網路準則
StorageGRID 11.5

NetApp
April 11, 2024

目錄

網路準則

深入瞭解StorageGRID 架構與網路拓撲。熟悉網路組態和資源配置的需求。

- "網路概述StorageGRID"
- "網路需求與準則"
- "部署特定的網路考量"
- "網路安裝與資源配置"
- "安裝後準則"
- "網路連接埠參考"

網路概述StorageGRID

若要設定StorageGRID 適用於某個效能不穩定系統的網路功能、需要具備乙太網路交換、TCP/IP網路、子網路、網路路由和防火牆等豐富經驗。

在您設定網路之前、請先熟悉StorageGRID _網格入門_中所述的功能。

在部署和設定StorageGRID 靜態之前、您必須先設定網路基礎架構。需要在網格中的所有節點之間、以及網格與外部用戶端和服務之間進行通訊。

外部用戶端和外部服務需要連線StorageGRID 至無法分享的網路、才能執行下列功能：

- 儲存及擷取物件資料
- 接收電子郵件通知
- 存取StorageGRID 功能完善的管理介面（Grid Manager與Tenant Manager）
- 存取稽核共用區（選用）
- 提供下列服務：
  - 網路時間傳輸協定（NTP）
  - 網域名稱系統（DNS）
  - 金鑰管理伺服器（KMS）

必須適當設定以處理這些功能及其他功能的流量。StorageGRID

在您決定要StorageGRID 使用哪三個資訊網、以及如何設定這些網路之後、StorageGRID 您可以依照適當的指示來安裝及設定這些節點。

相關資訊

"網格入門指南"

"管理StorageGRID"

"版本資訊"

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

"安裝VMware"

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"

網路類型StorageGRID

系統中的網格節點StorageGRID 會處理_GRID交通量_、*admin*交通量_和_*Client*交通量。您必須適當設定網路、以管理這三種流量類型、並提供控制與安全性。

流量類型

流量類型	說明	網路類型
網格流量	在網格中所有節點之間傳輸的內部StorageGRID 不完整流量。所有網格節點都必須能夠透過此網路與所有其他網格節點通訊。	網格網路（必填）
管理流量	用於系統管理與維護的流量。	管理網路（選用）
用戶端流量	在外部用戶端應用程式和網格之間傳輸的流量、包括S3和Swift用戶端的所有物件儲存要求。	用戶端網路（選用）

您可以使用下列方式設定網路：

- 僅限網格網路
- 網格和管理網路
- 網格和用戶端網路
- 網格、管理和用戶端網路

Grid Network是強制性的、可管理所有的網格流量。安裝時可納入管理網路和用戶端網路、或是稍後新增、以因應需求變更。雖然管理網路和用戶端網路是選用的、但當您使用這些網路來處理管理和用戶端流量時、網格網路可以隔離且安全無虞。

網路介面

使用下列特定介面將各個節點連線至各個網路：StorageGRID

網路	介面名稱
網格網路（必填）	eth0
管理網路（選用）	eth1
用戶端網路（選用）	eth2

如需將虛擬或實體連接埠對應至節點網路介面的詳細資訊、請參閱安裝說明。

您必須為節點上啟用的每個網路設定下列項目：

- IP 位址
- 子網路遮罩
- 閘道 IP 位址

您只能為每個網格節點上的三個網路中的每個網路設定一個IP位址/遮罩/閘道組合。如果您不想為網路設定閘道、應該使用IP位址作為閘道位址。

高可用度（HA）群組可將虛擬IP位址新增至Grid或Client Network介面。如需詳細資訊、請參閱《關於管理StorageGRID 功能的說明》。

網格網路

網格網路為必填項目。它用於所有內部StorageGRID 的資訊流量。Grid Network可在網格中的所有節點之間、跨所有站台和子網路提供連線功能。Grid Network上的所有節點都必須能夠與所有其他節點通訊。Grid Network可由多個子網路組成。包含關鍵網格服務（例如NTP）的網路也可新增為網格子網路。

不支援節點之間的網路位址轉譯（NAT）StorageGRID 。

即使已設定管理網路和用戶端網路、網格網路仍可用於所有管理流量和所有用戶端流量。除非節點已設定用戶端網路、否則Grid Network閘道是節點的預設閘道。

設定Grid Network時、您必須確保網路受到不受信任用戶端的保護、例如開放式網際網路上的用戶端。

請注意Grid Network的下列需求與詳細資料：

- 如果有多個網格子網路、則必須設定網格網路閘道。
- 網格網路閘道是節點的預設閘道、直到網格組態完成為止。
- 所有節點的靜態路由都會自動產生、以到達全域網格網路子網路清單中所設定的所有子網路。
- 如果新增了用戶端網路、則當網格組態完成時、預設閘道會從網格網路閘道切換至用戶端網路閘道。

管理網路

管理網路為選用網路。設定後、即可用於系統管理和維護流量。管理網路通常是私有網路、不需要在節點之間進行路由傳送。

您可以選擇哪些網格節點應啟用管理網路。

透過管理網路、管理和維護流量不需要跨越Grid Network。管理網路的一般用途包括存取Grid Manager使用者介面、存取NTP、DNS、外部金鑰管理（KMS）和輕量型目錄存取傳輸協定（LDAP）等關鍵服務、存取管理節點上的稽核記錄、以及存取安全Shell傳輸協定（SSH）以進行維護和支援。

管理網路絕不用於內部網格流量。系統會提供管理網路閘道、並允許管理網路與多個外部子網路通訊。不過、管理網路閘道永遠不會用作節點的預設閘道。

請注意管理網路的下列需求與詳細資料：

- 如果要從管理網路子網路外部建立連線、或是設定了多個管理網路子網路、則需要管理網路閘道。
- 會針對節點的管理網路子網路清單中所設定的每個子網路建立靜態路由。

用戶端網路

用戶端網路為選用項目。設定後、可讓使用者存取S3和Swift等用戶端應用程式的網格服務。如果您計畫讓StorageGRID 外部資源（例如雲端儲存資源池或StorageGRID CloudMirror複寫服務）能夠存取這些資料、則外部資源也可以使用用戶端網路。網格節點可透過用戶端網路閘道與任何可連線的子網路進行通訊。

您可以選擇哪些網格節點上應該啟用「用戶端網路」。所有節點不一定都位於同一個用戶端網路、而且節點永遠不會透過用戶端網路彼此通訊。在網格安裝完成之前、用戶端網路不會運作。

為了增加安全性、您可以指定節點的用戶端網路介面不受信任、以便用戶端網路對允許的連線有更多限制。如果節點的用戶端網路介面不受信任、介面會接受傳出連線、例如CloudMirror複寫所使用的連線、但只接受已明確設定為負載平衡器端點之連接埠上的傳入連線。如需不受信任用戶端網路功能和負載平衡器服務的詳細資訊、請參閱《關於管理StorageGRID 》的指示。

當您使用用戶端網路時、用戶端流量不需要跨越Grid Network。網格網路流量可分隔至安全、不可路由的網路。下列節點類型通常是以用戶端網路進行設定：

- 閘道節點、因為這些節點可讓您存取StorageGRID 「動態負載平衡器」服務、以及S3和Swift用戶端存取網格。
- 儲存節點、因為這些節點可存取S3和Swift傳輸協定、雲端儲存資源池和CloudMirror複寫服務。
- 管理節點、確保租戶使用者無需使用管理網路即可連線至租戶管理程式。

請注意以下有關用戶端網路的資訊：

- 如果已設定用戶端網路、則需要用戶端網路閘道。
- 當網格組態完成時、用戶端網路閘道會成為網格節點的預設路由。

相關資訊

"網路需求與準則"

"管理StorageGRID"

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

"安裝VMware"

網路拓撲範例

除了所需的Grid Network之外、您也可以選擇在設計單一或多站台部署的網路拓撲時、是否要設定管理網路和用戶端網路介面。

內部連接埠只能透過Grid Network存取。外部連接埠可從所有網路類型存取。這種靈活度提供多種選項、可設計StorageGRID 出一套功能豐富的功能、並在交換器和防火牆中設定外部IP和連接埠篩選功能。如需內部和外部連接埠的詳細資訊、請參閱網路連接埠參考。

如果您指定節點的用戶端網路介面不受信任、請設定負載平衡器端點以接受傳入流量。如需設定不受信任的用戶端網路和負載平衡器端點的相關資訊、請參閱《管理StorageGRID 》。

相關資訊

"管理StorageGRID"

"網路連接埠參考"

網格網路拓撲

最簡單的網路拓撲是透過僅設定Grid Network來建立。

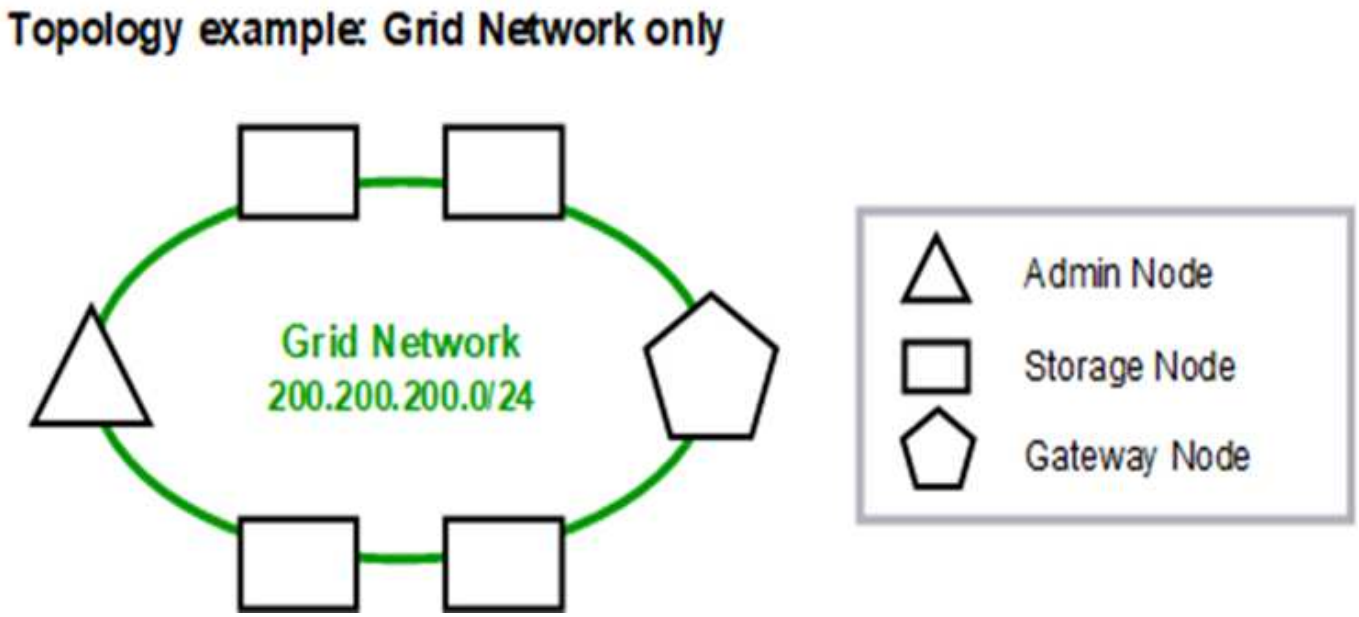
當您設定Grid Network時、會為每個網格節點的eth0介面建立主機IP位址、子網路遮罩和閘道IP位址。

在組態期間、您必須將所有網格網路子網路新增至網格網路子網路清單（GNSL）。此清單包含所有站台的所有子網路、也可能包含外部子網路、可讓您存取NTP、DNS或LDAP等關鍵服務。

安裝時、Grid Network介面會針對GNSL中的所有子網路套用靜態路由、並設定節點通往Grid Network閘道的預設路由（如果已設定）。如果沒有用戶端網路、而Grid Network閘道是節點的預設路由、則不需要GNSL。也會產生通往網格中所有其他節點的主機路由。

在此範例中、所有流量都會共用相同的網路、包括S3和Swift用戶端要求的相關流量、以及管理和維護功能。

> 此拓撲適用於無法在外部使用、概念驗證或測試部署的單一站台部署、或是當協力廠商負載平衡器做為用戶端存取界限時。如有可能、網格網路應僅用於內部流量。管理網路和用戶端網路都有額外的防火牆限制、可封鎖外部的內部服務流量。支援將Grid Network用於外部用戶端流量、但這種使用方式可提供較少的保護層。



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

管理網路拓撲

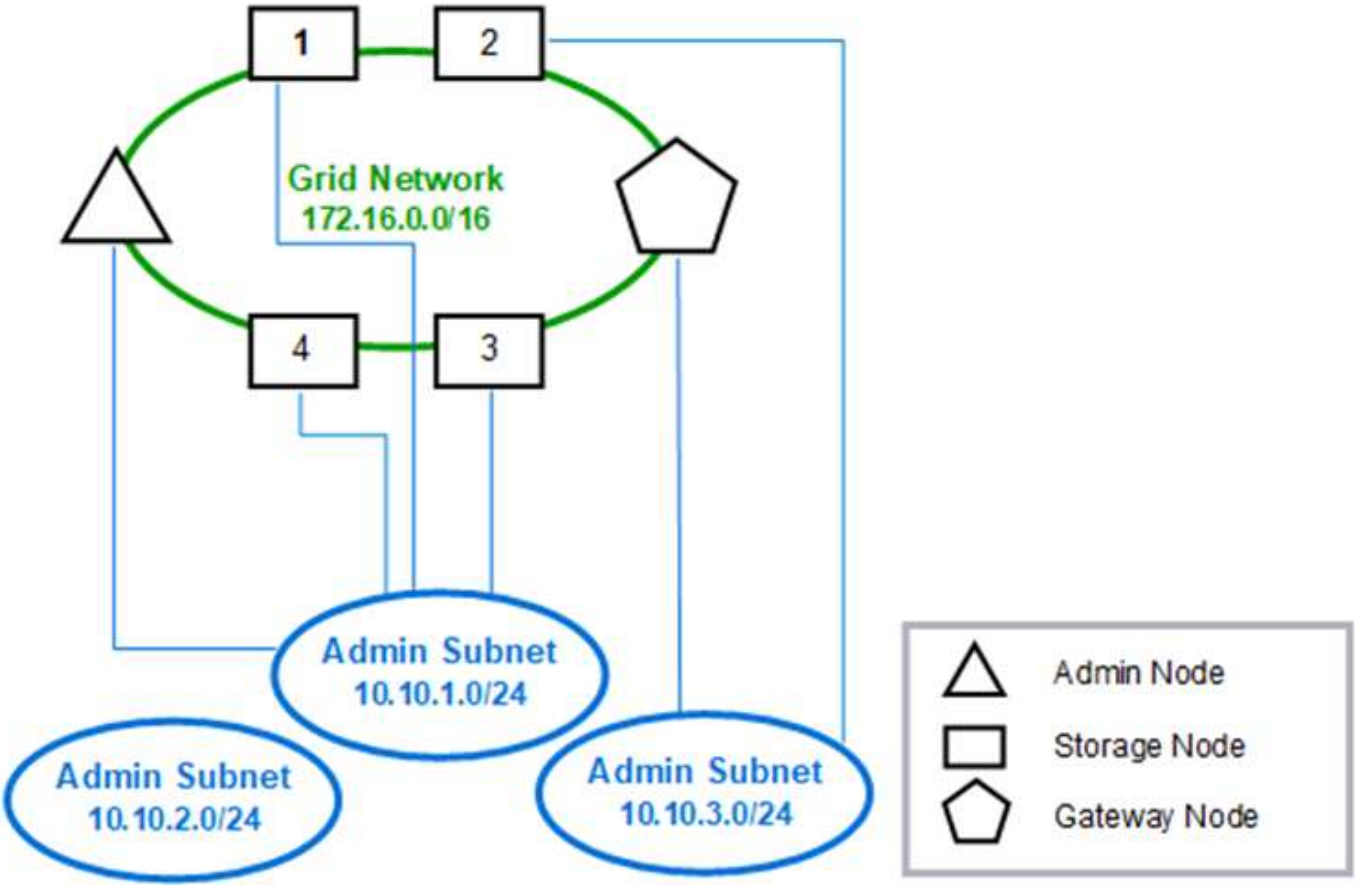
擁有管理網路是選擇性的。使用管理網路和網格網路的其中一種方法、就是為每個節點設定可路由的網格網路和有邊界的管理網路。

當您設定管理網路時、會為每個網格節點的eth1介面建立主機IP位址、子網路遮罩和閘道IP位址。

管理網路可為每個節點唯一、並可由多個子網路組成。每個節點均可設定管理外部子網路清單（Aesl）。Aesl會列出每個節點可透過管理網路連線的子網路。Aesl也必須包含網格透過管理網路存取的任何服務子網路、例如NTP、DNS、KMS和LDAP。靜態路由會套用至Aesl中的每個子網路。

在此範例中、Grid Network用於與S3和Swift用戶端要求和物件管理相關的流量。而管理網路則用於管理功能。

Topology example: Grid and Admin Networks



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

用戶端網路拓撲

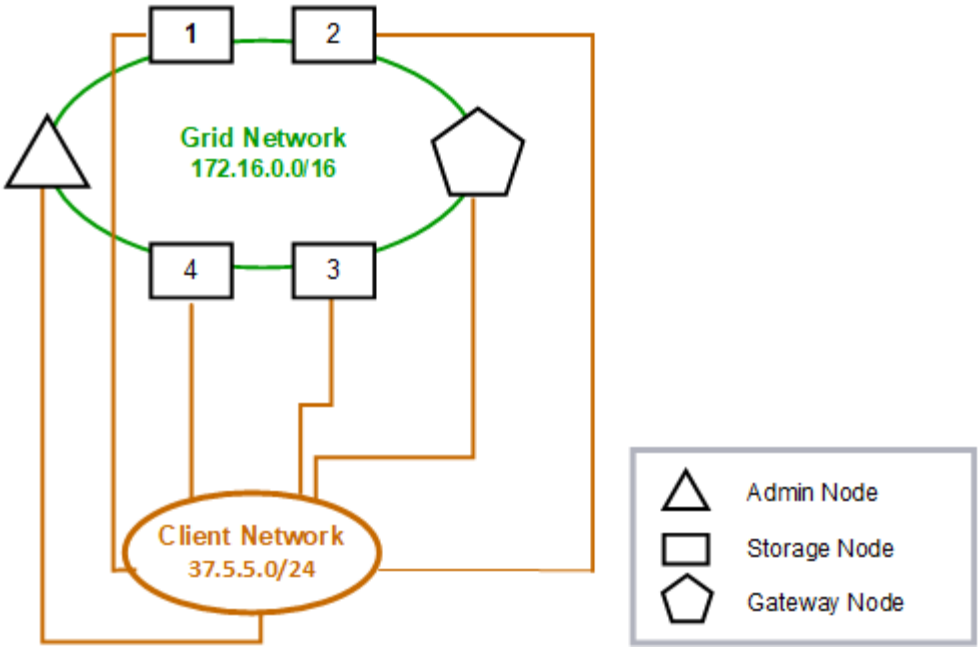
擁有用戶端網路為選用功能。使用用戶端網路可將用戶端網路流量（例如S3和Swift）與網格內部流量區隔、讓網格網路更安全。未設定管理網路時、用戶端或網格網路均可處理管理流量。

當您設定用戶端網路時、會為所設定節點的eth2介面建立主機IP位址、子網路遮罩和閘道IP位址。每個節點的用戶端網路可以獨立於任何其他節點上的用戶端網路。

如果您在安裝期間為節點設定用戶端網路、節點的預設閘道會在安裝完成時從Grid Network閘道切換至Client Network閘道。如果稍後新增用戶端網路、則節點的預設閘道交換器會採用相同的方式。

在此範例中、用戶端網路用於S3和Swift用戶端要求及管理功能、而Grid Network則用於內部物件管理作業。

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network 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

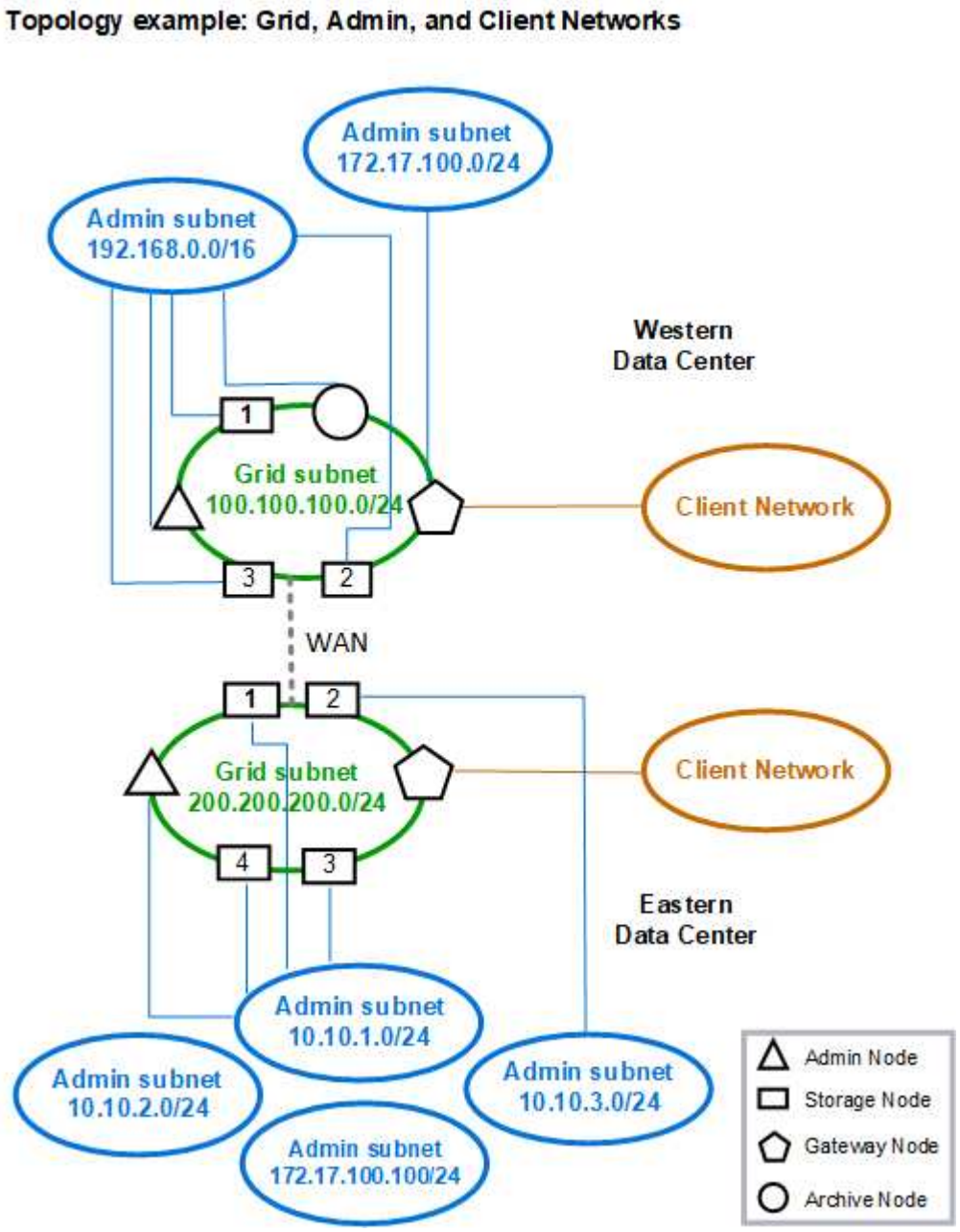
三個網路的拓撲

您可以將這三個網路設定為一個網路拓撲、其中包含私有網格網路、限定站台專屬的管理網路和開放式用戶端網路。使用負載平衡器端點和不受信任的用戶端網路、可視需要提供

額外的安全性。

在此範例中：

- Grid Network用於與內部物件管理作業相關的網路流量。
- 管理網路用於與管理功能相關的流量。
- 用戶端網路用於與S3和Swift用戶端要求相關的流量。



網路需求

您必須驗證目前的網路基礎架構和組態是否可支援計畫StorageGRID 性的網路設計。

一般網路需求

所有StorageGRID 的支援部署都必須能夠支援下列連線。

這些連線可透過Grid、Admin或Client Networks進行、或是如網路拓撲範例所示的這些網路組合。

- 管理連線：系統管理員與節點之間的傳入連線、通常是透過SSH。網頁瀏覽器可存取Grid Manager、租戶管理程式及StorageGRID 《NetApp應用裝置安裝程式」。
- * NTP伺服器連線*：接收傳入udp回應的傳出udp連線。

  主要管理節點必須至少能連線到一部NTP伺服器。

- * DNS伺服器連線*：接收傳入udp回應的傳出udp連線。
- * LDAP/Active Directory伺服器連線*：儲存節點上身分識別服務的傳出TCP連線。
- 《》：從管理節點到eithersupport.netapp.com或客戶設定的Proxy的輸出TCP連線AutoSupport 。
- 外部金鑰管理伺服器：從每個應用裝置節點連出TCP連線、並啟用節點加密。
- 來自S3和Swift用戶端的傳入TCP連線。
- 來自諸如Cloud Mirror複寫或來自Cloud Storage Pool等平台服務的傳出要求StorageGRID 。

如果StorageGRID 使用預設路由規則無法聯絡任何已配置的NTP或DNS伺服器、只要指定DNS和NTP伺服器的IP位址、它就會自動嘗試聯絡所有網路（Grid、Admin和Client）。如果可以在任何網路上連線到NTP或DNS伺服器、StorageGRID 則會自動建立額外的路由規則、以確保未來所有連線的嘗試都會使用網路。

> 雖然您可以使用這些自動探索的主機路由、但一般而言、您應該手動設定DNS和NTP路由、以確保自動探索失敗時的連線能力。

如果您尚未準備好在部署期間設定選用的管理和用戶端網路、則可在設定步驟期間核准網格節點時設定這些網路。此外、您也可以在安裝完成後、使用「變更IP」工具來設定這些網路、如還原與維護指示所述。

管理節點和閘道節點的連線

管理節點必須始終受到不受信任用戶端（例如開放式網際網路上的用戶端）的保護。您必須確保任何不受信任的用戶端都無法存取Grid Network、管理網路或用戶端網路上的任何管理節點。

您要新增至高可用度群組的管理節點和閘道節點必須設定靜態IP位址。如需管理StorageGRID 功能的說明、請參閱高可用度群組的相關資訊。

使用網路位址轉譯（NAT）

請勿在網格網路上的網格節點之間或StorageGRID 在各個站台之間使用網路位址轉譯（NAT）。當您將私有的IPv4位址用於Grid Network時、這些位址必須從每個站台的每個網格節點直接路由傳送。不過、您可以視需要在外部用戶端和網格節點之間使用NAT、例如為閘道節點提供公有IP位址。只有當您採用對網格中所有節點透明的通道應用程式時、才支援使用NAT來橋接公共網路區段、亦即網格節點不需要知道公有IP位址。

相關資訊

"網格入門指南"

"管理StorageGRID"

網路特定需求

請遵循StorageGRID 每種類型的需求。

網路閘道和路由器

- 如果已設定、則指定網路的閘道必須位於特定網路的子網路內。
- 如果使用靜態定址設定介面、則必須指定0.00.0以外的閘道位址。
- 如果您沒有閘道、最佳做法是將閘道位址設定為網路介面的IP位址。

子網路

每個網路都必須連線至自己的子網路、而不會與節點上的任何其他網路重疊。

下列限制會在部署期間由Grid Manager強制執行。此處提供這些工具、可協助您進行部署前的網路規劃。

- 任何網路IP位址的子網路遮罩不可為255・255・255或255・255・255（CIDR表示法為/31或/32）。
- 網路介面IP位址和子網路遮罩（CIDR）所定義的子網路、不能與同一個節點上所設定的任何其他介面的子網路重疊。
- 每個節點的Grid Network子網路必須包含在GNSL中。
- 管理網路子網路不能與Grid Network子網路、用戶端網路子網路或GNSL中的任何子網路重疊。
- Aesl中的子網路不能與GNSL中的任何子網路重疊。
- 用戶端網路子網路不能與Grid Network子網路、管理網路子網路、GNSL中的任何子網路或Aesl中的任何子網路重疊。

網格網路

- 在部署時、每個網格節點都必須附加至網格網路、而且必須能夠使用部署節點時指定的網路組態與主要管理節點通訊。
- 在正常的網格作業期間、每個網格節點都必須能夠透過網格網路與所有其他網格節點通訊。

  Grid Network必須在每個節點之間直接路由傳送。不支援節點之間的網路位址轉譯（NAT）。

- 如果網格網路由多個子網路組成、請將其新增至網格網路子網路清單（GNSL）。會在GNSL中的每個子網路的所有節點上建立靜態路由。

管理網路

管理網路為選用網路。如果您計畫設定管理網路、請遵循下列要求與準則。

管理網路的一般用途包括管理連線、AutoSupport 功能完善、KMS、連線至關鍵伺服器、例如NTP、DNS和LDAP、如果這些連線並非透過Grid Network或Client Network提供。

只要能夠連線所需的網路服務和用戶端、每個節點都可以使用管理網路和Aesl。

您必須在管理網路上定義至少一個子網路、才能啟用來自外部子網路的傳入連線。在Aesl的每個子網路中、會自動在每個節點上產生靜態路由。

用戶端網路

用戶端網路為選用項目。如果您打算設定用戶端網路、請注意下列考量事項。

用戶端網路的設計可支援來自S3和Swift用戶端的流量。如果已設定、用戶端網路閘道會成為節點的預設閘道。

如果您使用用戶端網路、StorageGRID 只有在明確設定的負載平衡器端點上接受傳入用戶端流量、才能保護不受惡意攻擊的可靠性。如需管理StorageGRID VMware的說明、請參閱有關管理負載平衡和管理不受信任的用戶端網路的資訊。

相關資訊

"管理StorageGRID"

部署特定的網路考量

視您使用的部署平台而定、StorageGRID 您可能需要考量其他有關您的網路設計的考量。

網格節點可部署為：

- 以軟體為基礎的網格節點、部署為VMware vSphere Web Client中的虛擬機器
- 部署在Linux主機上Docker容器內的軟體型網格節點
- 應用裝置型節點

如需網格節點的其他資訊、請參閱_Grid入門指南_。

相關資訊

"網格入門指南"

Linux部署

為了提高效率、可靠性和安全性、StorageGRID 此功能可在Linux上以Docker容器的集合方式執行。不需要StorageGRID 在一個不支援的系統中使用與Docker相關的網路組態。

將非連結裝置（例如VLAN或虛擬乙太網路（varth）配對）用於容器網路介面。將此裝置指定為節點組態檔中的網路介面。

請勿直接使用連結或橋接裝置做為容器網路介面。這樣做可能會因為在Container命名空間中使用含Bond和Bridge裝置的Macvlan時發生核心問題、而導致節點無法啟動。

請參閱Red Hat Enterprise Linux/CentOS或Ubuntu / Debian部署的安裝說明。

相關資訊

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

適用於**Docker**部署的主機網路組態

在StorageGRID Docker Container平台上開始進行非功能性部署之前、請先判斷每個節點將使用哪些網路（Grid、管理、用戶端）。您必須確保每個節點的網路介面都設定在正確的虛擬或實體主機介面上、而且每個網路都有足夠的頻寬。

實體主機

如果您使用實體主機來支援網格節點：

- 確保所有主機都對每個節點介面使用相同的主機介面。此策略可簡化主機組態、並可在未來進行節點移轉。
- 取得實體主機本身的IP位址。

> 主機上的實體介面可由主機本身和主機上執行的一或多個節點使用。使用此介面指派給主機或節點的任何IP位址都必須是唯一的。主機和節點無法共用IP位址。

- 開啟主機所需的連接埠。

建議的最低頻寬

下表提供每種StorageGRID 類型的節點和每種網路類型的最低頻寬建議。您必須為每部實體或虛擬主機配置足夠的網路頻寬、以符合StorageGRID 您計畫在該主機上執行的所有節點數和類型的總頻寬需求。

節點類型	網路類型		
	網格	管理	用戶端
管理	10 Gbps	1 Gbps	1 Gbps
閘道	10 Gbps	1 Gbps	10 Gbps
儲存設備	10 Gbps	1 Gbps	10 Gbps
歸檔	10 Gbps	1 Gbps	10 Gbps

> 此表不包含存取共享儲存設備所需的SAN頻寬。如果您使用透過乙太網路存取的共享儲存設備（iSCSI或FCoE）、則應在每個主機上配置個別的實體介面、以提供足夠的SAN頻寬。為了避免出現瓶頸、特定主機的SAN頻寬應大致符合該主機上執行之所有儲存節點的Aggregate Storage Node網路頻寬。

請根據StorageGRID 您計畫在該主機上執行的各個節點數量和類型、使用表格來判斷每個主機上要配置的網路介面數量下限。

例如、若要在單一主機上執行一個管理節點、一個閘道節點和一個儲存節點：

- 連接管理節點上的網格和管理網路（需要10 + 1 = 11 Gbps）
- 在閘道節點上連接網格和用戶端網路（需要10 + 10 = 20 Gbps）
- 連接儲存節點上的網格網路（需要10 Gbps）

在此案例中、您應提供至少11 + 20 + 10 = 41 Gbps的網路頻寬、 可由兩個40 Gbps介面或五個10 Gbps介面滿足、這些介面可能會集合成主幹、然後由三個以上的VLAN共用、這些VLAN會將Grid、Admin和用戶端子網路裝載到包含主機的實體資料中心。

如需在StorageGRID 您的叢集中的主機上設定實體和網路資源以準備StorageGRID 進行支援的建議方法、請參閱Linux平台安裝說明中有關設定主機網路的資訊。

相關資訊

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

適用於平台服務和雲端儲存資源池的網路和連接埠

如果您計畫使用StorageGRID 支援不支援的平台服務或雲端儲存資源池、則必須設定網格網路和防火牆、以確保能夠到達目的地端點。平台服務包括提供搜尋整合、事件通知及CloudMirror複寫的外部服務。

平台服務需要從儲存節點存取、而儲存節點則是StorageGRID 將此項目裝載到外部服務端點。提供存取的範例包括：

- 在具有ADC服務的儲存節點上、使用Aesl項目來設定唯一的管理網路、這些項目會路由傳送至目標端點。
- 仰賴用戶端網路提供的預設路由。在此範例中、不受信任的用戶端網路功能可用來限制傳入連線。

雲端儲存資源池也需要從儲存節點存取外部服務所提供的端點、例如Amazon S3 Glacier或Microsoft Azure Blob儲存設備。

根據預設、平台服務和雲端儲存資源池通訊會使用下列連接埠：

- **80**：適用於以開頭的端點URI `http`
- * 443*：適用於以開頭的端點URI `https`

建立或編輯端點時、可以指定不同的連接埠。

如果您使用不透明的Proxy伺服器、也必須設定Proxy設定、允許訊息傳送到外部端點、例如網際網路上的端點。請參閱管理StorageGRID 功能、瞭解如何設定Proxy設定。

如需不受信任用戶端網路的詳細資訊、請參閱《關於管理StorageGRID 》的說明。如需平台服務的詳細資訊、請參閱租戶帳戶使用說明。如需Cloud Storage Pool的詳細資訊、請參閱使用資訊生命週期管理來管理物件的指示。

相關資訊

"網路連接埠參考"

"網格入門指南"

"管理StorageGRID"

"使用租戶帳戶"

"使用ILM管理物件"

應用裝置節點

您可以設定StorageGRID 使用連接埠綁定模式的網路連接埠、以符合處理量、備援和容錯移轉的需求。

您可以在固定或集合式連結模式中設定適用於連接至Grid Network和Client Network的10/25-GbE連接埠StorageGRID 。

1-GbE管理網路連接埠可設定為獨立或主動備份模式、以連線至管理網路。

請參閱設備安裝與維護說明中有關連接埠連結模式的資訊。

相關資訊

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"

網路安裝與資源配置

您必須瞭解在節點部署和網格組態期間、如何使用Grid Network以及選用的管理和用戶端網路。

節點的初始部署

當您第一次部署節點時、必須將節點附加至Grid Network、並確保其具有主要管理節點的存取權。如果網格網路已隔離、您可以在主要管理節點上設定管理網路、以便從網格網路外部進行組態和安裝存取。

在部署期間、已設定閘道的Grid Network會成為節點的預設閘道。預設閘道可讓個別子網路上的網格節點在設定網格之前、先與主要管理節點通訊。

如有必要、也可將包含NTP伺服器或需要存取Grid Manager或API的子網路設定為網格子網路。

使用主要管理節點自動登錄節點

部署節點之後、他們會使用Grid Network向主要管理節點註冊。然後您可以使用Grid Manager `configure-storagegrid.py` Python指令碼或安裝API、用於設定網格並核准已登錄的節點。在網格組態期間、您可以設定多個網格子網路。完成網格組態時、將會在每個節點上建立經由網格網路閘道通往這些子網路的靜態路由。

停用管理網路或用戶端網路

如果您要停用管理網路或用戶端網路、可以在節點核准程序期間移除這些網路或用戶端網路的組態、也可以在安裝完成後使用變更IP工具。請參閱恢復與維護說明中有關網路維護程序的資訊。

相關資訊

"維護"

安裝後準則

完成網格節點部署與組態之後、請遵循下列原則進行DHCP定址和網路組態變更。

- 如果使用DHCP來指派IP位址、請為使用中網路上的每個IP位址設定DHCP保留。

  您只能在部署階段設定DHCP。您無法在設定期間設定DHCP。

  > 當節點的IP位址變更時、節點會重新開機、如果DHCP位址變更同時影響多個節點、可能會導致中斷運作。

- 如果您想要變更網格節點的IP位址、子網路遮罩和預設閘道、則必須使用變更IP程序。請參閱恢復與維護說明中有關設定IP位址的資訊。
- 如果您進行網路組態變更（包括路由和閘道變更）、則可能會失去與主要管理節點和其他網格節點的用戶端連線。視所套用的網路變更而定、您可能需要重新建立這些連線。

相關資訊

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

"安裝VMware"

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"

"維護"

網路連接埠參考

您必須確保網路基礎架構能夠在網格內的節點之間、以及外部用戶端和服務之間、提供內部和外部通訊。您可能需要跨內部和外部防火牆、交換系統和路由系統進行存取。

請使用內部網格節點通訊和外部通訊所提供的詳細資料、判斷如何設定每個必要的連接埠。

- "內部網格節點通訊"
- "外部通訊"

內部網格節點通訊

除了連接埠22、80、123和443之外、內部防火牆僅允許連入網格網路上的特定連接埠（請參閱外部通訊資訊）StorageGRID 。負載平衡器端點所定義的連接埠也接受連線。

NetApp建議您在網格節點之間啟用網際網路控制訊息傳輸協定（ICMP）流量。如果無法到達網格節點、則允許ICMP流量可改善容錯移轉效能。

除了ICMP和表中所列的連接埠之外、StorageGRID VMware還使用虛擬路由器備援傳輸協定（VRP）。VRP是一種使用IP傳輸協定編號112的網際網路傳輸協定。僅在單點傳播模式中使用VRP。StorageGRID只有在設定高可用度（HA）群組時、才需要RP。

Linux型節點準則

如果企業網路原則限制存取任何這些連接埠、您可以使用部署組態參數、在部署時重新對應連接埠。如需連接埠重新對應和部署組態參數的詳細資訊、請參閱Linux平台的安裝說明。

VMware型節點的準則

只有在需要定義VMware網路外部的防火牆限制時、才需設定下列連接埠。

如果企業網路原則限制存取任何這些連接埠、則您可以在使用VMware vSphere Web Client部署節點時重新對應連接埠、或在自動化網格節點部署時使用組態檔設定來重新對應連接埠。如需連接埠重新對應和部署組態參數的詳細資訊、請參閱VMware的安裝說明。

應用裝置儲存節點準則

如果企業網路原則限制存取任何這些連接埠、您可以使用StorageGRID 《不可靠設備安裝程式》重新對應連接埠。如需應用裝置的連接埠重新對應的詳細資訊、請參閱儲存應用裝置的安裝說明。

內部連接埠StorageGRID

連接埠	TCP或udp	寄件者	至	詳細資料
22	TCP	主要管理節點	所有節點	在維護程序中、主要管理節點必須能夠使用連接埠22上的SSH與所有其他節點通訊。允許來自其他節點的SSH流量為選用功能。

80	TCP	應用裝置	主要管理節點	由不受應用裝置使用StorageGRID 、可與主要管理節點進行通訊、以開始安裝。
123.	UDP	所有節點	所有節點	網路時間傳輸協定服務。每個節點都會使用NTP與其他節點同步時間。
443..	TCP	所有節點	主要管理節點	用於在安裝和其他維護程序期間、將狀態傳達給主要管理節點。
1139.	TCP	儲存節點	儲存節點	儲存節點之間的內部流量。
1501.	TCP	所有節點	具有ADC的儲存節點	報告、稽核及組態內部流量。
1502	TCP	所有節點	儲存節點	S3和Swift相關的內部流量。
1504	TCP	所有節點	管理節點	NMS服務報告與組態內部流量。
1505年	TCP	所有節點	管理節點	AMS服務內部流量。
1506	TCP	所有節點	所有節點	伺服器狀態內部流量。
1507	TCP	所有節點	閘道節點	負載平衡器內部流量。
1508年	TCP	所有節點	主要管理節點	組態管理內部流量：
1509	TCP	所有節點	歸檔節點	歸檔節點內部流量。
1511.	TCP	所有節點	儲存節點	中繼資料內部流量。
533.	UDP	所有節點	所有節點	可選擇用於完整網格IP變更、以及在安裝、擴充和還原期間探索主要管理節點。

7001	TCP	儲存節點	儲存節點	Cassandra TLS節點間叢集通訊。
7443.	TCP	所有節點	管理節點	維護程序和錯誤報告的內部流量。
9042.	TCP	儲存節點	儲存節點	Cassandra用戶端連接埠。
9999	TCP	所有節點	所有節點	多項服務的內部流量。包括維護程序、指標和網路更新。
10226	TCP	儲存節點	主要管理節點	由功能不全的應用程式所使用StorageGRID 、可將AutoSupport E-系列SANtricity 的資訊從E-系統管理程式轉送到主要管理節點。
11139.	TCP	歸檔/儲存節點	歸檔/儲存節點	儲存節點與歸檔節點之間的內部流量。
18000	TCP	管理/儲存節點	具有ADC的儲存節點	帳戶服務內部流量。
18001	TCP	管理/儲存節點	具有ADC的儲存節點	身分識別聯盟內部流量。
18002	TCP	管理/儲存節點	儲存節點	與物件傳輸協定相關的內部API流量。
18003	TCP	管理/儲存節點	具有ADC的儲存節點	平台服務內部流量。
18017	TCP	管理/儲存節點	儲存節點	Cloud Storage Pool的Data Mover服務內部流量。
18019	TCP	儲存節點	儲存節點	用於銷毀編碼的區塊服務內部流量。
18082.	TCP	管理/儲存節點	儲存節點	S3相關的內部流量。
18083	TCP	所有節點	儲存節點	與Swift相關的內部流量。

18200年	TCP	管理/儲存節點	儲存節點	有關用戶端要求的其他統計資料。
19000年	TCP	管理/儲存節點	具有ADC的儲存節點	Keystone服務內部流量。

相關資訊

"外部通訊"

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

"安裝VMware"

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"

外部通訊

用戶端需要與網格節點通訊、才能擷取和擷取內容。使用的連接埠取決於所選的物件儲存傳輸協定。用戶端需要存取這些連接埠。

如果企業網路原則限制存取任何連接埠、您可以使用負載平衡器端點來允許存取使用者定義的連接埠。不受信任的用戶端網路功能只能用於負載平衡器端點連接埠上的存取。

若要使用系統和傳輸協定、例如：SMTP、DNS、SSH或DHCP、您必須在部署節點時重新對應連接埠。不過、您不應該重新對應平衡器端點。如需連接埠重新對應的相關資訊、請參閱您平台的安裝說明。

下表顯示用於流量進入節點的連接埠。

此清單不包含可能設定為負載平衡器端點的連接埠。如需詳細資訊、請參閱設定負載平衡器端點的指示。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
22	TCP	SSH	服務筆記型電腦	所有節點	主控台步驟的程序需要SSH或主控台存取。您也可以選擇使用連接埠2022、而非22。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
25	TCP	SMTP	管理節點	電子郵件伺服器	用於警示和電子郵件AutoSupport 導向的功能。您可以使用「電子郵件伺服器」頁面覆寫預設的連接埠設定25。
53.	TCP/ udp	DNS	所有節點	DNS伺服器	用於網域名稱系統。
67	UDP	DHCP	所有節點	DHCP服務	（可選）用於支援DHCP型網路組態。對於靜態設定的網格、則不會執行dhClient服務。
68	UDP	DHCP	DHCP服務	所有節點	（可選）用於支援DHCP型網路組態。對於使用靜態IP位址的網格、dhClient服務不會執行。
80	TCP	HTTP	瀏覽器	管理節點	連接埠80會針對管理節點使用者介面重新導向至連接埠443。
80	TCP	HTTP	瀏覽器	應用裝置	連接埠80重新導向至StorageGRID 連接埠8443、以供使用。
80	TCP	HTTP	具有ADC的儲存節點	AWS	用於傳送至AWS或其他使用HTTP的外部服務的平台服務訊息。當建立端點時、租戶可以覆寫預設的HTTP連接埠設定80。
80	TCP	HTTP	儲存節點	AWS	雲端儲存資源池要求傳送至使用HTTP的AWS目標。網格管理員可在設定雲端儲存資源池時、覆寫預設的HTTP連接埠設定80。
111.	TCP/ udp	rpcbind	NFS用戶端	管理節點	用於NFS型稽核匯出（portmap）。 *附註：*此連接埠僅在NFS型稽核匯出已啟用時才需要。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
123.	UDP	NTP	主要NTP節點	外部NTP	網路時間傳輸協定服務。選取為主要NTP來源的節點也會將時鐘時間與外部NTP時間來源同步。
137.	UDP	NetBios	SMB用戶端	管理節點	用於需要支援NetBios的用戶端SMB型稽核匯出。 *附註：*此連接埠僅在啟用SMB型稽核匯出時才需要。
138	UDP	NetBios	SMB用戶端	管理節點	用於需要支援NetBios的用戶端SMB型稽核匯出。 *附註：*此連接埠僅在啟用SMB型稽核匯出時才需要。
139.	TCP	中小企業	SMB用戶端	管理節點	用於需要支援NetBios的用戶端SMB型稽核匯出。 *附註：*此連接埠僅在啟用SMB型稽核匯出時才需要。
161.	TCP/ udp	SNMP	SNMP用戶端	所有節點	用於SNMP輪詢。所有節點均提供基本資訊；管理節點也提供警示和警示資料。設定時、預設為udp連接埠161。 *附註：*此連接埠僅為必要、且僅在設定SNMP時於節點防火牆上開啟。如果您打算使用SNMP、可以設定替代連接埠。 *附註：*如需使用SNMP搭配StorageGRID 使用功能的相關資訊、請聯絡您的NetApp客戶代表。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
162%	TCP/ udp	SNMP通知	所有節點	通知目的地	傳出SNMP通知和設陷預設為UDP連接埠162。 *附註：*此連接埠僅在啟用SNMP且已設定通知目的地時才需要。如果您打算使用SNMP、可以設定替代連接埠。 *附註：*如需使用SNMP搭配StorageGRID 使用功能的相關資訊、請聯絡您的NetApp客戶代表。
389	TCP/ udp	LDAP	具有ADC的儲存節點	Active Directory / LDAP	用於連線至Active Directory或LDAP伺服器以進行身分識別聯盟。
443..	TCP	HTTPS	瀏覽器	管理節點	由網頁瀏覽器和管理API用戶端使用、用於存取Grid Manager和租戶管理程式。
443..	TCP	HTTPS	管理節點	Active Directory	如果啟用單一登入（SSO）、則管理節點會使用此選項來連線至Active Directory。
443..	TCP	HTTPS	歸檔節點	Amazon S3	用於從歸檔節點存取Amazon S3。
443..	TCP	HTTPS	具有ADC的儲存節點	AWS	用於傳送至AWS或其他使用HTTPS的外部服務的平台服務訊息。當建立端點時、租戶可以覆寫預設的HTTP連接埠設定443。
443..	TCP	HTTPS	儲存節點	AWS	雲端儲存資源池要求傳送至使用HTTPS的AWS目標。網格管理員可在設定雲端儲存資源池時、覆寫預設的HTTPS連接埠設定443。
445	TCP	中小企業	SMB用戶端	管理節點	用於SMB型稽核匯出。 *附註：*此連接埠僅在啟用SMB型稽核匯出時才需要。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
903	TCP	NFS	NFS用戶端	管理節點	用於NFS型稽核匯出（`rpc.mountd`）。 *附註：*此連接埠僅在NFS型稽核匯出已啟用時才需要。
2022年	TCP	SSH	服務筆記型電腦	所有節點	主控台步驟的程序需要SSH或主控台存取。您也可以選擇使用連接埠22、而非2022。
2049	TCP	NFS	NFS用戶端	管理節點	用於NFS型稽核匯出（NFS）。 *附註：*此連接埠僅在NFS型稽核匯出已啟用時才需要。
5696	TCP	KMIP	應用裝置	公里	金鑰管理互通性傳輸協定（KMIP）、從設定為節點加密的應用裝置、到金鑰管理伺服器（KMS）的外部流量、除非StorageGRID 在《與眾不同的應用程式安裝程式》的KMS組態頁面上指定不同的連接埠。
8022	TCP	SSH	服務筆記型電腦	所有節點	連接埠8022上的SSH可讓您存取應用裝置和虛擬節點平台上的基礎作業系統、以進行支援和疑難排解。此連接埠不適用於Linux型（裸機）節點、不需要在網格節點之間或正常作業期間存取。
8082.	TCP	HTTPS	S3用戶端	閘道節點	S3相關的外部流量至閘道節點（HTTPS）。
8083	TCP	HTTPS	Swift用戶端	閘道節點	連至閘道節點（HTTPS）的快速相關外部流量。
8084	TCP	HTTP	S3用戶端	閘道節點	S3相關的外部流量至閘道節點（HTTP）。
8085	TCP	HTTP	Swift用戶端	閘道節點	連至閘道節點（HTTP）的快速相關外部流量。

連接埠	**TCP**或**udp**	傳輸協定	寄件者	至	詳細資料
8443.	TCP	HTTPS	瀏覽器	管理節點	選用。供網頁瀏覽器和管理API用戶端用來存取Grid Manager。可用於分隔Grid Manager與Tenant Manager通訊。
9022	TCP	SSH	服務筆記型電腦	應用裝置	允許以StorageGRID 預先組態模式存取不支援和疑難排解功能。在網格節點之間或正常作業期間、不需要存取此連接埠。
9091.	TCP	HTTPS	外部Grafana服務	管理節點	由外部Grafana服務所使用、可安全存取StorageGRID 《The》《The》《The》《The》《The》《The》《The》《The》》《The *附註：*此連接埠僅在啟用憑證型Prometheus存取時才需要。
9443	TCP	HTTPS	瀏覽器	管理節點	選用。由網頁瀏覽器和管理API用戶端用於存取租戶管理程式。可用於分隔Grid Manager與Tenant Manager通訊。
18082.	TCP	HTTPS	S3用戶端	儲存節點	S3相關的外部流量至儲存節點（HTTPS）。
18083	TCP	HTTPS	Swift用戶端	儲存節點	儲存節點（HTTPS）的快速相關外部流量。
18084	TCP	HTTP	S3用戶端	儲存節點	S3相關的外部流量至儲存節點（HTTP）。
18085	TCP	HTTP	Swift用戶端	儲存節點	儲存節點（HTTP）的快速相關外部流量。

相關資訊

"內部網格節點通訊"

"安裝Red Hat Enterprise Linux或CentOS"

"安裝Ubuntu或DEBIAN"

"安裝VMware"

"SG100 機；SG1000服務應用裝置"

"SG6000儲存設備"

"SG5700儲存設備"

"SG5600儲存設備"