



Netzwerkrichtlinien

StorageGRID

NetApp
November 04, 2025

Inhalt

| | |
|---|----|
| Netzwerkrichtlinien | 1 |
| Netzwerkrichtlinien: Überblick | 1 |
| Informationen zu diesen Anweisungen | 1 |
| Bevor Sie beginnen | 1 |
| StorageGRID-Netzwerktypen | 2 |
| Verkehrstypen | 2 |
| Netzwerkschnittstellen | 2 |
| Grid-Netzwerk | 3 |
| Admin-Netzwerk | 4 |
| Client-Netzwerk | 5 |
| Optionale VLAN-Netzwerke | 5 |
| Beispiele für Netzwerktopologie | 6 |
| Grid-Netzwerktopologie | 6 |
| Admin-Netzwerktopologie | 7 |
| Client-Netzwerktopologie | 9 |
| Topologie für alle drei Netzwerke | 11 |
| Netzwerkanforderungen | 12 |
| Allgemeine Netzwerkanforderungen | 13 |
| Wide Area Networks (WANs) für mehrere Standorte | 13 |
| Verbindungen für Admin-Nodes und Gateway-Nodes | 14 |
| Verwendung von NAT (Network Address Translation) | 14 |
| Netzwerkspezifische Anforderungen | 14 |
| Netzwerk-Gateways und -Router | 14 |
| Subnetze | 14 |
| Grid-Netzwerk | 15 |
| Admin-Netzwerk | 16 |
| Client-Netzwerk | 16 |
| Implementierungs-spezifische Netzwerküberlegungen | 16 |
| Linux Implementierungen | 16 |
| Networking und Ports für Plattform-Services und Cloud Storage-Pools | 18 |
| Appliance-Nodes | 19 |
| Netzwerkinstallation und -Bereitstellung | 20 |
| Erste Implementierung eines Node | 20 |
| Automatische Knotenregistrierung mit primärem Admin-Node | 20 |
| Deaktivieren des Admin-Netzwerks oder des Client-Netzwerks | 20 |
| Richtlinien nach der Installation | 20 |
| Referenz für Netzwerk-Ports | 21 |
| Interne Kommunikation mit Grid-Nodes | 21 |
| Externe Kommunikation | 25 |

Netzwerkrichtlinien

Netzwerkrichtlinien: Überblick

Mithilfe dieser Richtlinien lernen Sie die StorageGRID Architektur und Netzwerktopologien kennen und erfahren Sie mehr über die Anforderungen für Netzwerkkonfiguration und Provisionierung.

Informationen zu diesen Anweisungen

Diese Richtlinien stellen Informationen bereit, die zum Erstellen der StorageGRID Netzwerkinfrastruktur vor der Bereitstellung und Konfiguration von StorageGRID Nodes verwendet werden können. Verwenden Sie diese Richtlinien, um sicherzustellen, dass die Kommunikation zwischen allen Knoten im Netz und zwischen dem Netz und externen Clients und Diensten erfolgen kann.

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

- Speichern und Abrufen von Objektdaten
- Benachrichtigungen erhalten
- Zugriff auf die StorageGRID Management-Schnittstelle (Grid Manager und MandantenManager)
- Zugriff auf die Revisionsfreigabe (optional)
- Die Bereitstellung von Services wie:
 - Network Time Protocol (NTP)
 - Domain Name System (DNS)
 - Verschlüsselungsmanagement-Server (KMS)

StorageGRID-Netzwerke müssen entsprechend konfiguriert werden, um den Datenverkehr für diese Funktionen und vieles mehr zu verarbeiten.

Bevor Sie beginnen

Die Konfiguration des Netzwerks für ein StorageGRID System erfordert eine hohe Erfahrung mit Ethernet-Switching, TCP/IP-Netzwerken, Subnetzen, Netzwerk-Routing und Firewalls.

Machen Sie sich vor dem Konfigurieren des Netzwerknetzwerks mit der StorageGRID-Architektur vertraut, wie in beschrieben "[Weitere Informationen zu StorageGRID](#)".

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

Installieren Sie Appliance-Knoten

- "[Appliance-Hardware installieren](#)"

Installation softwarebasierter Nodes

- "[Installieren Sie StorageGRID unter Red hat Enterprise Linux](#)"
- "[Installieren Sie StorageGRID auf Ubuntu oder Debian](#)"

- ["Installieren Sie StorageGRID auf VMware"](#)

StorageGRID Software konfigurieren und verwalten

- ["StorageGRID verwalten"](#)
- ["Versionshinweise"](#)

StorageGRID-Netzwerktypen

Die Grid-Nodes in einem StorageGRID-Systemprozess *Grid Traffic*, *admin Traffic* und *Client Traffic*. Sie müssen das Netzwerk entsprechend konfigurieren, um diese drei Arten von Datenverkehr zu managen und um Kontrolle und Sicherheit zu bieten.

Verkehrstypen

| Verkehrstyp | Beschreibung | Netzwerktyp |
|--------------------|---|--|
| Grid-Traffic | Der interne StorageGRID-Datenverkehr zwischen allen Nodes im Grid. Alle Grid-Nodes müssen über dieses Netzwerk mit allen anderen Grid-Nodes kommunizieren können. | Grid-Netzwerk (erforderlich) |
| Admin-Datenverkehr | Der für die Systemadministration und -Wartung verwendete Datenverkehr. | Admin-Netzwerk (optional), VLAN-Netzwerk (optional) |
| Client-Traffic | Der Datenverkehr zwischen externen Client-Applikationen und dem Grid, einschließlich aller Objekt-Storage-Anforderungen von S3 und Swift Clients | Client-Netzwerk (optional), VLAN-Netzwerk (optional) |

Sie haben folgende Möglichkeiten zur Konfiguration des Netzwerks:

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

Das Grid-Netzwerk ist obligatorisch und kann den gesamten Grid-Verkehr verwalten. Die Admin- und Client-Netzwerke können zum Zeitpunkt der Installation hinzugefügt oder später hinzugefügt werden, um sich an Änderungen der 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 für den administrativen und Client-Datenverkehr verwenden.

Auf interne Ports kann nur über das Grid-Netzwerk zugegriffen werden. Auf externe Ports kann von allen Netzwerktypen zugegriffen werden. Diese Flexibilität bietet mehrere Optionen für den Entwurf einer StorageGRID-Implementierung sowie für die Einrichtung einer externen IP- und Portfilterung in Switches und Firewalls. Siehe ["Interne Kommunikation mit Grid-Nodes"](#) Und ["Externe Kommunikation"](#).

Netzwerkschnittstellen

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

| Netzwerk | Schnittstellename |
|------------------------------|-------------------|
| Grid-Netzwerk (erforderlich) | Eth0 |
| Admin-Netzwerk (optional) | Eth1 |
| Client-Netzwerk (optional) | Eth2 |

Weitere Informationen über die Zuordnung von virtuellen oder physischen Ports zu Node-Netzwerkschnittstellen finden Sie in den Installationsanweisungen:

Softwarebasierte Nodes

- ["Installieren Sie StorageGRID unter Red hat Enterprise Linux"](#)
- ["Installieren Sie StorageGRID auf Ubuntu oder Debian"](#)
- ["Installieren Sie StorageGRID auf VMware"](#)

Appliance-Nodes

- ["SG6160 Storage Appliance"](#)
- ["SGF6112 Storage Appliance"](#)
- ["SG6000 Storage Appliance"](#)
- ["Storage Appliance SG5800"](#)
- ["SG5700 Storage-Appliance"](#)
- ["Service Appliances für SG110 und SG1100"](#)
- ["SG100- und SG1000-Services-Appliances"](#)

Netzwerkinformationen für jeden Node

Sie müssen für jedes auf einem Node zu konfigurierende Netzwerk Folgendes konfigurieren:

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

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

Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) bieten die Möglichkeit, virtuelle IP-Adressen (VIP) zur Grid- oder Client-Netzwerkschnittstelle hinzuzufügen. Weitere Informationen finden Sie unter ["Management von Hochverfügbarkeitsgruppen"](#).

Grid-Netzwerk

Das Grid-Netzwerk ist erforderlich. Er wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das Grid-Netzwerk bietet Konnektivität zwischen allen Nodes im Grid über alle Standorte und Subnetze hinweg. Alle Knoten im Grid-Netzwerk müssen in der Lage sein, mit allen anderen Knoten zu kommunizieren.

Das Grid-Netzwerk kann aus mehreren Subnetzen bestehen. Netzwerke, die kritische Grid-Services wie NTP enthalten, können auch als Grid-Subnetze hinzugefügt werden.



StorageGRID unterstützt keine Network Address Translation (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 Network Gateway ist das Standard-Gateway des Nodes, es sei denn, der Knoten hat das Client Network konfiguriert.



Wenn Sie das Grid-Netzwerk konfigurieren, müssen Sie sicherstellen, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie 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 es mehrere Grid-Subnetze gibt.
- Das Grid-Netzwerk-Gateway ist der Node-Standard-Gateway, bis die Grid-Konfiguration abgeschlossen ist.
- Statische Routen werden automatisch für alle Nodes zu allen Subnetzen generiert, die in der globalen Grid-Netzwerk-Subnetliste konfiguriert sind.
- 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. Bei der Konfiguration kann diese für die Systemadministration und für den Wartungs-Traffic verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Knoten routingfähig sein.

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

Wenn Sie das Admin-Netzwerk verwenden, muss der Verwaltungs- und Wartungsverkehr nicht über das Grid-Netzwerk geleitet werden. Typische Anwendungen des Admin-Netzwerks umfassen Folgendes:

- Zugriff auf die Benutzeroberflächen von Grid Manager und Tenant Manager.
- Zugriff auf wichtige Services wie NTP-Server, DNS-Server, externe Verschlüsselungsmanagement-Server (KMS) und LDAP-Server (Lightweight Directory Access Protocol)
- Zugriff auf Prüfprotokolle an Admin-Nodes.
- Secure Shell Protocol (SSH)-Zugriff für Wartung und Support

Das Admin-Netzwerk wird nie für den internen Grid-Verkehr verwendet. Ein Admin-Netzwerk-Gateway wird bereitgestellt und ermöglicht dem Admin-Netzwerk die Kommunikation mit mehreren externen Subnetzen. Das Admin-Netzwerk-Gateway wird jedoch nie als Standard-Gateway für den Node verwendet.

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

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

Client-Netzwerk

Das Client-Netzwerk ist optional. Bei der Konfiguration ermöglicht er den Zugriff auf Grid-Services für Client-Applikationen wie S3 und Swift. Wenn Sie StorageGRID Daten für eine externe Ressource zugänglich machen möchten (z. B. einen Cloud-Speicherpool oder den StorageGRID CloudMirror Replikationsservice), kann die externe Ressource auch das Client-Netzwerk nutzen. 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 sein soll. Alle Knoten müssen sich nicht im gleichen Client-Netzwerk befinden, und Knoten kommunizieren nie über das Client-Netzwerk miteinander. Das Client-Netzwerk ist erst nach Abschluss der Grid-Installation betriebsbereit.

Für zusätzliche Sicherheit können Sie angeben, dass die Client-Netzwerk-Schnittstelle eines Node nicht vertrauenswürdig ist, sodass das Client-Netzwerk restriktiver ist, welche Verbindungen zulässig sind. Wenn die Client-Netzwerk-Schnittstelle eines Node nicht vertrauenswürdig ist, akzeptiert die Schnittstelle ausgehende Verbindungen, wie sie von der CloudMirror-Replikation verwendet werden, akzeptiert jedoch nur eingehende Verbindungen an Ports, die explizit als Load-Balancer-Endpunkte konfiguriert wurden. Siehe ["Management der Firewall-Kontrollen"](#) Und ["Konfigurieren von Load Balancer-Endpunkten"](#).

Wenn Sie ein Client-Netzwerk verwenden, muss der Client-Datenverkehr nicht über das Grid-Netzwerk geleitet werden. Der Netzwerkverkehr kann in ein sicheres, nicht routingbares Netzwerk getrennt werden. Die folgenden Node-Typen werden häufig mit einem Client-Netzwerk konfiguriert:

- Gateway-Nodes, da diese Nodes Zugriff auf den StorageGRID Load Balancer Service und S3- und Swift-Client-Zugriff auf das Grid bieten.
- Storage-Nodes, da diese Nodes Zugriff auf die S3- und Swift-Protokolle sowie auf Cloud Storage Pools und den CloudMirror-Replizierungsservice bieten.
- Admin-Nodes, um sicherzustellen, dass Mandantenbenutzer mit dem Tenant Manager verbinden können, ohne das Admin Network 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 die Standardroute für den Grid-Node, wenn die Grid-Konfiguration abgeschlossen ist.

Optionale VLAN-Netzwerke

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

Zur Unterstützung der Verwendung von VLANs müssen Sie eine oder mehrere Schnittstellen auf einem Node als Trunk-Schnittstellen am Switch konfigurieren. Sie können die Grid-Netzwerkschnittstelle (eth0) oder die Client-Netzwerkschnittstelle (eth2) als Trunk konfigurieren oder dem Knoten Leitungsschnittstellen hinzufügen.

Wenn eth0 als Trunk konfiguriert ist, fließt Grid-Netzwerk-Traffic über die native Trunk-Schnittstelle, wie auf dem Switch konfiguriert. Wenn eth2 als Trunk konfiguriert ist und das Client-Netzwerk auch auf demselben Node konfiguriert ist, verwendet das Client-Netzwerk das native VLAN des Trunk-Ports wie auf dem Switch konfiguriert.

Nur eingehender Admin-Traffic, wie er für SSH, Grid Manager oder Tenant Manager-Datenverkehr verwendet wird, wird über VLAN-Netzwerke unterstützt. Outbound-Traffic, z. B. für NTP, DNS, LDAP, KMS und Cloud

Storage-Pools, wird nicht über VLAN-Netzwerke unterstützt.



VLAN-Schnittstellen können nur zu Admin-Nodes und Gateway-Nodes hinzugefügt werden. Sie können keine VLAN-Schnittstelle für den Client- oder Administratorzugriff auf Storage Nodes oder Archive Nodes verwenden.

Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)" Anweisungen und Richtlinien.

VLAN-Schnittstellen werden nur in HA-Gruppen verwendet und auf dem aktiven Node werden VIP-Adressen zugewiesen. Siehe "[Management von Hochverfügbarkeitsgruppen](#)" Anweisungen und Richtlinien.

Beispiele für Netzwerktopologie

Grid-Netzwerktopologie

Die einfachste Netzwerktopologie wird nur durch die Konfiguration des Grid-Netzwerks erstellt.

Wenn Sie das Grid-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth0-Schnittstelle für jeden Grid-Node ein.

Während der Konfiguration müssen Sie alle Grid-Netzwerk-Subnetze der Grid-Netzwerk-Subnetz-Liste (GNSL) hinzufügen. Diese Liste enthält alle Subnetze für alle Standorte und kann auch externe Subnetze enthalten, die den Zugriff auf kritische Services wie NTP, DNS oder LDAP bieten.

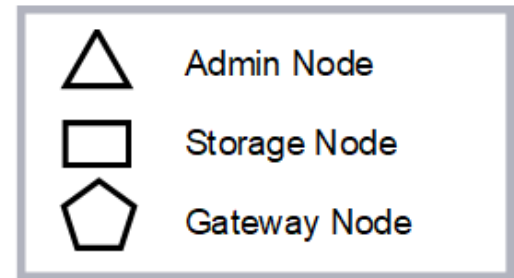
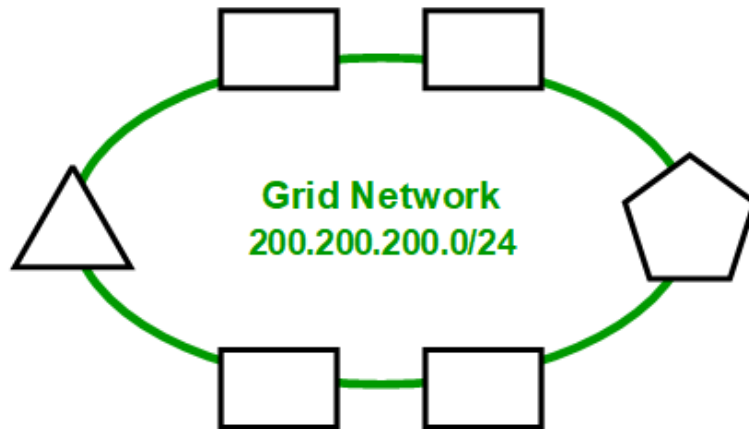
Bei der Installation wendet die Grid-Netzwerkschnittstelle statische Routen für alle Subnetze in der GNSL an und setzt die Standardroute des Knotens auf das Grid-Netzwerk-Gateway, wenn eine konfiguriert ist. Die GNSL ist nicht erforderlich, wenn kein Client-Netzwerk vorhanden ist und das Grid-Netzwerk-Gateway die Standardroute des Knotens ist. Zudem werden Host-Routen zu allen anderen Knoten im Grid generiert.

In diesem Beispiel verwendet der gesamte Datenverkehr dasselbe Netzwerk, einschließlich des Datenverkehrs für S3- und Swift-Client-Anforderungen sowie Administrations- und Wartungsfunktionen.



Diese Topologie eignet sich für Implementierungen an einem einzigen Standort, die nicht extern verfügbar sind, Proof-of-Concept- oder Testbereitstellungen oder wenn ein Load Balancer eines Drittanbieters als Grenze für den Client-Zugriff fungiert. Wenn möglich, sollte das Grid-Netzwerk ausschließlich für den internen Datenverkehr verwendet werden. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk haben zusätzliche Firewall-Einschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, aber diese Verwendung bietet 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

Die Verwendung eines Admin-Netzwerks ist optional. Eine Möglichkeit, wie Sie ein Admin-Netzwerk und ein Grid-Netzwerk verwenden können, besteht darin, ein routingbares Grid-Netzwerk und ein verbundenes Admin-Netzwerk für jeden Knoten zu konfigurieren.

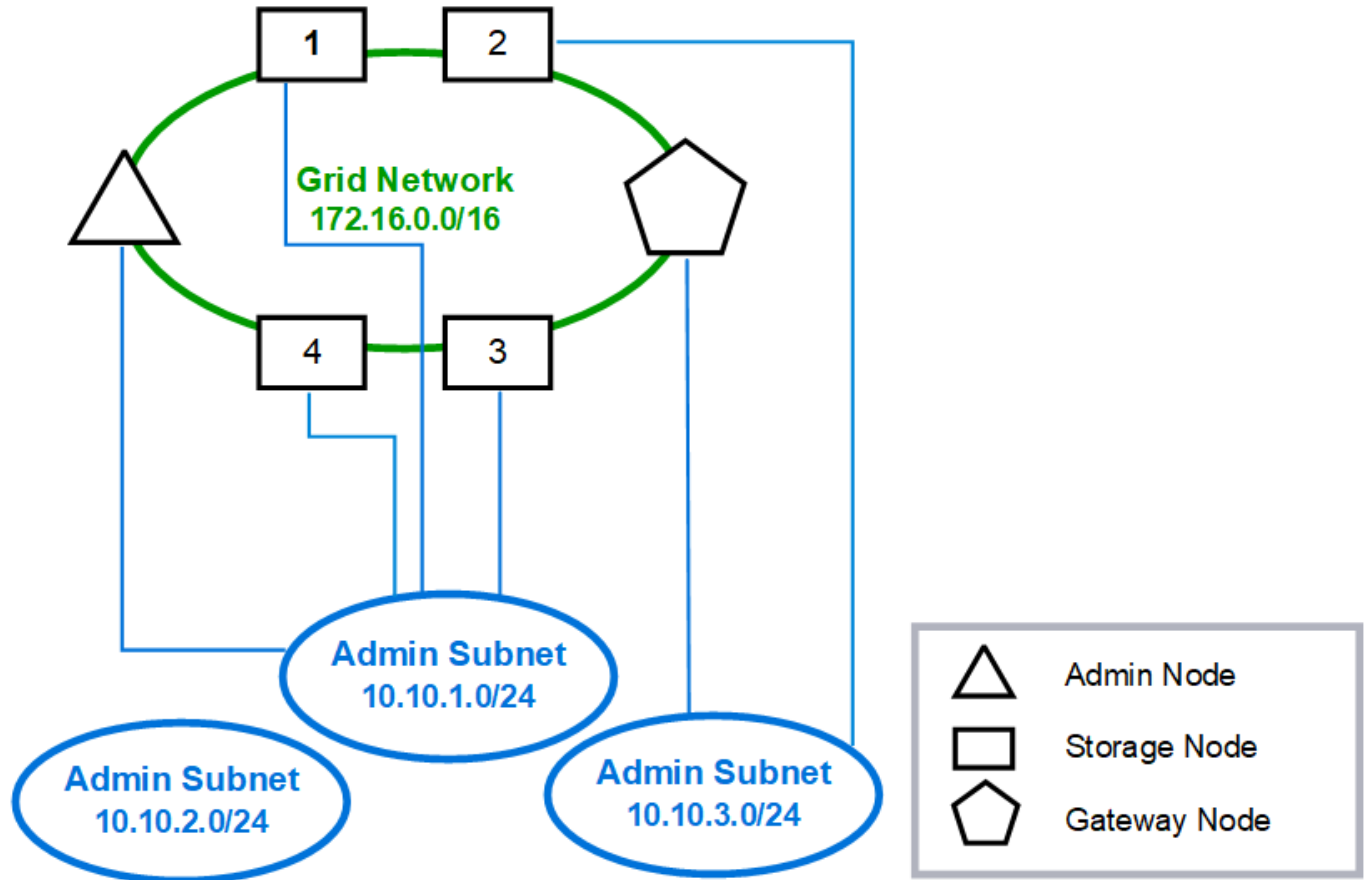
Wenn Sie das Admin-Netzwerk konfigurieren, stellen Sie für jeden Grid-Node die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth1-Schnittstelle fest.

Das Admin-Netzwerk kann für jeden Knoten eindeutig sein und aus mehreren Subnetzen bestehen. Jeder Node kann mit einer externen Subnetz-Liste (AESL) des Administrators konfiguriert werden. Die AESL listet die Subnetze auf, die über das Admin-Netzwerk für jeden Knoten erreichbar sind. Die AESL muss auch die Subnetze aller Dienste enthalten, auf die das Grid über das Admin-Netzwerk zugreifen kann, wie NTP, DNS,

KMS und LDAP. Für jedes Subnetz in der AESL werden statische Routen angewendet.

In diesem Beispiel wird das Grid Network für Traffic verwendet, der mit S3- und Swift-Client-Anforderungen und Objektmanagement zusammenhängt. Während das Admin-Netzwerk für administrative Funktionen verwendet wird.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

| Nodes | Grid Network | | Admin Network | |
|-----------|------------------|--------------|---------------|-----------|
| | 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. Über ein Client-Netzwerk kann der Netzwerk-Traffic des Clients (z. B. S3 und Swift) vom internen Grid-Datenverkehr getrennt werden, wodurch die Sicherheit des Grid-Netzwerks erhöht wird. Wenn das Admin-Netzwerk nicht konfiguriert ist, kann der administrative Datenverkehr entweder vom Client oder vom Grid-Netzwerk verarbeitet werden.

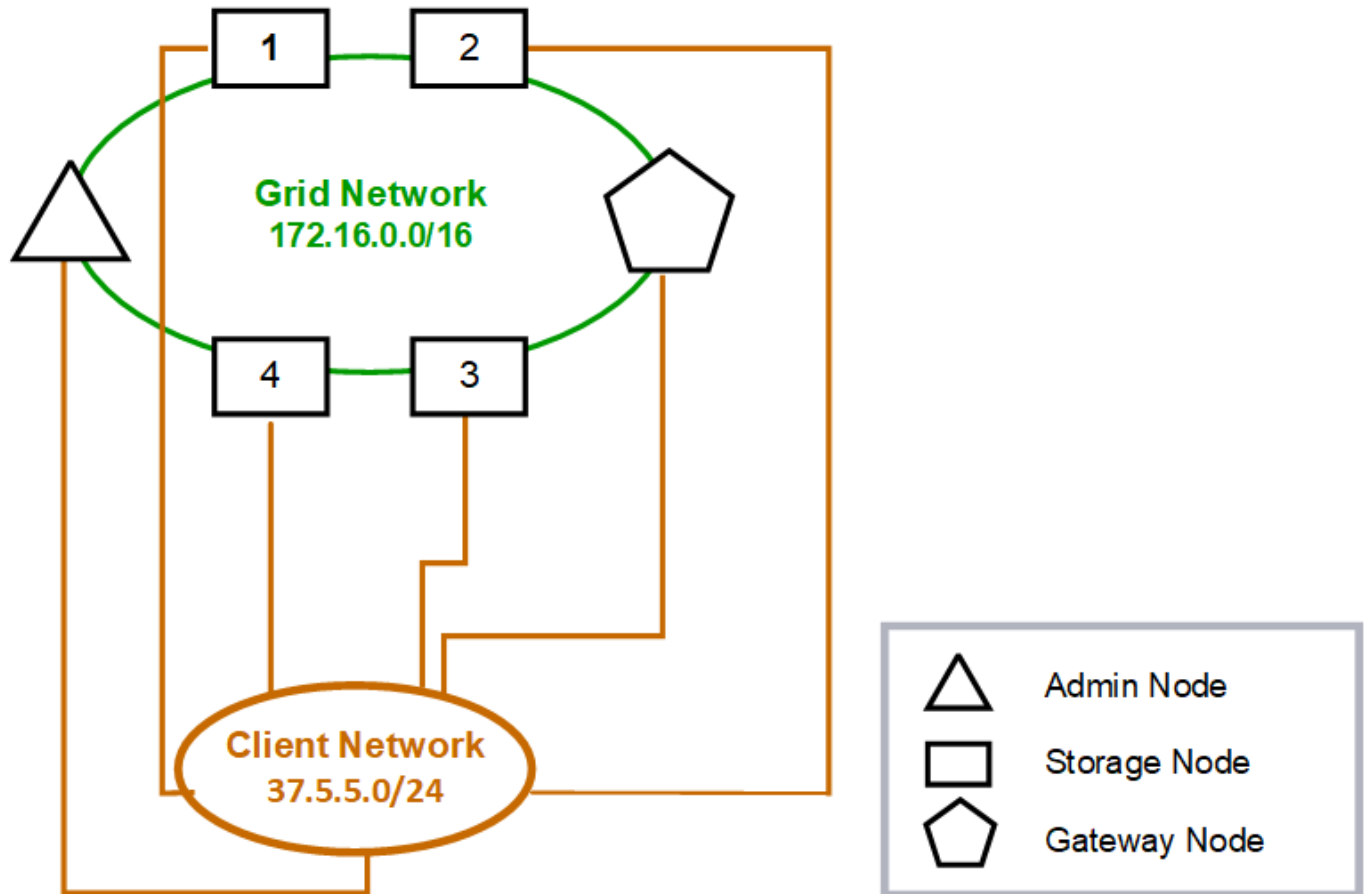
Wenn Sie das Client-Netzwerk konfigurieren, stellen Sie die Host-IP-Adresse, die Subnetzmaske und die Gateway-IP-Adresse für die eth2-Schnittstelle für den konfigurierten Node fest. Das Client-Netzwerk jedes Knotens kann unabhängig vom Client-Netzwerk auf jedem anderen Knoten sein.

Wenn Sie während der Installation ein Client-Netzwerk für einen Node konfigurieren, wechselt das Standard-Gateway des Node vom Grid Network Gateway zum Client Network Gateway, wenn die Installation abgeschlossen ist. Wenn später ein Client-Netzwerk hinzugefügt wird, wechselt das Standard-Gateway des Node auf die gleiche Weise.

In diesem Beispiel wird das Client-Netzwerk für S3- und Swift-Client-Anforderungen sowie für administrative

Funktionen verwendet, während das Grid-Netzwerk internen Objektmanagementvorgängen zugewiesen ist.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

| Nodes | Grid Network | Client Network | |
|---------|------------------|----------------|----------|
| | 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 |

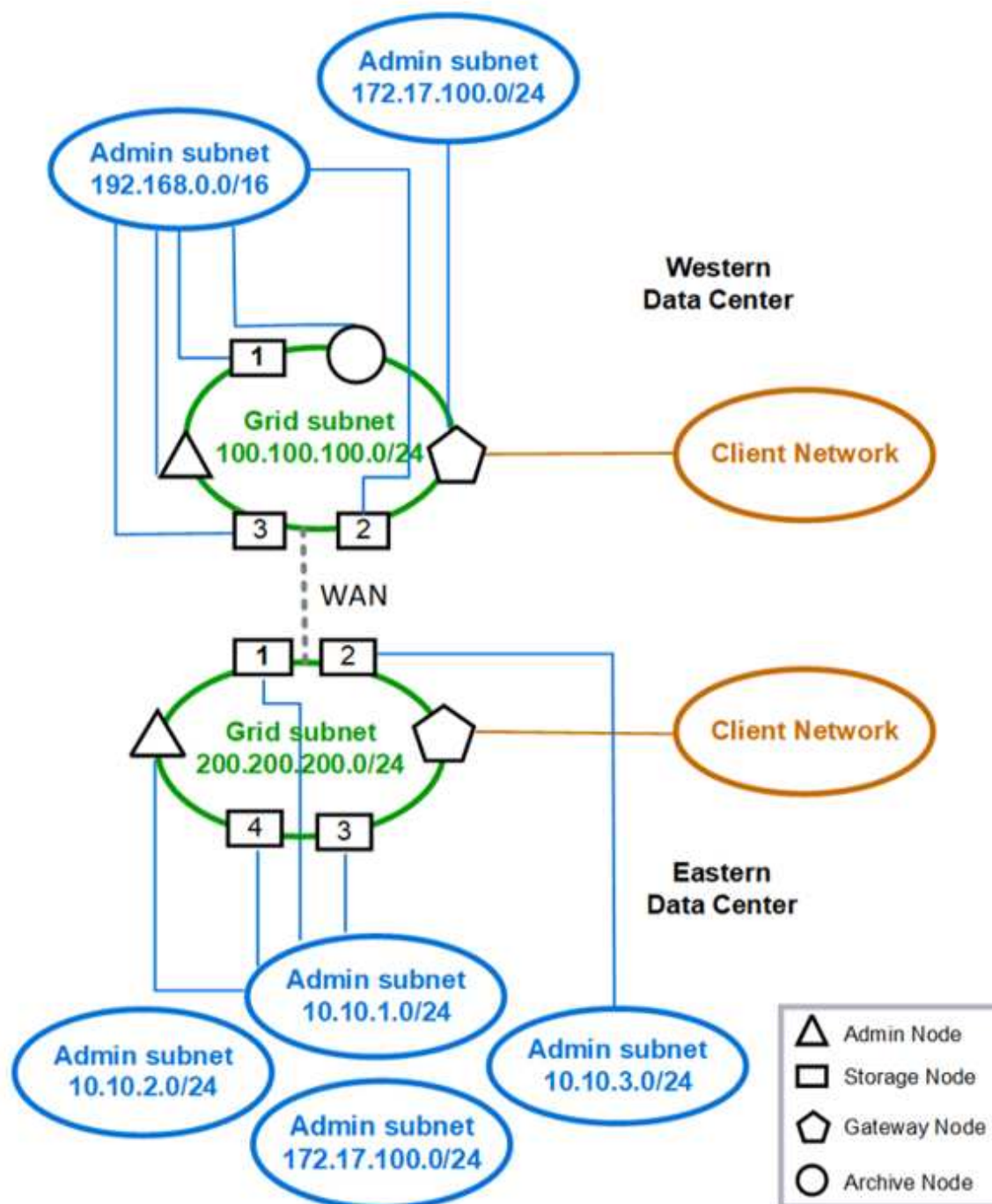
Topologie für alle drei Netzwerke

Sie können alle drei Netzwerke in einer Netzwerktopologie konfigurieren, die aus einem privaten Grid-Netzwerk, eingeschränkten 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 Netzwerkdatenverkehr verwendet, der mit internen Objektmanagementvorgängen in Verbindung steht.
- Das Admin-Netzwerk wird für den Datenverkehr in Verbindung mit administrativen Funktionen verwendet.
- Das Client-Netzwerk wird für Datenverkehr verwendet, der mit S3- und Swift-Client-Anforderungen verbunden ist.

Topology example: Grid, Admin, and Client Networks



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 die Grid-, Admin- oder Client-Netzwerke oder die Kombinationen dieser Netzwerke erfolgen, wie in den Beispielen der Netzwerktopologie dargestellt.

- **Management Connections:** Eingehende Verbindungen von einem Administrator zum Knoten, normalerweise über SSH. Zugriff über einen Webbrowser auf den Grid Manager, den Mandantenmanager und das Installationsprogramm der StorageGRID-Appliance.
- * NTP-Serververbindungen*: Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.

Mindestens ein NTP-Server muss über den primären Admin-Node erreichbar sein.

- **DNS-Serververbindungen:** Ausgehende UDP-Verbindung, die eine eingehende UDP-Antwort empfängt.
- **LDAP/Active Directory-Serververbindungen:** Ausgehende TCP-Verbindung vom Identitätsservice auf Speicherknoten.
- **AutoSupport:** Ausgehende TCP-Verbindung von den Admin-Knoten zu entweder `support.netapp.com` Oder einen vom Kunden konfigurierten Proxy.
- **Externer Schlüsselverwaltungsserver:** Ausgehende TCP-Verbindung von jedem Appliance-Knoten mit aktivierter Node-Verschlüsselung.
- Eingehende TCP-Verbindungen von S3 und Swift Clients.
- Ausgehende Anforderungen von StorageGRID Plattform-Services wie CloudMirror Replizierung oder von Cloud-Storage-Pools.

Wenn StorageGRID keinen der bereitgestellten NTP- oder DNS-Server unter Verwendung der standardmäßigen Routing-Regeln kontaktieren kann, versucht es automatisch, in allen Netzwerken (Grid, Admin und Client) Kontakt aufzunehmen, solange die IP-Adressen der DNS- und NTP-Server angegeben sind. Wenn die NTP- oder DNS-Server in einem Netzwerk erreicht werden können, erstellt StorageGRID automatisch zusätzliche Routingregeln, um sicherzustellen, dass das Netzwerk für alle zukünftigen Verbindungsversuche verwendet wird.



Obwohl Sie diese automatisch ermittelten Host-Routen verwenden können, sollten Sie die DNS- und NTP-Routen manuell konfigurieren, um die Verbindung zu gewährleisten, falls die automatische Erkennung fehlschlägt.

Wenn Sie während der Bereitstellung 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 Change IP-Tool konfigurieren (siehe "[Konfigurieren Sie IP-Adressen](#)").

Nur S3- und Swift-Client-Verbindungen sowie SSH-, Grid Manager- und Mandanten-Manager-Administratorverbindungen werden über VLAN-Schnittstellen unterstützt. Outbound-Verbindungen, z. B. zu NTP-, DNS-, LDAP-, AutoSupport- und KMS-Servern, muss die Client-, Admin- oder Grid-Netzwerkschnittstellen direkt überführen. Wenn die Schnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, fließt dieser Datenverkehr über das native VLAN der Schnittstelle, wie es am Switch konfiguriert ist.

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/s in jeder Richtung aufweisen, bevor der Client-Datenverkehr berücksichtigt wird. Datenreplizierung oder Erasure Coding zwischen Standorten, Erweiterung von Nodes oder Standorten, Recovery von Nodes und anderen Vorgängen oder Konfigurationen erfordern zusätzliche Bandbreite.

Die tatsächlichen Anforderungen an die WAN-Mindestbandbreite hängen von der Client-Aktivität und dem ILM-Schutzschema ab. Wenden Sie sich an Ihren NetApp Professional Services Berater, um die Mindestanforderungen an die WAN-Bandbreite einschätzen zu können.

Verbindungen für Admin-Nodes und Gateway-Nodes

Admin-Knoten müssen immer von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, gesichert werden. Sie müssen sicherstellen, dass kein nicht vertrauenswürdiger Client auf einen beliebigen Admin-Node im Grid-Netzwerk, auf das Admin-Netzwerk oder auf das Client-Netzwerk zugreifen kann.

Admin-Nodes und Gateway-Nodes, die Sie zu Hochverfügbarkeitsgruppen hinzufügen möchten, müssen mit einer statischen IP-Adresse konfiguriert werden. Weitere Informationen finden Sie unter "[Management von Hochverfügbarkeitsgruppen](#)".

Verwendung von NAT (Network Address Translation)

Verwenden Sie keine Network Address Translation (NAT) im Grid-Netzwerk zwischen Grid-Knoten oder zwischen StorageGRID-Standorten. Wenn Sie private IPv4-Adressen für das Grid-Netzwerk verwenden, müssen diese Adressen von jedem Grid-Knoten an jedem Standort direkt routingfähig sein. Sie können jedoch bei Bedarf NAT zwischen externen Clients und Grid-Nodes verwenden, beispielsweise um eine öffentliche IP-Adresse für einen Gateway Node bereitzustellen. Die Verwendung von NAT zur Brücke eines öffentlichen Netzwerksegments wird nur unterstützt, wenn Sie eine Tunneling-Anwendung verwenden, die für alle Knoten im Netz transparent ist. Das bedeutet, dass die Grid-Knoten keine Kenntnisse über öffentliche IP-Adressen benötigen.

Netzwerkspezifische Anforderungen

Befolgen Sie die Anforderungen für jeden StorageGRID Netzwerktyp.

Netzwerk-Gateways und -Router

- Wenn gesetzt, muss sich das Gateway für ein bestimmtes Netzwerk im Subnetz des spezifischen Netzwerks befinden.
- Wenn Sie eine Schnittstelle mit statischer Adresse konfigurieren, müssen Sie eine andere Gateway-Adresse als 0.0.0.0 angeben.
- Wenn Sie kein Gateway haben, sollten Sie die Gateway-Adresse als IP-Adresse der Netzwerkschnittstelle festlegen.

Subnetze



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

Die folgenden Einschränkungen werden während der Bereitstellung durch den Grid Manager durchgesetzt. Sie werden hier zur Unterstützung bei der Netzwerkplanung vor der Implementierung bereitgestellt.

- Die Subnetzmaske für eine beliebige Netzwerk-IP-Adresse darf nicht 255.255.255.254 oder 255.255.255.255 sein (/31 oder /32 in CIDR-Notation).
- Das Subnetz, das durch eine IP-Adresse der Netzwerkschnittstelle und eine Subnetzmaske (CIDR) definiert ist, kann das Subnetz einer anderen Schnittstelle, die auf demselben Knoten konfiguriert ist, nicht überlappen.
- 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 Node muss in der GNSL enthalten sein.
- Das Subnetz Admin Network darf sich nicht mit dem Subnetz Grid Network, dem Subnetz Client Network oder einem Subnetz im GNSL überlappen.
- Die Subnetze im AESL dürfen sich nicht mit Subnetzen im GNSL überlappen.
- Das Client-Netzwerk-Subnetz darf sich nicht mit dem Subnetz des Grid-Netzwerks, dem Subnetz des Admin-Netzwerks, einem beliebigen Subnetz im GNSL oder einem beliebigen Subnetz im AESL überlappen.

Grid-Netzwerk

- Bei der Bereitstellung muss jeder Grid-Node mit dem Grid-Netzwerk verbunden sein und mit dem primären Admin-Node über die bei der Bereitstellung des Node angegebene Netzwerkkonfiguration kommunizieren können.
- Während normaler Grid-Vorgänge muss jeder Grid-Node in der Lage sein, über das Grid-Netzwerk mit allen anderen Grid-Nodes zu kommunizieren.



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

- Wenn das Grid-Netzwerk aus mehreren Subnetzen besteht, fügen Sie sie der Grid Network Subnet List (GNSL) hinzu. Für jedes Subnetz in der GNSL werden auf allen Knoten statische Routen erstellt.
- Wenn die Grid-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, muss das Trunk-native VLAN das VLAN sein, das für Grid-Netzwerk-Traffic verwendet wird. Über das native Trunk-VLAN muss auf alle Grid-Nodes zugegriffen werden können.

Admin-Netzwerk

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

Typische Verwendungszwecke des Admin-Netzwerks sind Managementverbindungen, 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 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 aus externen Subnetzen zu aktivieren. Für jedes Subnetz in der AESL werden automatisch statische Routen auf jedem Knoten erzeugt.

Client-Netzwerk

Das Client-Netzwerk ist optional. Wenn Sie ein Client-Netzwerk konfigurieren möchten, beachten Sie die folgenden Überlegungen.

- Das Client Network unterstützt Datenverkehr von S3 und Swift Clients. Wenn konfiguriert, wird das Client-Netzwerk-Gateway zum Standard-Gateway des Node.
- Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Load Balancer-Endpunkten akzeptieren. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)".
- Wenn die Client-Netzwerkschnittstelle als Trunk zur Unterstützung von VLAN-Schnittstellen konfiguriert ist, sollten Sie prüfen, ob die Konfiguration der Client-Netzwerkschnittstelle (eth2) erforderlich ist. Wenn konfiguriert, wird der Client-Netzwerk-Datenverkehr über das native Trunk-VLAN geleitet, wie es im Switch konfiguriert ist.

Implementierungs-spezifische Netzwerküberlegungen

Linux Implementierungen

Das StorageGRID System wird unter Linux als Sammlung von Container-Engines ausgeführt, um Effizienz, Zuverlässigkeit und Sicherheit zu gewährleisten. Die Container-Engine-bezogene Netzwerkkonfiguration ist bei einem StorageGRID System nicht erforderlich.

Verwenden Sie für die Container-Netzwerkschnittstelle ein Gerät ohne Bindung, z. B. ein VLAN- oder ein virtuelles Ethernet-Paar (Veth). Geben Sie dieses Gerät als Netzwerkschnittstelle in der Node-Konfigurationsdatei an.



Verwenden Sie keine Bond- oder Bridge-Geräte direkt als Container-Netzwerkschnittstelle. Dies könnte den Start von Knoten verhindern, weil ein Kernel-Problem mit der Verwendung von macvlan mit Bond- und Bridge-Geräten im Container-Namespace vorliegt.

Siehe Installationsanweisungen für "[Red Hat Enterprise Linux](#)" Oder "[Ubuntu oder Debian](#)" Implementierungen.

Hostnetzwerkconfiguration für Container-Engine-Implementierungen

Bevor Sie Ihre StorageGRID-Implementierung auf einer Container-Engine-Plattform starten, ermitteln Sie, welche Netzwerke (Grid, Administrator, Client) jeder Node verwenden wird. Sie müssen sicherstellen, dass die Netzwerkschnittstelle jedes Node auf der richtigen 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-Nodes verwenden:

- Stellen Sie sicher, dass alle Hosts für jede Node-Schnittstelle dieselbe Host-Schnittstelle verwenden. Diese Strategie vereinfacht die Host-Konfiguration und ermöglicht die zukünftige Node-Migration.
- Beziehen Sie eine IP-Adresse für den physischen Host selbst.



Eine physische Schnittstelle auf dem Host kann vom Host selbst und von einem oder mehreren Nodes verwendet werden, die auf dem Host ausgeführt werden. Alle IP-Adressen, die dem Host oder Knoten über diese Schnittstelle zugewiesen sind, müssen eindeutig sein. Der Host und der Node können keine IP-Adressen gemeinsam nutzen.

- Öffnen Sie die erforderlichen Ports zum Host.
- Wenn Sie beabsichtigen, VLAN-Schnittstellen in StorageGRID zu verwenden, 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 in den Node-Container übergeben werden. Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:
 - **RHEL (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **Ubuntu oder Debian (vor der Installation des Knotens):** ["Erstellen von Node-Konfigurationsdateien"](#)
 - **RHEL, Ubuntu oder Debian (nach der Installation des Knotens):** ["Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"](#)

Empfehlungen für die minimale Bandbreite

Die folgende Tabelle enthält die Empfehlungen für die minimale LAN-Bandbreite für jeden StorageGRID-Node-Typ und jeden Netzwerktyp. Sie müssen jeden physischen oder virtuellen Host mit ausreichender Netzwerkbandbreite bereitstellen, um die Mindestanforderungen an die Bandbreite für das Aggregat für die Gesamtzahl und den Typ der StorageGRID Nodes, die auf diesem Host ausgeführt werden sollen, zu erfüllen.

| Node-Typ | Netzwerktyp | | |
|-----------|-------------|--------------|-----------|
| | Raster | Admin | Client |
| | | Admin | 10 Gbit/S |
| 1 Gbit/S. | 1 Gbit/S. | Gateway | 10 Gbit/S |
| 1 Gbit/S. | 10 Gbit/S | Storage | 10 Gbit/S |
| 1 Gbit/S. | 10 Gbit/S | Archivierung | 10 Gbit/S |



Diese Tabelle enthält keine SAN-Bandbreite, die für den Zugriff auf Shared Storage erforderlich ist. Wenn Sie gemeinsam genutzten Storage verwenden, auf den Sie über Ethernet (iSCSI oder FCoE) zugreifen können, sollten Sie separate physische Schnittstellen für jeden Host bereitstellen, um ausreichend SAN-Bandbreite zur Verfügung zu stellen. Um einen Engpass zu vermeiden, sollte die SAN-Bandbreite für einen bestimmten Host in etwa der aggregierten Storage Node-Netzwerkbandbreite für alle Storage Nodes, die auf diesem Host ausgeführt werden, entsprechen.

Mithilfe der Tabelle können Sie die Mindestanzahl an Netzwerkschnittstellen bestimmen, die für jeden Host bereitgestellt werden sollen. Diese basieren auf der Anzahl und dem Typ der StorageGRID Nodes, die Sie auf diesem Host ausführen möchten.

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

- Verbinden Sie die Grid- und Admin-Netzwerke auf dem Admin-Node (erfordert $10 + 1 = 11$ Gbit/s).
- Verbinden der Grid- und Client-Netzwerke auf dem Gateway-Node (erfordert $10 + 10 = 20$ Gbit/s)
- Verbinden des Grid-Netzwerks mit dem Storage-Node (erfordert 10 Gbit/s)

In diesem Szenario sollten Sie mindestens $11 + 20 + 10 = 41$ GBit/s Netzwerkbandbreite angeben. Dies konnte von zwei 40 Gbps Schnittstellen oder fünf 10 Gbps Schnittstellen erreicht werden, die möglicherweise in Trunks aggregiert und dann von den drei oder mehr VLANs, die die Grid-, Admin- und Client-Subnetze lokal zum physischen Rechenzentrum mit dem Host übertragen, gemeinsam genutzt werden.

Einige empfohlene Möglichkeiten zur Konfiguration physischer und Netzwerkressourcen auf den Hosts in Ihrem StorageGRID Cluster zur Vorbereitung der StorageGRID-Bereitstellung finden Sie im folgenden:

- ["Konfiguration des Hostnetzwerks \(Red hat Enterprise Linux\)"](#)
- ["Konfigurieren des Hostnetzwerks \(Ubuntu oder Debian\)"](#)

Networking und Ports für Plattform-Services und Cloud Storage-Pools

Wenn Sie Vorhaben, StorageGRID Plattform-Services oder Cloud-Storage-Pools zu verwenden, müssen Sie Grid-Netzwerke und Firewalls konfigurieren, um sicherzustellen, dass die Ziel-Endpunkte erreicht werden können.

Networking für Plattform-Services

Wie in beschrieben ["Management von Plattform-Services für Mandanten"](#) Und ["Management von Plattform-Services"](#), Plattform-Services umfassen externe Services, die Integration von Suchvorgängen, Ereignisbenachrichtigung und CloudMirror Replikation bieten.

Plattform-Services benötigen Zugriff von Storage-Nodes, die den StorageGRID ADC-Service für die externen Service-Endpunkte hosten. Beispiele für die Bereitstellung des Zugriffs:

- Konfigurieren Sie auf den Speicherknoten mit ADC-Diensten eindeutige Admin-Netzwerke mit AESL-Einträgen, die zu den Ziel-Endpunkten weiterleiten.
- Verlassen Sie sich auf die Standardroute, die von einem Client-Netzwerk bereitgestellt wird. Wenn Sie die Standardroute verwenden, können Sie die verwenden ["Nicht vertrauenswürdige Client-Netzwerkfunktion"](#) So beschränken Sie eingehende Verbindungen.

Netzwerk für Cloud-Storage-Pools

Cloud-Storage-Pools erfordern außerdem Zugriff von Storage-Nodes auf die Endpunkte, die durch einen externen Service wie Amazon S3 Glacier oder Microsoft Azure Blob Storage bereitgestellt werden. Weitere Informationen finden Sie unter ["Was ist ein Cloud-Storage-Pool"](#).

Ports für Plattform-Services und Cloud-Storage-Pools

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

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

Ein anderer Port kann angegeben werden, wenn der Endpunkt erstellt oder bearbeitet wird. Siehe ["Referenz für Netzwerk-Ports"](#).

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch ["Konfigurieren Sie Speicher-Proxy-Einstellungen"](#) Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

VLANs und Plattform-Services und Cloud-Storage-Pools

VLAN-Netzwerke können nicht für Plattformservices oder Cloud Storage-Pools verwendet werden. Die Zielpunkte müssen über das Raster, den Administrator oder das Client-Netzwerk erreichbar sein.

Appliance-Nodes

Die Netzwerk-Ports auf StorageGRID Applikationen können so konfiguriert werden, dass die Port Bond-Modi verwendet werden, die den Anforderungen an Durchsatz, Redundanz und Failover entsprechen.

Die 10/25-GbE-Ports auf den StorageGRID Appliances können im Bond-Modus „Fest“ oder „Aggregat“ für Verbindungen zum Grid-Netzwerk und zum Client-Netzwerk konfiguriert werden.

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

Weitere Informationen zu den Port-Bond-Modi Ihrer Appliance finden Sie unter:

- ["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 Node-Bereitstellung und der Grid-Konfiguration verwendet werden.

Erste Implementierung eines Node

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

Ein Grid-Netzwerk mit einem konfigurierten Gateway wird während der Bereitstellung zum Standard-Gateway für einen Node. Das Standard-Gateway ermöglicht Grid-Knoten in separaten Subnetzen, mit dem primären Admin-Node zu kommunizieren, bevor das Grid konfiguriert wurde.

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

Automatische Knotenregistrierung mit primärem Admin-Node

Nach der Bereitstellung der Nodes registrieren sie sich mit dem primären Admin-Node über das Grid-Netzwerk. Sie können dann den Grid Manager verwenden, das `configure-storagegrid.py` Python-Skript oder die Installations-API, um das Grid zu konfigurieren und die registrierten Nodes zu genehmigen. Während der Grid-Konfiguration können Sie mehrere Grid-Subnetze konfigurieren. Beim Abschluss der Grid-Konfiguration werden auf jedem Knoten statische Routen zu diesen Subnetzen über das Grid-Netzwerk-Gateway erstellt.

Deaktivieren des Admin-Netzwerks oder des Client-Netzwerks

Wenn Sie das Admin-Netzwerk oder das Client-Netzwerk deaktivieren möchten, können Sie die Konfiguration während des Node-Genehmigungsprozesses von ihnen entfernen oder das Change IP-Tool verwenden, nachdem die Installation abgeschlossen ist (siehe ["Konfigurieren Sie IP-Adressen"](#)).

Richtlinien nach der Installation

Befolgen Sie nach Abschluss der Implementierung und Konfiguration des Grid-Node die folgenden Richtlinien für DHCP-Adressen und Änderungen der Netzwerkkonfiguration.

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

Sie können DHCP nur während der Bereitstellungsphase einrichten. DHCP kann während der Konfiguration nicht eingerichtet werden.



Nodes werden neu gebootet, wenn sich ihre IP-Adressen ändern. Dies kann zu Ausfällen führen, wenn sich eine DHCP-Adresse gleichzeitig auf mehrere Nodes auswirkt.

- Sie müssen die Verfahren zum Ändern der IP-Adresse verwenden, wenn Sie IP-Adressen, Subnetzmaske und Standard-Gateways für einen Grid-Node ändern möchten. Siehe ["Konfigurieren Sie IP-Adressen"](#).

- Wenn Sie Änderungen an der Netzwerkkonfiguration vornehmen, einschließlich Routing- und Gateway-Änderungen, geht die Client-Verbindung zum primären Admin-Node und anderen Grid-Nodes unter Umständen verloren. Je nach den vorgenommenen Änderungen müssen Sie diese Verbindungen möglicherweise erneut herstellen.

Referenz für Netzwerk-Ports

Sie müssen sicherstellen, dass die Netzwerkinfrastruktur interne und externe Kommunikation zwischen Knoten innerhalb des Grid und externen Clients und Services ermöglicht. Möglicherweise benötigen Sie Zugriff über interne und externe Firewalls, Switching-Systeme und Routing-Systeme.

Verwenden Sie die Details für ["Interne Kommunikation mit Grid-Nodes"](#) Und ["Externe Kommunikation"](#) Um zu bestimmen, wie die einzelnen erforderlichen Ports konfiguriert werden.

Interne Kommunikation mit Grid-Nodes

Die interne StorageGRID Firewall ermöglicht eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. Verbindungen werden auch an Ports akzeptiert, die durch Load Balancer-Endpunkte definiert wurden.



NetApp empfiehlt, ICMP (Internet Control Message Protocol)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Wenn ICMP-Datenverkehr zugelassen wird, kann die Failover-Performance verbessert werden, 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 IP-Protokoll Nummer 112 verwendet. StorageGRID verwendet VRRP nur im Unicast-Modus. VRRP ist nur erforderlich, wenn ["Hochverfügbarkeitsgruppen"](#) Werden konfiguriert.

Richtlinien für Linux-basierte Knoten

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können Sie Ports während der Bereitstellung mithilfe eines Konfigurationsparameters neu zuordnen. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unter:

- ["Installieren Sie StorageGRID unter Red hat Enterprise Linux"](#)
- ["Installieren Sie StorageGRID auf Ubuntu oder Debian"](#)

Richtlinien für VMware-basierte Nodes

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

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie bei der Implementierung von Nodes mit dem VMware vSphere Web Client Ports neu zuordnen oder bei der Automatisierung der Grid Node-Bereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unter ["Installieren Sie StorageGRID auf VMware"](#).

Richtlinien für Appliance-Nodes

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Siehe ["Optional: Netzwerkports für Appliance neu zuordnen"](#).

Interne StorageGRID-Ports

| Port | TCP oder UDP | Von | Bis | Details |
|------|--------------|---------------------|-----------------------|---|
| 22 | TCP | Primärer Admin-Node | Alle Nodes | Bei Wartungsarbeiten muss der primäre Admin-Node mit SSH am Port 22 mit allen anderen Nodes kommunizieren können. Das Aktivieren von SSH-Datenverkehr von anderen Nodes ist optional. |
| 80 | TCP | Appliances | Primärer Admin-Node | Verwendet von StorageGRID-Appliances, um mit dem primären Admin-Knoten zu kommunizieren, um die Installation zu starten. |
| 123 | UDP | Alle Nodes | Alle Nodes | Netzwerkzeitprotokolldienst. Jeder Node synchronisiert seine Zeit mithilfe von NTP mit jedem anderen Node. |
| 443 | TCP | Alle Nodes | Primärer Admin-Node | Wird zur Kommunikation des Status an den primären Admin-Knoten während der Installation und anderen Wartungsverfahren verwendet. |
| 1055 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren. |
| 1139 | TCP | Storage-Nodes | Storage-Nodes | Interner Datenverkehr zwischen Speicherknoten. |
| 1501 | TCP | Alle Nodes | Storage-Nodes mit ADC | Reporting-, Audit- und Konfigurationsdatenverkehr. |
| 1502 | TCP | Alle Nodes | Storage-Nodes | Interner S3- und Swift-Datenverkehr. |
| 1504 | TCP | Alle Nodes | Admin-Nodes | NMS-Service-Berichterstellung und interner Datenverkehr bei der Konfiguration. |
| 1505 | TCP | Alle Nodes | Admin-Nodes | AMS-Dienst internen Verkehr. |
| 1506 | TCP | Alle Nodes | Alle Nodes | Serverstatus interner Datenverkehr. |

| Port | TCP oder UDP | Von | Bis | Details |
|-------|--------------|---------------------|---------------------|---|
| 1507 | TCP | Alle Nodes | Gateway-Nodes | Interner Datenverkehr des Load Balancer: |
| 1508 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr im Konfigurationsmanagement. |
| 1509 | TCP | Alle Nodes | Archiv-Nodes | Interner Datenverkehr des Archivierungs-Knotens. |
| 1511 | TCP | Alle Nodes | Storage-Nodes | Interner Metadaten-Datenverkehr: |
| 5353 | UDP | Alle Nodes | Alle Nodes | <p>Bietet den Multicast-DNS-Dienst (mDNS), der für IP-Änderungen im gesamten Netzwerk und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.</p> <p>Hinweis: Die Konfiguration dieses Ports ist optional.</p> |
| 7001 | TCP | Storage-Nodes | Storage-Nodes | Cassandra TLS zwischen Nodes-Cluster-Kommunikation |
| 7443 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung. |
| 8011 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren. |
| 8443 | TCP | Primärer Admin-Node | Appliance-Nodes | Interner Datenverkehr im Zusammenhang mit dem Wartungsmodus. |
| 9042 | TCP | Storage-Nodes | Storage-Nodes | Cassandra-Client-Port: |
| 9999 | TCP | Alle Nodes | Alle Nodes | Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsvorgänge, Kennzahlen und Netzwerk-Updates. |
| 10226 | TCP | Storage-Nodes | Primärer Admin-Node | Wird von StorageGRID Appliances für die Weiterleitung von AutoSupport-Paketen vom E-Series SANtricity System Manager zum primären Admin-Node verwendet. |

| Port | TCP oder UDP | Von | Bis | Details |
|-------|--------------|-----------------------------|-----------------------------|--|
| 10342 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren. |
| 11139 | TCP | Archivierung /Storage-Nodes | Archivierung /Storage-Nodes | Interner Datenverkehr zwischen Speicherknoten und Archivknoten. |
| 18000 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Kontodienst, interner Datenverkehr. |
| 18001 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Interner Datenverkehr der Identitätsföderation. |
| 18002 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner API-Traffic im Zusammenhang mit Objektprotokollen. |
| 18003 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Plattform Dienste internen Traffic. |
| 18017 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner Datenverkehr des Data Mover-Service für Cloud-Speicherpools. |
| 18019 | TCP | Storage-Nodes | Storage-Nodes | Interner Traffic beim Chunk-Service für Erasure Coding. |
| 18082 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner S3-Datenverkehr. |
| 18083 | TCP | Alle Nodes | Storage-Nodes | Swift-bezogener interner Traffic: |
| 18086 | TCP | Alle Grid-Nodes | Alle Storage-Nodes | Interner Datenverkehr im Zusammenhang mit dem LDR-Dienst. |
| 18200 | TCP | Admin/Storage-Nodes | Storage-Nodes | Weitere Statistiken zu Client-Anforderungen. |
| 19000 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Keystone-Service: Interner Datenverkehr. |

Verwandte Informationen

Externe Kommunikation

Die Clients müssen mit den Grid-Nodes kommunizieren, um Inhalte aufzunehmen und abzurufen. Die verwendeten Ports hängen von den ausgewählten Objekt-Storage-Protokollen ab. Diese Ports müssen dem Client zugänglich sein.

Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf beliebige Ports einschränken, können Sie dies verwenden ["Load Balancer-Endpunkte"](#) Um den Zugriff auf benutzerdefinierte Ports zu erlauben.

Port-Neuzuordnung

Um Systeme und Protokolle wie SMTP, DNS, SSH oder DHCP verwenden zu können, müssen Sie beim Implementieren von Nodes Ports neu zuordnen. Sie sollten jedoch die Load Balancer-Endpunkte nicht neu zuordnen. Informationen zur Port-Neuzuordnung finden Sie in den Installationsanweisungen:

- ["Installieren Sie StorageGRID unter Red hat Enterprise Linux"](#)
- ["Installieren Sie StorageGRID auf Ubuntu oder Debian"](#)
- ["Installieren Sie StorageGRID auf VMware"](#)
- ["Optional: Netzwerkports für Appliance neu zuordnen"](#)

Anschlüsse für externe Kommunikation

In der folgenden Tabelle werden die Ports für den Datenverkehr zu den Nodes aufgeführt.



Diese Liste enthält keine Ports, die als konfiguriert werden können ["Load Balancer-Endpunkte"](#).

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-----------|----------------|---------------|---|
| 22 | TCP | SSH | Service-Laptop | Alle Nodes | Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden. |
| 25 | TCP | SMTP | Admin-Nodes | E-Mail-Server | Wird für Warnungen und E-Mail-basierte AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 über die Seite „E-Mail-Server“ außer Kraft setzen. |
| 53 | TCP/UDP | DNS | Alle Nodes | DNS-Server | Wird für DNS verwendet. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-----------|-----------------------|--------------|--|
| 67 | UDP | DHCP | Alle Nodes | DHCP-Service | Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für statisch konfigurierte Grids ausgeführt. |
| 68 | UDP | DHCP | DHCP-Service | Alle Nodes | Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für Raster ausgeführt, die statische IP-Adressen verwenden. |
| 80 | TCP | HTTP | Browser | Admin-Nodes | Port 80 wird für die Admin-Node-Benutzeroberfläche an Port 443 umgeleitet. |
| 80 | TCP | HTTP | Browser | Appliances | Port 80 wird für das Installationsprogramm der StorageGRID-Appliance an Port 8443 umgeleitet. |
| 80 | TCP | HTTP | Storage-Nodes mit ADC | AWS | Wird für Plattform-Services-Meldungen verwendet, die an AWS oder andere externe Services gesendet werden, die HTTP verwenden. Mandanten können bei der Erstellung eines Endpunkts die Standard-HTTP-Porteinstellung von 80 außer Kraft setzen. |
| 80 | TCP | HTTP | Storage-Nodes | AWS | An AWS Ziele mit HTTP gesendete Anfragen von Cloud-Storage-Pools Grid-Administratoren können die Standard-HTTP-Port-Einstellung von 80 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen. |
| 111 | TCP/UDP | Rpcbind | NFS Client | Admin-Nodes | <p>Wird vom NFS-basierten Audit-Export verwendet (Portmap).</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist.</p> <p>Hinweis: die Unterstützung für NFS wurde veraltet und wird in einer zukünftigen Version entfernt.</p> |
| 123 | UDP | NTP | Primäre NTP-Knoten | Externe NTP | Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-----------|-------------|-------------|--|
| 137 | UDP | NetBIOS | SMB-Client | Admin-Nodes | <p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn SMB-basierter Audit-Export aktiviert ist.</p> |
| 138 | UDP | NetBIOS | SMB-Client | Admin-Nodes | <p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn SMB-basierter Audit-Export aktiviert ist.</p> |
| 139 | TCP | SMB | SMB-Client | Admin-Nodes | <p>Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn SMB-basierter Audit-Export aktiviert ist.</p> |
| 161 | TCP/UDP | SNMP | SNMP-Client | Alle Nodes | <p>Wird für SNMP-Abfrage verwendet. Alle Knoten stellen grundlegende Informationen zur Verfügung; Admin Nodes stellen auch Alarm- und Alarmdaten zur Verfügung. Standardmäßig auf UDP-Port 161 gesetzt, wenn konfiguriert.</p> <p>Hinweis: dieser Port ist nur erforderlich und wird nur auf der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p> |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-------------------------|-----------------------|------------------------|--|
| 162 | TCP/UDP | SNMP-Benachrichtigungen | Alle Nodes | Benachrichtigungsziele | <p>Ausgehende SNMP-Benachrichtigungen und Traps standardmäßig auf UDP-Port 162.</p> <p>Hinweis: dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p> |
| 389 | TCP/UDP | LDAP | Storage-Nodes mit ADC | Active Directory/LDAP | Wird zur Verbindung mit einem Active Directory- oder LDAP-Server für Identity Federation verwendet. |
| 443 | TCP | HTTPS | Browser | Admin-Nodes | <p>Wird von Webbrowsern und Management-API-Clients für den Zugriff auf Grid Manager und Tenant Manager verwendet.</p> <p>Hinweis: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port angeschlossen sind, einschließlich Ihnen, den Zugriff auf den Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Konfigurieren Sie die Firewall-Steuererelemente" So konfigurieren Sie privilegierte IP-Adressen:</p> |
| 443 | TCP | HTTPS | Admin-Nodes | Active Directory | Wird von Admin-Nodes verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist. |
| 443 | TCP | HTTPS | Archiv-Nodes | Amazon S3 | Wird für den Zugriff von Archiv-Nodes auf Amazon S3 verwendet. |
| 443 | TCP | HTTPS | Storage-Nodes mit ADC | AWS | Wird für Plattform-Services-Nachrichten verwendet, die an AWS oder andere externe Services gesendet werden, die HTTPS verwenden. Mandanten können beim Erstellen eines Endpunkts die Standard-HTTP-Porteinstellung 443 außer Kraft setzen. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-----------|----------------|-------------|---|
| 443 | TCP | HTTPS | Storage-Nodes | AWS | Cloud-Storage-Pools-Anfragen werden an AWS-Ziele mit HTTPS gesendet. Grid-Administratoren können die HTTPS-Porteinstellung von 443 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen. |
| 445 | TCP | SMB | SMB-Client | Admin-Nodes | Wird vom SMB-basierten Audit-Export verwendet. Hinweis: dieser Port ist nur erforderlich, wenn SMB-basierter Audit-Export aktiviert ist. |
| 903 | TCP | NFS | NFS Client | Admin-Nodes | Wird vom NFS-basierten Audit-Export verwendet (<code>rpc.mountd</code>). Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist. Hinweis: die Unterstützung für NFS wurde veraltet und wird in einer zukünftigen Version entfernt. |
| 2022 | TCP | SSH | Service-Laptop | Alle Nodes | Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie statt 2022 auch Port 22 verwenden. |
| 2049 | TCP | NFS | NFS Client | Admin-Nodes | Wird vom NFS-basierten Audit-Export verwendet (<code>nfs</code>). Hinweis: dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist. Hinweis: die Unterstützung für NFS wurde veraltet und wird in einer zukünftigen Version entfernt. |
| 5353 | UDP | MDNS | Alle Nodes | Alle Nodes | Bietet den Multicast-DNS-Dienst (mDNS), der für IP-Änderungen im gesamten Netzwerk und für die Ermittlung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird. Hinweis: Die Konfiguration dieses Ports ist optional. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|------|--------------|-----------|--------------------------|-------------|---|
| 5696 | TCP | KMIP | Appliance | KMS | KMIP (Key Management Interoperability Protocol): Externer Datenverkehr von Appliances, die für die Node-Verschlüsselung auf den Verschlüsselungsmanagement-Server (Key Management Interoperability Protocol) konfiguriert sind, es sei denn, ein anderer Port wird auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer angegeben. |
| 8022 | TCP | SSH | Service-Laptop | Alle Nodes | SSH auf Port 8022 gewährt Zugriff auf das Betriebssystem auf Appliance- und virtuellen Node-Plattformen zur Unterstützung und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare Metal-)Nodes verwendet und muss nicht zwischen Grid-Nodes oder während des normalen Betriebs zugänglich sein. |
| 8443 | TCP | HTTPS | Browser | Admin-Nodes | <p>Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden.</p> <p>Hinweis: Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port angeschlossen sind, einschließlich Ihnen, den Zugriff auf den Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt. Siehe "Konfigurieren Sie die Firewall-Steuerelemente" So konfigurieren Sie privilegierte IP-Adressen:</p> |
| 9022 | TCP | SSH | Service-Laptop | Appliances | Gewährt Zugriff auf StorageGRID Appliances im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss während des normalen Betriebs nicht zwischen Grid-Nodes oder auf diesen zugreifen können. |
| 9091 | TCP | HTTPS | Externer Grafana-Service | Admin-Nodes | <p>Wird von externen Grafana Services für sicheren Zugriff auf den StorageGRID Prometheus Service verwendet.</p> <p>Hinweis: dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.</p> |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|-------------|--------------|-----------|--|--|--|
| 9092 | TCP | Kafka | Storage-Nodes mit ADC | Kafka-Cluster | Wird für Meldungen über Plattformdienste verwendet, die an ein Kafka-Cluster gesendet werden. Mandanten können beim Erstellen eines Endpunkts die Standard-Kafka-Porteinstellung 9092 außer Kraft setzen. |
| 9443 | TCP | HTTPS | Browser | Admin-Nodes | Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Mandanten-Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden. |
| 18082 | TCP | HTTPS | S3-Clients | Storage-Nodes | S3-Client-Datenverkehr direkt zu Storage-Nodes (HTTPS). |
| 18083 | TCP | HTTPS | Swift Clients | Storage-Nodes | Schneller Client-Verkehr direkt zu Storage Nodes (HTTPS). |
| 18084 | TCP | HTTP | S3-Clients | Storage-Nodes | S3-Client-Traffic direkt zu Storage-Nodes (HTTP). |
| 18085 | TCP | HTTP | Swift Clients | Storage-Nodes | Swift-Client-Datenverkehr direkt zu Storage-Nodes (HTTP). |
| 23000-23999 | TCP | HTTPS | Alle Nodes im Quell-Grid für die Grid-übergreifende Replizierung | Admin Nodes und Gateway Nodes im Ziel-Grid für Grid-übergreifende Replizierung | Dieser Port-Bereich ist für Grid Federation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden den gleichen 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 IRGEND EINER 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.