網路概述StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

目錄

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。

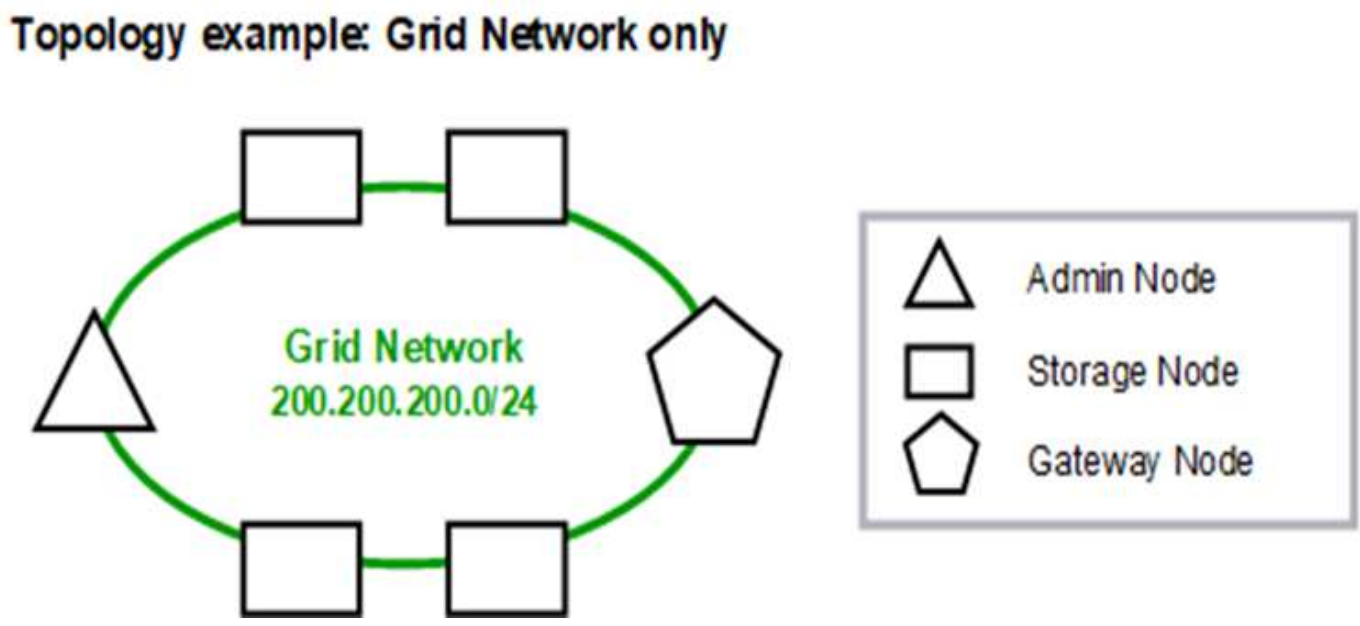
當您設定Grid Network時、會為每個網格節點的eth0介面建立主機IP位址、子網路遮罩和閘道IP位址。

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

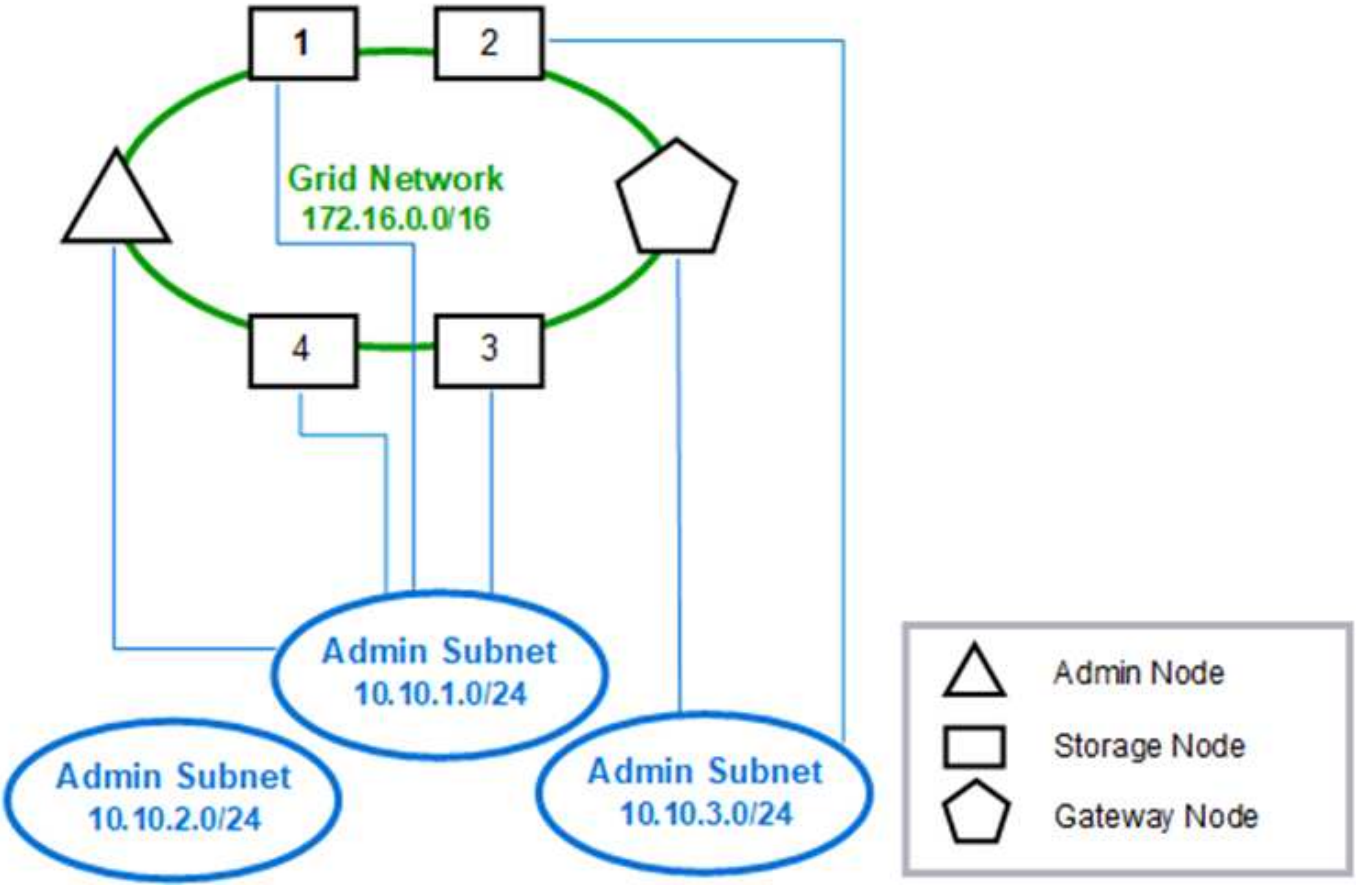
擁有管理網路是選擇性的。使用管理網路和網格網路的其中一種方法、就是為每個節點設定可路由的網格網路和有邊界的管理網路。

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

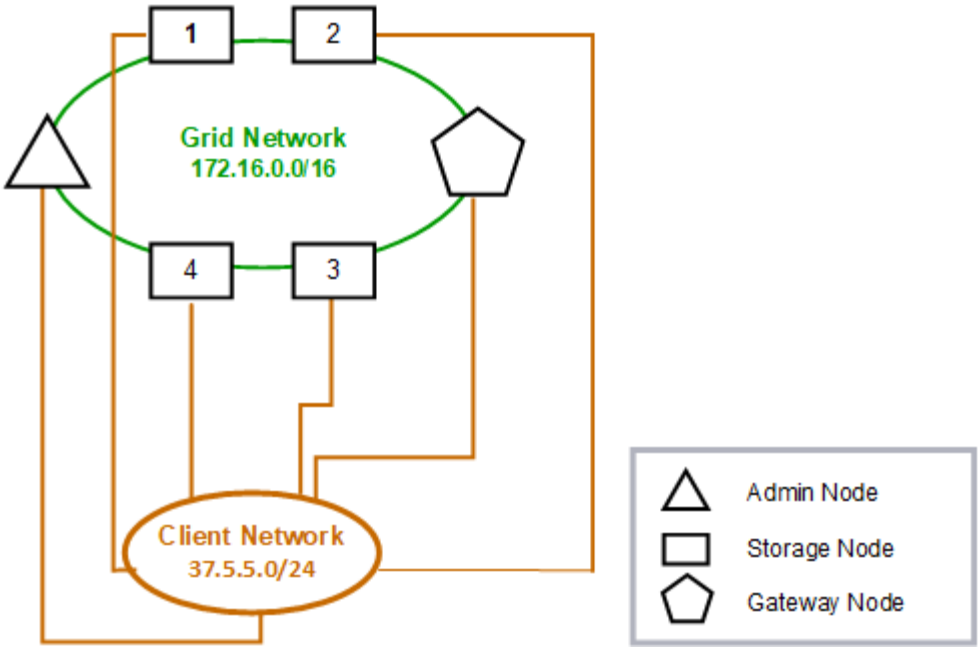
擁有用戶端網路為選用功能。使用用戶端網路可將用戶端網路流量（例如S3和Swift）與網格內部流量區隔、讓網格網路更安全。未設定管理網路時、用戶端或網格網路均可處理管理流量。

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

	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

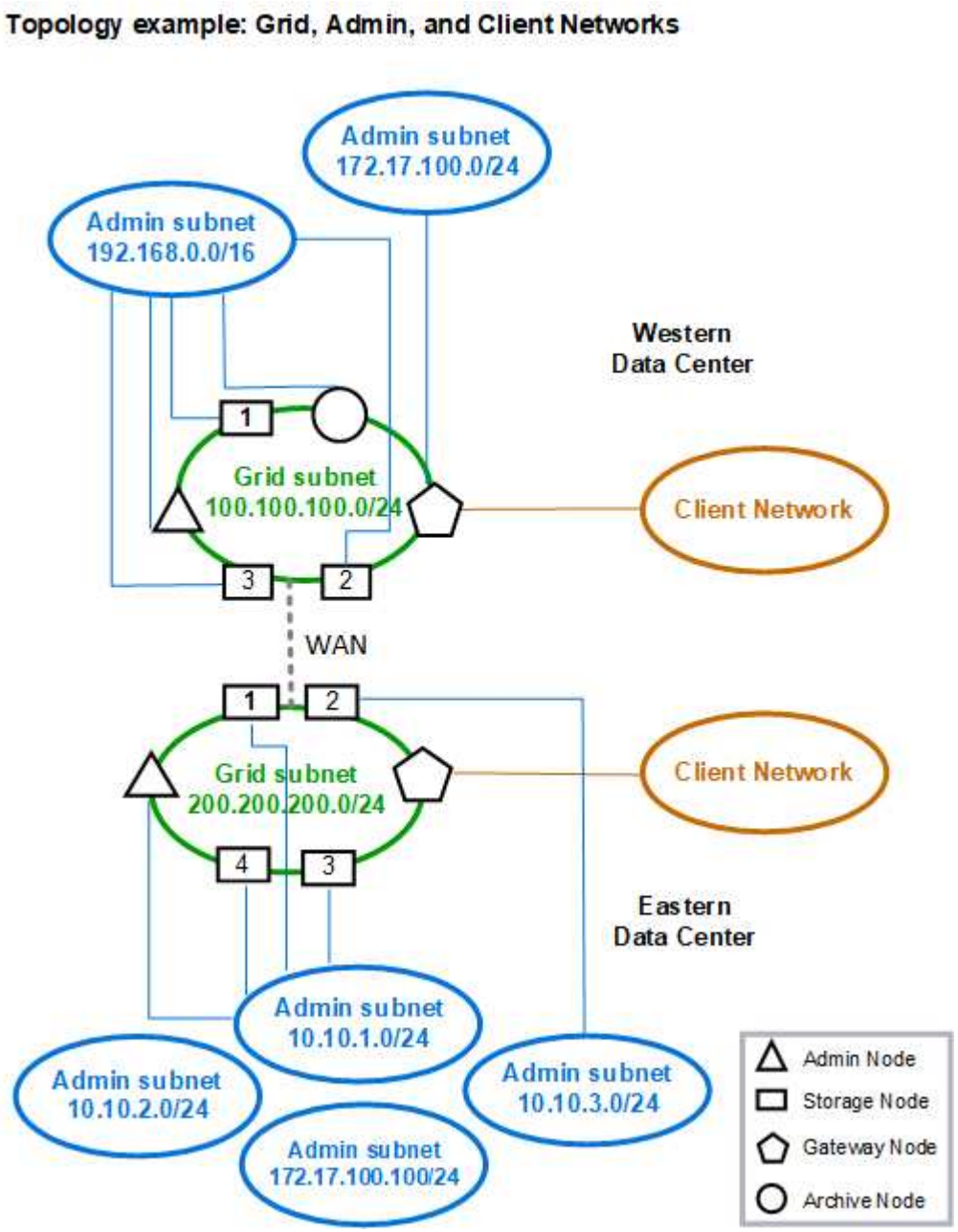
三個網路的拓撲

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。



版權資訊

商標資訊