Network-Subnetze zur Grid Network Subnet List (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Sites und kann auch externe Subnetze enthalten, die Zugriff auf kritische Dienste wie NTP, DNS oder LDAP bieten.

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

In diesem Beispiel wird der gesamte Datenverkehr über dasselbe Netzwerk abgewickelt, einschließlich des Datenverkehrs im Zusammenhang mit S3-Clientanforderungen sowie Verwaltungs- und Wartungsfunktionen.

> Diese Topologie eignet sich für Einzelstandortbereitstellungen, die nicht extern verfügbar sind, für Proof-of-Concept- oder Testbereitstellungen oder wenn ein Lastenausgleich eines Drittanbieters als Clientzugriffsgrenze fungiert. Wenn möglich, sollte das Grid-Netzwerk ausschließlich für den internen Verkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk unterliegen zusätzlichen Firewall-Einschränkungen, die den externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Verkehr wird unterstützt, diese Verwendung 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

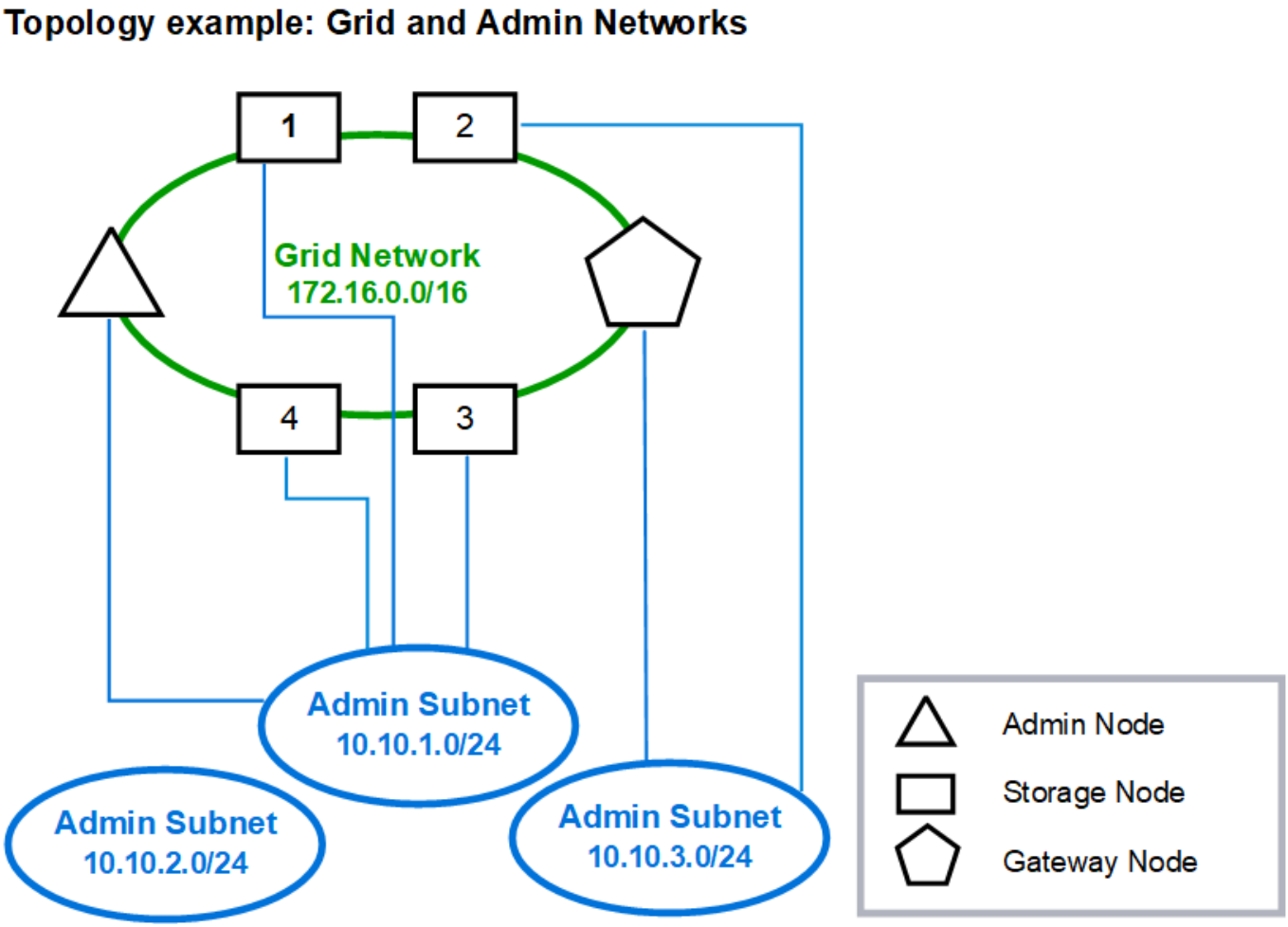
Admin-Netzwerktopologie

Ein Admin-Netzwerk ist optional. Eine Möglichkeit, ein Admin-Netzwerk und ein Grid-Netzwerk zu verwenden, besteht darin, für jeden Knoten ein routingfähiges Grid-Netzwerk und ein begrenztes Admin-Netzwerk zu konfigurieren.

Wenn Sie das Admin-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth1-Schnittstelle für jeden Grid-Knoten fest.

Das Admin-Netzwerk kann für jeden Knoten eindeutig sein und aus mehreren Subnetzen bestehen. Jeder Knoten kann mit einer Admin External Subnet List (AESL) konfiguriert werden. Die AESL listet die über das Admin-Netzwerk erreichbaren Subnetze für jeden Knoten auf. Die AESL muss auch die Subnetze aller Dienste enthalten, auf die das Grid über das Admin-Netzwerk zugreift, z. B. NTP, DNS, KMS und LDAP. Für jedes Subnetz in der AESL werden statische Routen angewendet.

In diesem Beispiel wird das Grid-Netzwerk für den Datenverkehr im Zusammenhang mit S3-Clientanforderungen und Objektverwaltung verwendet, während das Admin-Netzwerk für Verwaltungsfunktionen verwendet 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

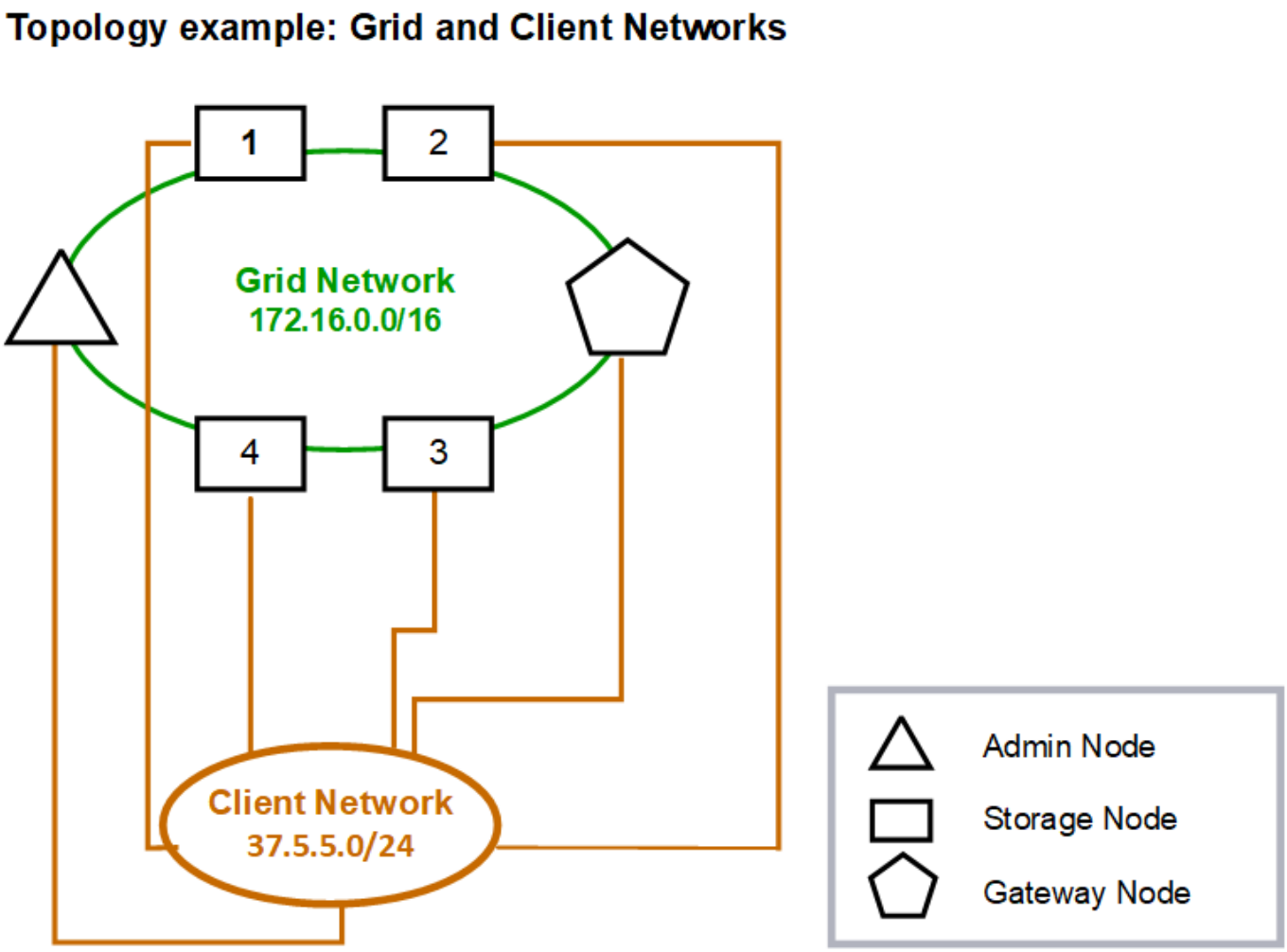
Ein Client-Netzwerk ist optional. Durch die Verwendung eines Client-Netzwerks kann der Client-Netzwerkverkehr (z. B. S3) vom internen Grid-Verkehr getrennt werden, wodurch die Grid-Vernetzung sicherer wird. Der Verwaltungsverkehr kann entweder vom Client- oder vom Grid-Netzwerk abgewickelt werden, wenn das Admin-Netzwerk nicht konfiguriert ist.

Wenn Sie das Client-Netzwerk konfigurieren, legen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle für den konfigurierten Knoten fest. Das Client-Netzwerk jedes Knotens kann unabhängig vom Client-Netzwerk auf jedem anderen Knoten sein.

Wenn Sie während der Installation ein Client-Netzwerk für einen Knoten konfigurieren, wechselt das Standard-Gateway des Knotens nach Abschluss der Installation vom Grid-Netzwerk-Gateway zum Client-Netzwerk-Gateway. Wenn später ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway des Knotens auf die gleiche Weise.

In diesem Beispiel wird das Client-Netzwerk für S3-Client-Anfragen und für Verwaltungsfunktionen verwendet,

während das Grid-Netzwerk für interne Objektverwaltungsvorgänge 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

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

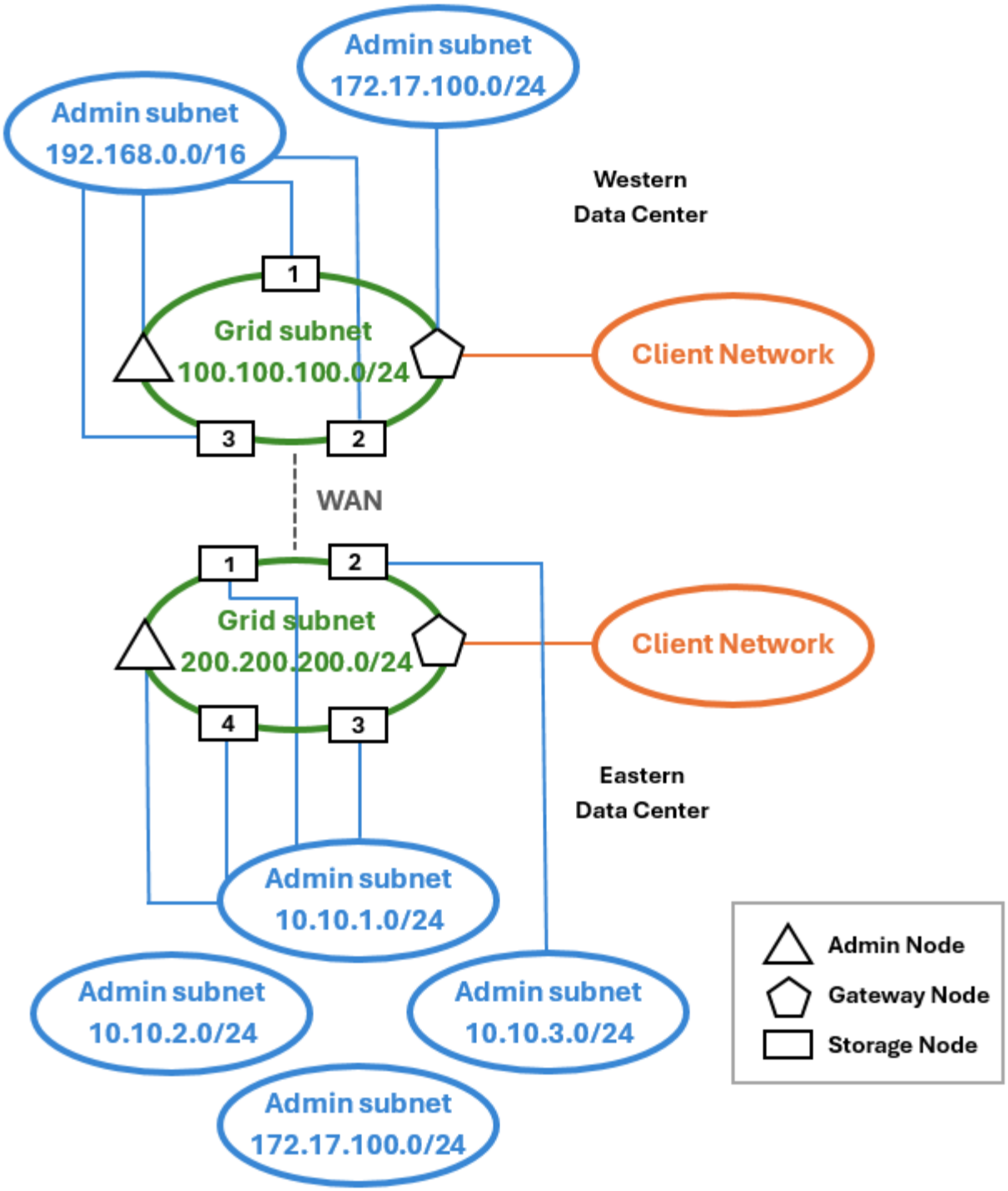
Topologie für alle drei Netzwerke

Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, begrenzten standortspezifischen Admin-Netzwerken und offenen Client-Netzwerken besteht. Die Verwendung von Load Balancer-Endpunkten und nicht vertrauenswürdigen Client-Netzwerken kann bei Bedarf zusätzliche Sicherheit bieten.

In diesem Beispiel:

- Das Grid-Netzwerk wird für den Netzwerkverkehr im Zusammenhang mit internen Objektverwaltungsvorgängen verwendet.
- Das Admin-Netzwerk wird für den Datenverkehr im Zusammenhang mit Verwaltungsfunktionen verwendet.
- Das Client-Netzwerk wird für den Datenverkehr im Zusammenhang mit S3-Client-Anfragen verwendet.

Topologiebeispiel: Grid-, Admin- und Client-Netzwerke



Netzwerkanforderungen

Sie müssen 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, normalerweise 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 aus erreichbar sein.
- **DNS-Serververbindungen**: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory-Serververbindungen**: Ausgehende TCP-Verbindung vom Identitätsdienst auf Speicherknoten.
- * AutoSupport*: Ausgehende TCP-Verbindung von den Admin-Knoten zu entweder `support.netapp.com` oder ein vom Kunden konfigurierter 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.

Wenn StorageGRID mithilfe der Standardroutingregeln keinen der bereitgestellten NTP- oder DNS-Server kontaktieren kann, versucht es automatisch, in allen Netzwerken (Grid, Admin und Client) Kontakt aufzunehmen, sofern die IP-Adressen der DNS- und NTP-Server angegeben sind. Wenn die NTP- oder DNS-Server in einem beliebigen Netzwerk erreichbar sind, erstellt StorageGRID automatisch zusätzliche Routing-Regeln, um sicherzustellen, dass dieses Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.

Obwohl Sie diese automatisch erkannten Hostrouten verwenden können, sollten Sie die DNS- und NTP-Routen im Allgemeinen manuell konfigurieren, um die Konnektivität sicherzustellen, falls die automatische Erkennung fehlschlägt.

Wenn Sie während der Bereitstellung noch nicht bereit sind, die optionalen Admin- und Client-Netzwerke zu konfigurieren, können Sie diese Netzwerke konfigurieren, wenn Sie während der Konfigurationsschritte Grid-Knoten genehmigen. Darüber hinaus können Sie diese Netzwerke nach der Installation mit dem Tool „IP ändern“ konfigurieren (siehe"Konfigurieren von IP-Adressen").

Über VLAN-Schnittstellen werden nur S3-Clientverbindungen und SSH-, Grid Manager- und Tenant Manager-Verwaltungsverbindungen unterstützt. Ausgehende Verbindungen, beispielsweise 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.

Wide Area Networks (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/Sekunde in jede Richtung aufweisen, bevor der Client-Verkehr berücksichtigt wird. Für die Datenreplikation oder Erasure Coding zwischen Standorten, die Erweiterung von Knoten oder Standorten, die Wiederherstellung von Knoten und andere Vorgänge oder Konfigurationen ist zusätzliche Bandbreite erforderlich.

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

Schutzschema ab. Wenn Sie Hilfe bei der Schätzung der Mindestanforderungen für die WAN-Bandbreite benötigen, wenden Sie sich an Ihren NetApp Professional Services-Berater.

Verbindungen für Admin-Knoten und Gateway-Knoten

Admin-Knoten müssen immer vor nicht vertrauenswürdigen Clients, wie beispielsweise denen im offenen Internet, geschützt werden. Sie müssen sicherstellen, dass kein nicht vertrauenswürdiger Client auf einen Admin-Knoten im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk zugreifen kann.

Admin-Knoten und Gateway-Knoten, die Sie zu Hochverfügbarkeitsgruppen hinzufügen möchten, müssen mit einer statischen IP-Adresse konfiguriert werden. Weitere Informationen finden Sie unter "Verwalten von Hochverfügbarkeitsgruppen" .

Verwenden der Netzwerkadressübersetzung (NAT)

Verwenden Sie keine Netzwerkadressübersetzung (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID Sites. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt geroutet werden können. Bei Bedarf können Sie jedoch NAT zwischen externen Clients und Grid-Knoten verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway-Knoten bereitzustellen. Die Verwendung von NAT zum Überbrücken eines öffentlichen Netzwerksegments wird nur unterstützt, wenn Sie eine Tunnelanwendung verwenden, die für alle Knoten im Grid transparent ist, d. h. die Grid-Knoten benötigen keine Kenntnis der öffentlichen IP-Adressen.

Netzwerkspezifische Anforderungen

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und Router

- Wenn festgelegt, muss sich das Gateway für ein bestimmtes Netzwerk innerhalb des Subnetzes des jeweiligen Netzwerks befinden.
- Wenn Sie eine Schnittstelle mit statischer Adressierung konfigurieren, müssen Sie eine andere Gateway-Adresse als 0.0.0.0 angeben.
- Wenn Sie kein Gateway haben, empfiehlt es sich, die Gateway-Adresse auf die IP-Adresse der Netzwerkschnittstelle festzulegen.

Subnetze

> Jedes Netzwerk muss mit seinem eigenen Subnetz verbunden sein, das sich nicht mit anderen Netzwerken auf dem Knoten überschneidet.

Die folgenden Einschränkungen werden vom Grid Manager während der Bereitstellung erzwungen. Sie werden hier bereitgestellt, um bei der Netzwerkplanung vor der Bereitstellung zu helfen.

- Die Subnetzmaske für eine Netzwerk-IP-Adresse kann nicht 255.255.255.254 oder 255.255.255.255 (/31 oder /32 in der CIDR-Notation) sein.
- Das durch die IP-Adresse und Subnetzmaske (CIDR) einer Netzwerkschnittstelle definierte Subnetz darf sich nicht mit dem Subnetz einer anderen auf demselben Knoten konfigurierten Schnittstelle überschneiden.
- Verwenden Sie keine Subnetze, die die folgenden IPv4-Adressen für das Grid-Netzwerk, das Admin-

Netzwerk oder das Client-Netzwerk eines Knotens enthalten:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

  Verwenden Sie beispielsweise nicht die folgenden Subnetzbereiche für das Grid-Netzwerk, das Admin-Netzwerk oder das Client-Netzwerk eines Knotens:

- 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-Netzwerk-Subnetz für jeden Knoten muss in der GNSL enthalten sein.
- Das Admin-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Client-Netzwerk-Subnetz oder einem anderen Subnetz in der GNSL überschneiden.
- Die Subnetze in der AESL dürfen sich nicht mit Subnetzen in der GNSL überschneiden.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Grid-Netzwerk-Subnetz, dem Admin-Netzwerk-Subnetz, einem anderen Subnetz in der GNSL oder einem anderen Subnetz in der AESL überschneiden.

Netznetzwerk

- Zum Zeitpunkt der Bereitstellung muss jeder Grid-Knoten an das Grid-Netzwerk angeschlossen sein und über die Netzwerkkonfiguration, die Sie bei der Bereitstellung des Knotens angeben, mit dem primären Admin-Knoten kommunizieren können.
- Während des normalen Netzbetriebs muss jeder Netzknoten in der Lage sein, über das Netznetzwerk mit allen anderen Netzknoten zu kommunizieren.

> Das Grid-Netzwerk muss zwischen den einzelnen Knoten direkt routebar sein. Die Netzwerkadressübersetzung (NAT) zwischen Knoten wird nicht unterstützt.

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, fügen Sie diese der Grid-Netzwerk-Subnetzliste (GNSL) hinzu. Für jedes Subnetz im GNSL werden auf allen Knoten statische Routen erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das native Trunk-VLAN das für den Grid-Netzwerkverkehr verwendete VLAN sein. Alle Grid-Knoten müssen über das native Trunk-VLAN zugänglich sein.

Admin-Netzwerk

Das Admin-Netzwerk ist optional. Wenn Sie ein Admin-Netzwerk konfigurieren möchten, befolgen Sie diese Anforderungen und Richtlinien.

Zu den typischen Verwendungszwecken des Admin-Netzwerks gehören Verwaltungsverbindungen, AutoSupport, KMS und Verbindungen zu kritischen Servern wie NTP, DNS und LDAP, wenn diese

Verbindungen nicht über das Grid-Netzwerk oder das Client-Netzwerk bereitgestellt werden.

> Das Admin-Netzwerk und die AESL können für jeden Knoten eindeutig sein, solange die gewünschten Netzwerkdienste und Clients erreichbar sind.

> Sie müssen mindestens ein Subnetz im Admin-Netzwerk definieren, um eingehende Verbindungen von externen Subnetzen zu ermöglichen. Auf jedem Knoten werden für jedes Subnetz in der AESL automatisch statische Routen generiert.

Kundennetzwerk

Das Client-Netzwerk ist optional. Wenn Sie die Konfiguration eines Client-Netzwerks planen, beachten Sie die folgenden Überlegungen.

- Das Client-Netzwerk ist für die Unterstützung des Datenverkehrs von S3-Clients ausgelegt. Wenn konfiguriert, wird das Client-Netzwerk-Gateway zum Standard-Gateway des Knotens.
- Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur an explizit konfigurierten Load Balancer-Endpunkten akzeptieren. Sehen "Konfigurieren von Load Balancer-Endpunkten" .
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, überlegen Sie, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn dies konfiguriert ist, fließt der Client-Netzwerkverkehr über das native Trunk-VLAN, wie im Switch konfiguriert.

Ähnliche Informationen

"Knotennetzwerkkonfiguration ändern"

Bereitstellungsspezifische Netzwerküberlegungen

Linux-Bereitstellungen

Aus Gründen der Effizienz, Zuverlässigkeit und Sicherheit läuft das StorageGRID -System unter Linux als Sammlung von Container-Engines. Eine Container-Engine-bezogene Netzwerkkonfiguration ist in einem StorageGRID System nicht erforderlich.

Verwenden Sie für die Container-Netzwerkschnittstelle ein nicht gebundenes Gerät, z. B. ein VLAN oder ein virtuelles Ethernet-Paar (veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Knotenkonfigurationsdatei an.

> Verwenden Sie Bond- oder Bridge-Geräte nicht direkt als Container-Netzwerkschnittstelle. Dies könnte den Start des Knotens aufgrund eines Kernelproblems bei der Verwendung von Macvlan mit Bond- und Bridge-Geräten im Container-Namespace verhindern.

Siehe die Installationsanweisungen für"Red Hat Enterprise Linux" oder"Ubuntu oder Debian" Bereitstellungen.

Host-Netzwerkkonfiguration für Container-Engine-Bereitstellungen

Bevor Sie mit der StorageGRID -Bereitstellung auf einer Container-Engine-Plattform beginnen, legen Sie fest, welche Netzwerke (Grid, Admin, Client) jeder Knoten verwenden wird. Sie müssen sicherstellen, dass die Netzwerkschnittstelle jedes Knotens auf der richtigen virtuellen oder physischen Hostschnittstelle konfiguriert ist und dass jedes Netzwerk über ausreichend Bandbreite verfügt.

Physische Hosts

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

- Stellen Sie sicher, dass alle Hosts für jede Knotenschnittstelle dieselbe Hostschnittstelle verwenden. Diese Strategie vereinfacht die Hostkonfiguration und ermöglicht eine zukünftige Knotenmigration.
- Besorgen Sie sich eine IP-Adresse für den physischen Host selbst.

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

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie VLAN-Schnittstellen in StorageGRID verwenden möchten, muss der Host über eine oder mehrere Trunk-Schnittstellen verfügen, die Zugriff auf die gewünschten VLANs bieten. Diese Schnittstellen können als eth0, eth2 oder als zusätzliche Schnittstellen an den Knotencontainer übergeben werden. Informationen zum Hinzufügen von Trunk- oder Zugriffsschnittstellen finden Sie im Folgenden:
  - **RHEL (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **RHEL, Ubuntu oder Debian (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

Empfehlungen zur Mindestbandbreite

Die folgende Tabelle enthält Empfehlungen zur minimalen LAN-Bandbreite für jeden StorageGRID Knotentyp und jeden Netzwerktyp. Sie müssen jedem physischen oder virtuellen Host eine ausreichende Netzwerkbandbreite bereitstellen, um die aggregierten Mindestbandbreitenanforderungen für die Gesamtzahl und den Typ der StorageGRID Knoten zu erfüllen, die Sie auf diesem Host ausführen möchten.

Knotentyp	**Netzwerktyp**		
	Netz	Administrator	Kunde
	Mindest-LAN-Bandbreite	Administrator	10 Gbit/s
1 Gbit/s	1 Gbit/s	Tor	10 Gbit/s
1 Gbit/s	10 Gbit/s	Storage	10 Gbit/s
1 Gbit/s	10 Gbit/s	Archiv	10 Gbit/s

> Diese Tabelle enthält nicht die SAN-Bandbreite, die für den Zugriff auf gemeinsam genutzten Speicher erforderlich ist. Wenn Sie gemeinsam genutzten Speicher verwenden, auf den über Ethernet (iSCSI oder FCoE) zugegriffen wird, sollten Sie auf jedem Host separate physische Schnittstellen bereitstellen, um ausreichend SAN-Bandbreite bereitzustellen. Um Engpässe zu vermeiden, sollte die SAN-Bandbreite für einen bestimmten Host in etwa der aggregierten Netzwerkbandbreite aller auf diesem Host ausgeführten Speicherknoten entsprechen.

Verwenden Sie die Tabelle, um die Mindestanzahl der auf jedem Host bereitzustellenden Netzwerkschnittstellen zu bestimmen, basierend auf der Anzahl und dem Typ der StorageGRID -Knoten, die Sie auf diesem Host ausführen möchten.

So führen Sie beispielsweise einen Admin-Knoten, einen Gateway-Knoten und einen Speicherknoten auf einem einzelnen Host aus:

- Verbinden Sie das Grid und die Admin-Netzwerke auf dem Admin-Knoten (erfordert 10 + 1 = 11 Gbit/s)
- Verbinden Sie das Grid und die Client-Netzwerke mit dem Gateway-Knoten (erfordert 10 + 10 = 20 Gbit/s)
- Verbinden Sie das Grid-Netzwerk mit dem Speicherknoten (erfordert 10 Gbit/s)

In diesem Szenario sollten Sie mindestens 11 + 20 + 10 = 41 Gbit/s Netzwerkbandbreite bereitstellen. Diese kann durch zwei 40-Gbit/s-Schnittstellen oder fünf 10-Gbit/s-Schnittstellen erreicht werden, die möglicherweise zu Trunks zusammengefasst und dann von den drei oder mehr VLANs gemeinsam genutzt werden, die die Grid-, Admin- und Client-Subnetze lokal zum physischen Rechenzentrum mit dem Host übertragen.

Einige empfohlene Methoden zum Konfigurieren physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung Ihrer StorageGRID Bereitstellung finden Sie im Folgenden:

- "Konfigurieren des Hostnetzwerks (Red Hat Enterprise Linux)"
- "Konfigurieren Sie das Hostnetzwerk (Ubuntu oder Debian)."

Vernetzung und Ports für Plattformdienste und Cloud-Speicherpools

Wenn Sie StorageGRID -Plattformdienste oder Cloud Storage Pools verwenden möchten, müssen Sie Grid-Netzwerke und Firewalls konfigurieren, um sicherzustellen, dass die Zielendpunkte erreicht werden können.

Vernetzung für Plattformdienste

Wie beschrieben in"Plattformdienste für Mandanten verwalten" Und"Plattformdienste verwalten" Zu den Plattformdiensten gehören externe Dienste, die Suchintegration, Ereignisbenachrichtigung und CloudMirror-Replikation bereitstellen.

Plattformdienste erfordern Zugriff von Speicherknoten, die den StorageGRID ADC-Dienst hosten, auf die externen Dienstendpunkte. Beispiele für die Bereitstellung des Zugriffs sind:

- Konfigurieren Sie auf den Speicherknoten mit ADC-Diensten eindeutige Admin-Netzwerke mit AESL-Einträgen, die zu den Zielendpunkten weiterleiten.
- Verlassen Sie sich auf die Standardroute, die von einem Client-Netzwerk bereitgestellt wird. Wenn Sie die Standardroute verwenden, können Sie die"nicht vertrauenswürdige Client-Netzwerkfunktion" um eingehende Verbindungen einzuschränken.

Vernetzung für Cloud-Speicherpools

Cloud-Speicherpools erfordern außerdem Zugriff von Speicherknoten auf die Endpunkte, die vom verwendeten externen Dienst bereitgestellt werden, z. B. Amazon S3 Glacier oder Microsoft Azure Blob Storage. Weitere Informationen finden Sie unter"Was ist ein Cloud-Speicherpool?" .

Ports für Plattformdienste und Cloud Storage Pools

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

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

Beim Erstellen oder Bearbeiten des Endpunkts kann ein anderer Port angegeben werden. Sehen "Netzwerkportreferenz" .

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren der Speicherproxyeinstellungen" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

VLANs und Plattformdienste und Cloud-Speicherpools

Sie können keine VLAN-Netzwerke für Plattformdienste oder Cloud-Speicherpools verwenden. Die Zielendpunkte müssen über das Grid-, Admin- oder Client-Netzwerk erreichbar sein.

Appliance-Knoten

Sie können die Netzwerkports auf StorageGRID -Geräten so konfigurieren, dass sie die Port-Bond-Modi verwenden, die Ihren Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

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

Die 1-GbE-Admin-Netzwerkports können für Verbindungen zum Admin-Netzwerk im unabhängigen oder aktiven Backup-Modus konfiguriert werden.

Informieren Sie sich über die Port-Bond-Modi für Ihr Gerät:

- "Port-Bond-Modi (SG6160)"
- "Port-Bond-Modi (SGF6112)"
- "Port-Bond-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

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

Erstmalige Bereitstellung eines Knotens

Wenn Sie einen Knoten zum ersten Mal bereitstellen, müssen Sie den Knoten an das Grid-Netzwerk anschließen und sicherstellen, dass er Zugriff auf den primären Admin-Knoten hat. Wenn das Grid-Netzwerk isoliert ist, können Sie das Admin-Netzwerk auf dem primären Admin-Knoten für den Konfigurations- und Installationszugriff von außerhalb des Grid-Netzwerks konfigurieren.

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

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

Automatische Knotenregistrierung mit primärem Admin-Knoten

Nachdem die Knoten bereitgestellt wurden, registrieren sie sich über das Grid-Netzwerk beim primären Admin-Knoten. Anschließend können Sie den Grid Manager, den `configure-storagegrid.py` Python-Skript oder die Installations-API zum Konfigurieren des Rasters und Genehmigen der registrierten Knoten. Während der Grid-Konfiguration können Sie mehrere Grid-Subnetze konfigurieren. Wenn Sie die Grid-Konfiguration abschließen, werden auf jedem Knoten statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway erstellt.

Deaktivieren des Admin-Netzwerks oder Client-Netzwerks

Wenn Sie das Admin-Netzwerk oder das Client-Netzwerk deaktivieren möchten, können Sie die Konfiguration während des Knotengenehmigungsprozesses entfernen oder nach Abschluss der Installation das Tool „IP ändern“ verwenden (siehe"Konfigurieren von IP-Adressen").

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Bereitstellung und Konfiguration des Grid-Knotens diese Richtlinien für DHCP-Adressierung und Netzwerkkonfigurationsänderungen.

- Wenn DHCP zum Zuweisen von IP-Adressen verwendet wurde, konfigurieren Sie eine DHCP-Reservierung für jede IP-Adresse in den verwendeten Netzwerken.

  Sie können DHCP nur während der Bereitstellungsphase einrichten. Sie können DHCP während der Konfiguration nicht einrichten.

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

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmasken und Standard-Gateways für einen Grid-Knoten ändern möchten. Sehen "Konfigurieren von IP-Adressen" .
- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, kann die Client-Konnektivität zum primären Admin-Knoten und anderen Grid-Knoten verloren gehen. Abhängig von den vorgenommenen Netzwerkänderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Netzwerkportreferenz

Interne Grid-Knoten-Kommunikation

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

NetApp empfiehlt, den ICMP-Verkehr (Internet Control Message Protocol) zwischen Grid-Knoten zu aktivieren. Das Zulassen von ICMP-Verkehr kann die Failover-Leistung verbessern, wenn ein Grid-Knoten nicht erreicht werden kann.

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 nur im Unicast-Modus. VRRP ist nur erforderlich, wenn"Hochverfügbarkeitsgruppen" konfiguriert sind.

Richtlinien für Linux-basierte Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports zum Zeitpunkt der Bereitstellung mithilfe eines Bereitstellungskonfigurationsparameters neu zuordnen. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter:

- "Installieren Sie StorageGRID unter Red Hat Enterprise Linux"
- "Installieren Sie StorageGRID unter Ubuntu oder Debian"

Richtlinien für VMware-basierte Knoten

Konfigurieren Sie die folgenden Ports nur, wenn Sie Firewall-Einschränkungen definieren müssen, die außerhalb des VMware-Netzwerks liegen.

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports neu zuordnen, wenn Sie Knoten mithilfe des VMware vSphere Web Client bereitstellen oder indem Sie bei der Automatisierung der Grid-Knotenbereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter"Installieren Sie StorageGRID auf VMware" .

Richtlinien für Appliance-Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Sehen "Optional: Netzwerkports für das Gerät neu zuordnen" .

Interne StorageGRID Ports

Hafen	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsverfahren muss der primäre Admin-Knoten in der Lage sein, über SSH auf Port 22 mit allen anderen Knoten zu kommunizieren. Das Zulassen von SSH-Verkehr von anderen Knoten ist optional.
80	TCP	Geräte	Primärer Admin-Knoten	Wird von StorageGRID -Geräten verwendet, um mit dem primären Admin-Knoten zu kommunizieren und die Installation zu starten.

Hafen	TCP oder UDP	Aus	Zu	Details
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mit jedem anderen Knoten über NTP.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um während der Installation und anderer Wartungsvorgänge den Status an den primären Admin-Knoten zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstellung, Prüfung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3- und Swift-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Knoten	NMS-Dienstberichterstattung und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Knoten	AMS-Service-interner Verkehr.
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Knoten	Interner Datenverkehr des Load Balancers.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr des Konfigurationsmanagements.
1511	TCP	Alle Knoten	Speicherknoten	Metadaten des internen Datenverkehrs.
5353	UDP	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.

Hafen	TCP oder UDP	Aus	Zu	Details
7001	TCP	Speicherknoten	Speicherknoten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
8443	TCP	Primärer Admin-Knoten	Appliance-Knoten	Interner Verkehr 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, Metriken und Netzwerkupdates.
10226	TCP	Speicherknoten	Primärer Admin-Knoten	Wird von StorageGRID -Geräten zum Weiterleiten von AutoSupport Paketen vom E-Series SANtricity System Manager an den primären Admin-Knoten verwendet.
10342	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
18000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr des Kontodienstes.
18001	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Speicherknoten	Speicherknoten	Interner API-Verkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Die Plattform bedient den internen Datenverkehr.

Hafen	TCP oder UDP	Aus	Zu	Details
18017	TCP	Admin-/Speicherknoten	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-/Speicherknoten	Speicherknoten	S3-bezogener interner Datenverkehr.
18083	TCP	Alle Knoten	Speicherknoten	Swift-bezogener interner Verkehr.
18086	TCP	Alle Knoten	Speicherknoten	Interner Verkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin-/Speicherknoten	Speicherknoten	Zusätzliche Statistiken zu Clientanfragen.
19000	TCP	Admin-/Speicherknoten	Speicherknoten mit ADC	Interner Verkehr des Keystone -Dienstes.

Ähnliche Informationen

"Externe Kommunikation"

Externe Kommunikation

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

Eingeschränkter Zugang zu Häfen

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, können Sie Folgendes tun:

- Verwenden"Load Balancer-Endpunkte" um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ordnen Sie die Ports beim Bereitstellen von Knoten neu zu. Sie sollten die Endpunkte des Lastenausgleichs jedoch nicht neu zuordnen. Sehen Sie sich die Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten an:
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Red Hat Enterprise Linux"
  - "Port-Neuzuordnungsschlüssel für StorageGRID unter Ubuntu oder Debian"

- "Ports für StorageGRID auf VMware neu zuordnen"
- "Optional: Netzwerkports für das Gerät neu zuordnen"

Für die externe Kommunikation verwendete Ports

Die folgende Tabelle zeigt die für den Datenverkehr in die Knoten verwendeten Ports.

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

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden.
25	TCP	SMTP	Admin-Knoten	E-Mail-Server	Wird für Warnungen und E-Mail-basierten AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 auf der Seite „E-Mail-Server“ überschreiben.
53	TCP/UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Knoten	DHCP-Dienst	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird für statisch konfigurierte Grids nicht ausgeführt.
68	UDP	DHCP	DHCP-Dienst	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-Knoten	Port 80 leitet für die Benutzeroberfläche des Admin-Knotens auf Port 443 um.
80	TCP	HTTP	Browser	Geräte	Port 80 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
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-Porteinstellung von 80 beim Erstellen eines Endpunkts überschreiben.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
80	TCP	HTTP	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTP verwenden. Grid-Administratoren können die Standard-HTTP-Porteinstellung von 80 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
111	TCP/UDP	RPCBind	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (Portmap) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
123	UDP	NTP	Primäre NTP-Knoten	Externes NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Knoten synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/UDP	SNMP	SNMP-Client	Alle Knoten	Wird für SNMP-Polling verwendet. Alle Knoten stellen grundlegende Informationen bereit; Admin-Knoten stellen auch Warndaten bereit. Bei Konfiguration wird standardmäßig der UDP-Port 161 verwendet. **Hinweis:** Dieser Port ist nur erforderlich und wird nur in der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	Ausgehende SNMP-Benachrichtigungen und Traps werden standardmäßig an UDP-Port 162 gesendet. **Hinweis:** Dieser Port ist nur erforderlich, wenn SNMP aktiviert und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren. **Hinweis:** Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
389	TCP/UDP	LDAP	Speicherknoten mit ADC	Active Directory/LDAP	Wird zum Herstellen einer Verbindung mit einem Active Directory- oder LDAP-Server für die Identitätsföderation verwendet.
443	TCP	HTTPS	Browser	Admin-Knoten	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 zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.
443	TCP	HTTPS	Admin-Knoten	Active Directory	Wird von Admin-Knoten 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 Standard-HTTP-Porteinstellung 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speicherknoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTPS verwenden. Grid-Administratoren können die Standard-HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
903	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export verwendet(`rpc.mountd`). **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
2022	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 22 anstelle von 2022 verwenden.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
2049	TCP	NFS	NFS-Client	Admin-Knoten	Wird vom NFS-basierten Audit-Export (NFS) verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist. **Hinweis:** Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.
5353	UDP	mDNS	Alle Knoten	Alle Knoten	Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. **Hinweis**: Die Konfiguration dieses Ports ist optional.
5696	TCP	KMIP	Gerät	KMS	Externer Datenverkehr des Key Management Interoperability Protocol (KMIP) von für die Knotenverschlüsselung konfigurierten Geräten zum Key Management Server (KMS), sofern auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer kein anderer Port angegeben ist.
8022	TCP	SSH	Service-Laptop	Alle Knoten	SSH auf Port 8022 gewährt Zugriff auf das Basisbetriebssystem auf Appliance- und virtuellen Knotenplattformen für Support und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare-Metal-)Knoten verwendet und muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
8443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen. **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 zur Liste der privilegierten Adressen hinzugefügt. Siehe"Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
8443	TCP	HTTPS	Browser	Geräte	Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen. **Hinweis**: Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
9022	TCP	SSH	Service-Laptop	Geräte	Gewährt Zugriff auf StorageGRID -Geräte 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-Knoten	Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet. **Hinweis:** Dieser Port wird nur benötigt, wenn der zertifikatsbasierte 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 standardmäßige Kafka-Porteinstellung von 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Knoten	Optional. Wird von Webbrowsern und Verwaltungs-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.
18082	TCP	HTTPS	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18083	TCP	HTTPS	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18084	TCP	HTTP	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTP).
18085	TCP	HTTP	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTP).

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die Cross-Grid-Replikation	Admin-Knoten und Gateway-Knoten im Ziel-Grid für die Cross-Grid-Replikation	Dieser Portbereich ist für Grid-Föderation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden denselben Port.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.