網路管理
ONTAP 9

NetApp
February 20, 2026

目錄

網路管理

開始使用

使用系統管理員視覺化 **ONTAP** 網路

從 ONTAP 9 開始、您可以使用系統管理員來顯示一個圖形、顯示網路的元件和組態、讓您查看主機、連接埠、 SVM 、 Volume 等各主機之間的網路連線路徑。從 ONTAP 9 。12.1 開始、您可以在網路介面網格上檢視 LIF 和子網路關聯。

當您選取 * 網路 > 總覽 * 或從儀表板的 * 網路 * 區段中選取時、圖形會顯示出來 → 。

下圖顯示下列元件類別：

- 主機
- 儲存連接埠
- 網路介面
- 儲存VM
- 資料存取元件

每個區段都會顯示其他詳細資料、您可以將滑鼠游標暫留或選取以執行網路管理和組態工作。

如果您使用的是傳統系統管理程式（僅適用於 ONTAP 9 7 及更早版本）、請參閱"管理網路"。

範例

以下是您可以與圖形互動的多種方式範例、用以檢視每個元件的詳細資料、或是啟動管理網路的行動：

- 按一下主機即可查看其組態：連接埠、網路介面、儲存 VM 及與其相關的資料存取元件。
- 將滑鼠游標移到儲存VM中的磁碟區數目上、即可選取磁碟區以檢視其詳細資料。
- 選取iSCSI介面以檢視其上週的效能。
- 按一下 ⋮ 元件旁的、即可啟動修改該元件的動作。
- 快速判斷網路中可能發生的問題所在位置、不正常元件旁會顯示「X」。

System Manager網路視覺化影片

瞭解 ONTAP 叢集的網路元件

在設定叢集之前、您應該先熟悉叢集的網路元件。將叢集的實體網路元件組態為邏輯元件、可在ONTAP 畫面上提供靈活度和多租戶功能。

叢集中的各種網路元件如下：

- 實體連接埠

  網路介面卡（NIC）和主機匯流排介面卡（HBA）可提供實體（乙太網路和光纖通道）連線、從每個節點連至實體網路（管理和資料網路）。

  如需站台需求、交換器資訊、連接埠纜線資訊、以及控制器內建連接埠纜線、請參閱Hardware Universe 上的《》（英文） "hwu.netapp.com"。

- 邏輯連接埠

  虛擬區域網路（VLAN）和介面群組構成邏輯連接埠。介面群組將多個實體連接埠視為單一連接埠、而VLAN則將實體連接埠細分為多個獨立連接埠。

- IPspaces

  您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

- 廣播網域

  廣播網域位於IPspace中、包含一組網路連接埠、這些連接埠可能來自叢集中的許多節點、屬於同一個第2層網路。群組中的連接埠用於SVM中的資料流量。

- 子網路

  子網路是在廣播網域內建立、其中包含屬於同一第3層子網路的IP位址集區。此IP位址集區可簡化LIF建立期間的IP位址配置。

- 邏輯介面

  邏輯介面（LIF）是與連接埠相關聯的IP位址或全球連接埠名稱（WWPN）。它與容錯移轉群組、容錯移轉規則及防火牆規則等屬性相關聯。LIF會透過目前繫結的連接埠（實體或邏輯）透過網路進行通訊。

  叢集中的不同類型生命體包括資料生命量、叢集範圍內的管理生命體、節點範圍內的管理生命體、叢集間生命體及叢集生命體。生命生命的所有權取決於LIF所在的SVM。資料生命體歸資料SVM所有、節點範圍內的管理生命體、叢集範圍內的管理、以及叢集間生命體歸管理SVM所有、叢集生命體歸叢集SVM所有。

- DNS區域

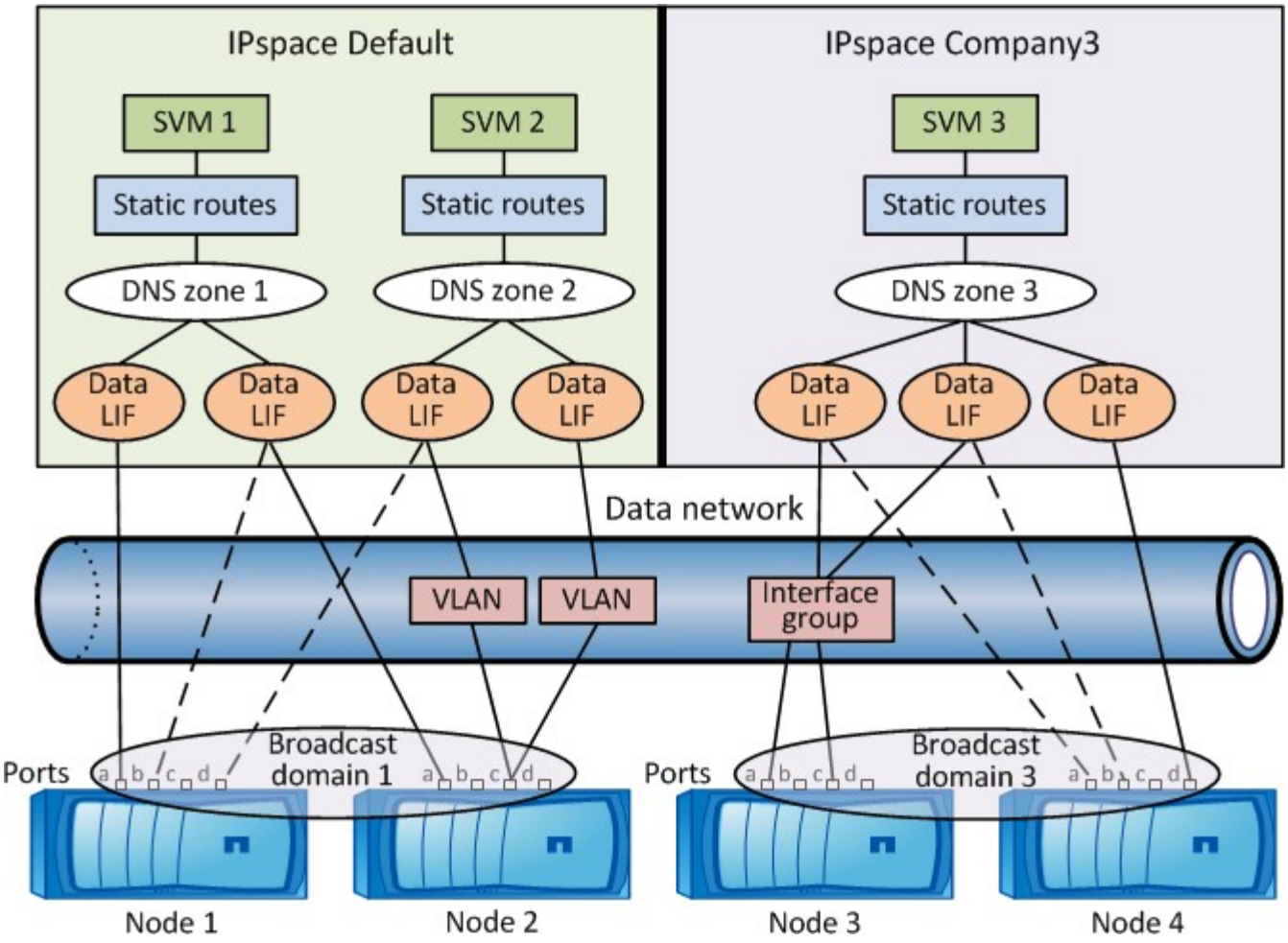
  DNS區域可在LIF建立期間指定、提供透過叢集DNS伺服器匯出LIF的名稱。多個LIF可以共用相同的名稱、讓DNS負載平衡功能根據負載來分配名稱的IP位址。

  SVM可以有多個DNS區域。

- 路由

  每個SVM在網路方面都是自給自足的。SVM擁有可連線至每個已設定外部伺服器的生命和路由。

  下圖說明不同的網路元件在四節點叢集中的關聯方式：

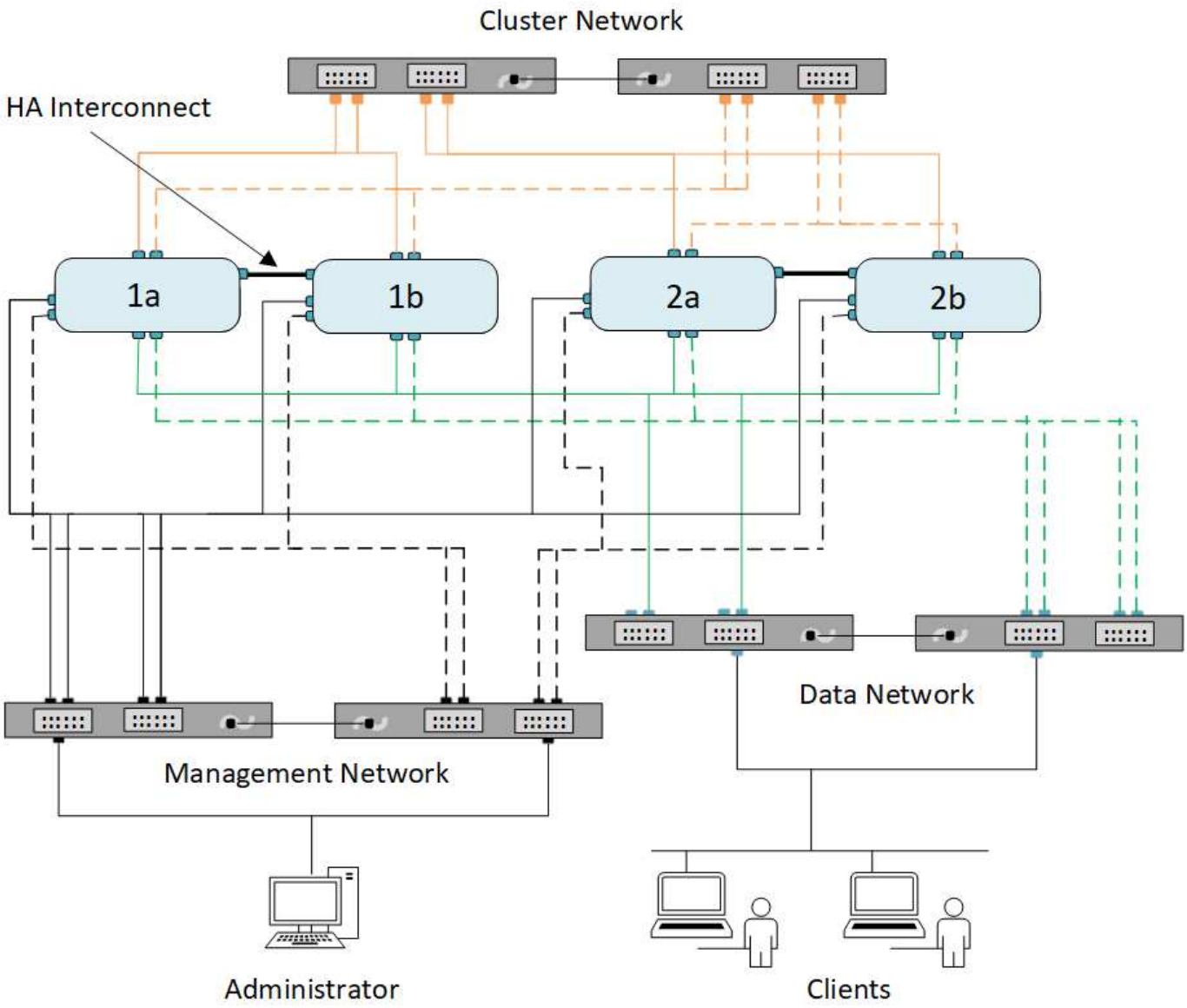


ONTAP 網路纜線的最佳實務做法

網路佈線最佳實務做法可將流量分隔至下列網路：叢集、管理和資料。

您應該連接叢集、使叢集流量與所有其他流量位於不同的網路上。這是一種選擇性做法、但建議您將網路管理流量與資料和叢集內流量分開。藉由維護個別的網路、您可以獲得更好的效能、更容易管理、並改善節點的安全性與管理存取。

下圖說明包含三個獨立網路的四節點HA叢集的網路佈線：



在佈線網路連線時、您應遵循特定準則：

- 每個節點都應連線至三個不同的網路。

  一個網路用於管理、一個用於資料存取、一個用於叢集內通訊。管理和資料網路可以邏輯分隔。

- 您可以將多個資料網路連線至每個節點、以改善用戶端（資料）流量傳輸。
- 建立叢集時無需資料網路連線、但必須包含叢集互連連連線。
- 每個節點都應有兩個或多個叢集連線。

如需網路纜線的詳細資訊、請參閱 "系統文件中心AFF FAS" 和 "Hardware Universe"。

判斷 ONTAP 網路中要使用的 LIF 容錯移轉原則

廣播網域、容錯移轉群組及容錯移轉原則可共同運作、以判斷在設定LIF的節點或連接埠發生故障時、哪個連接埠會接管。

廣播網域會列出同一層乙太網路中所有可連線的連接埠。從其中一個連接埠傳送的乙太網路廣播封包會被廣播網域中的所有其他連接埠所看到。廣播網域的這項通用可到達性特性對lifs很重要、因為如果LIF要容錯移轉至廣播網域中的任何其他連接埠、它仍可連線到從原始連接埠可連線的每個本機和遠端主機。

容錯移轉群組可定義廣播網域內的連接埠、以提供彼此的LIF容錯移轉涵蓋範圍。每個廣播網域都有一個容錯移轉群組、其中包含所有連接埠。此容錯移轉群組包含廣播網域中的所有連接埠、是LIF的預設及建議容錯移轉群組。您可以使用所定義的較小子集建立容錯移轉群組、例如在廣播網域中具有相同連結速度的連接埠容錯移轉群組。

容錯移轉原則決定LIF在節點或連接埠當機時、如何使用容錯移轉群組的連接埠。將容錯移轉原則視為套用至容錯移轉群組的篩選器類型。LIF的容錯移轉目標（LIF可容錯移轉的一組連接埠）是透過將LIF的容錯移轉原則套用至廣播網域中LIF的容錯移轉群組來決定。

您可以使用下列CLI命令檢視LIF的容錯移轉目標：

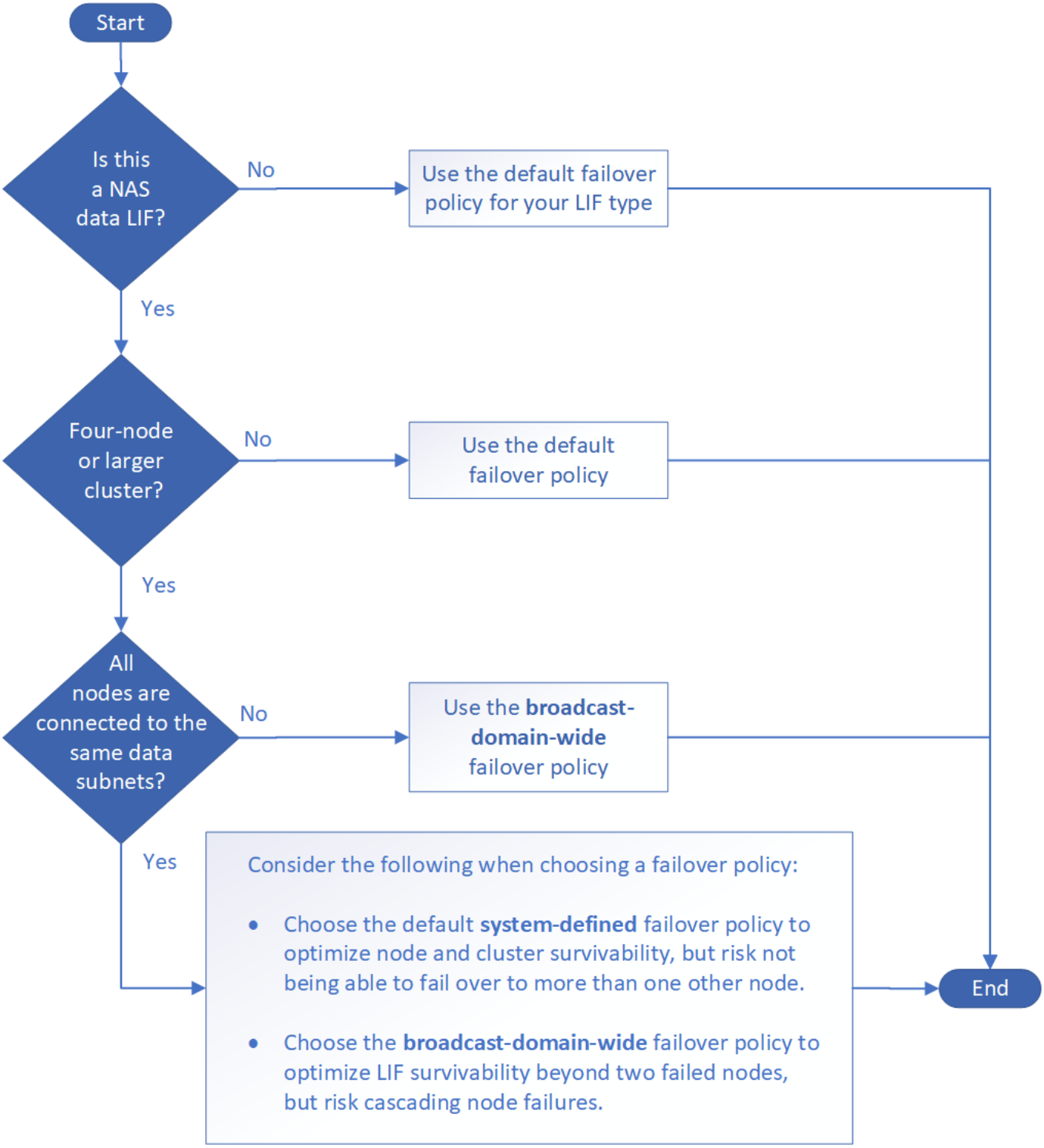
```
network interface show -failover
```

NetApp強烈建議針對LIF類型使用預設的容錯移轉原則。

決定要使用哪個**LIF**容錯移轉原則

決定是使用建議的預設容錯移轉原則、還是根據LIF類型和環境來變更。

容錯移轉原則決策樹狀結構



依**LIF**類型的預設容錯移轉原則

LIF類型	預設容錯移轉原則	說明
BGP lifs	已停用	LIF不會容錯移轉至其他連接埠。
叢集生命	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
叢集管理LIF	整個廣播網域	LIF會容錯移轉至同一個廣播網域中的連接埠、以及叢集中的任何節點。

叢集間LIF	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
NAS資料生命量	系統定義	LIF容錯移轉至另一個非HA合作夥伴的節點。
節點管理生命里	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
SAN 資料生命	已停用	LIF不會容錯移轉至其他連接埠。

「僅限SFO合作夥伴」容錯移轉原則並非預設值、但只有當您希望LIF容錯移轉至主節點或SFO合作夥伴上的連接埠時、才可使用此原則。

相關資訊

- "網路介面顯示"

NAS 路徑容錯移轉工作流程

在 ONTAP 網路上設定 NAS 路徑容錯移轉

如果您已經熟悉基本的網路概念、可以檢閱NAS路徑容錯移轉組態的「實際操作」工作流程、以節省設定網路的時間。

ONTAP 9.7 和舊版中的 NAS 路徑容錯移轉設定工作流程不同。如果您需要在運行 ONTAP 9.7 及更早版本的網絡上配置 NAS 故障切換"NAS 路徑容錯移轉工作流程（ ONTAP 9.7 及更早版本）"，請參閱工作流程。

NAS LIF會在目前連接埠的連結失敗後、自動移轉至正常運作的網路連接埠。您可以仰賴ONTAP 「恢復」預設值來管理路徑容錯移轉。

SAN LIF不會移轉（除非您在連結失敗後手動移動它）。相反地、主機上的多重路徑技術會將流量轉移到不同的LIF。如需詳細資訊、請參閱 "SAN管理"。

1. "填寫工作表單"

請使用工作表規劃 NAS 路徑容錯移轉。

2. "建立IPspaces"

為叢集中的每個 SVM 建立不同的 IP 位址空間。

3. "將廣播網域移至IPspaces"

將廣播網域移至 IPspace 。

4. "建立SVM"

建立 SVM 以將資料提供給用戶端。

5 "建立生命"

在您要用來存取資料的連接埠上建立生命。

6 "設定 SVM 的 DNS 服務"

建立 NFS 或 SMB 伺服器之前，請先設定 SVM 的 DNS 服務。

ONTAP 網路上的 NAS 路徑容錯移轉工作表

在設定NAS路徑容錯移轉之前、您應該先完成工作表的所有區段。

ONTAP 網路上的 NAS 容錯移轉資訊在 ONTAP 9.7 和舊版中有所不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上配置 NAS 故障切換，請"NAS 路徑容錯移轉組態工作表（ ONTAP 9.7 及更早版本）"參閱。

IPSpace組態

您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

資訊	必要？	您的價值
IPSpace名稱 IPspace 的唯一識別碼。	是的	

廣播網域組態

廣播網域會將屬於同一個第2層網路的連接埠分組、並設定廣播網域連接埠的MTU。

廣播網域會指派給IPspace。IPspace可包含一或多個廣播網域。

LIF容錯移轉的連接埠必須是LIF的容錯移轉群組成員。對於ONTAP 由Isname建立的每個廣播網域、也會建立名稱相同的容錯移轉群組、其中包含廣播網域中的所有連接埠。

資訊	必要？	您的價值
IPSpace名稱 指派廣播網域的IPspace。 此IPspace必須存在。	是的	
廣播網域名稱 廣播網域的名稱。 此名稱在IPspace中必須是唯一的。	是的	

MTU 廣播網域的最大傳輸單位值，通常設定為 **1500** 或 **9000** 。 MTU值會套用至廣播網域中的所有連接埠、以及稍後新增至廣播網域的任何連接埠。 MTU值應與連接至該網路的所有裝置相符。請注意、e0M連接埠處理管理和服務處理器流量應將MTU設定為不超過1500位元組。	是的	
連接埠 連接埠會根據連線能力指派給廣播網域。連接埠指派完成後、請執行來檢查連線能力 `network port reachability show` 命令。 這些連接埠可以是實體連接埠、VLAN或介面群組。 如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。	是的	

子網路組態

子網路包含IP位址集區和預設閘道、可指派給IP空間中的SVM所使用的生命區。

- 在SVM上建立LIF時、您可以指定子網路的名稱、而非提供IP位址和子網路。
- 由於子網路可以設定為預設閘道、因此在建立SVM時、您不需要在個別步驟中建立預設閘道。
- 廣播網域可以包含一或多個子網路。
- 您可以將多個子網路與IPspace的廣播網域建立關聯、以設定位於不同子網路上的SVM LIF。
- 每個子網路都必須包含IP位址、而不應與指派給相同IPspace中其他子網路的IP位址重疊。
- 您可以將特定的IP位址指派給SVM資料生命期、並為SVM建立預設閘道、而非使用子網路。

資訊	必要？	您的價值
IPSpace名稱 子網路指派的IPspace。 此IPspace必須存在。	是的	
子網路名稱 子網路名稱。 此名稱在IPspace中必須是唯一的。	是的	

廣播網域名稱 要指派子網路的廣播網域。 此廣播網域必須位於指定的IPspace中。	是的	
子網路名稱和遮罩 IP位址所在的子網路和遮罩。	是的	
閘道 您可以指定子網路的預設閘道。 如果您在建立子網路時未指派閘道、可以稍後指派一個閘道。	否	
IP位址範圍 您可以指定IP位址範圍或特定IP位址。 例如、您可以指定一個範圍、例如： `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` 如果未指定IP位址範圍、則指定子網路中的IP位址範圍將可指派給LIF。	否	
強制更新LIF關聯 指定是否強制更新現有LIF關聯。 根據預設、如果任何服務處理器介面或網路介面使用所提供範圍內的IP位址、則建立子網路會失敗。 使用此參數可將任何手動定址的介面與子網路建立關聯、並允許命令成功執行。	否	

SVM 組態

您可以使用SVM將資料提供給用戶端和主機。

您記錄的值是建立預設資料SVM。如果您要建立MetroCluster 一個SVM的不確定來源、請參閱 "Fabric附加MetroCluster 的《安裝與組態指南》" 或 "延伸MetroCluster 《安裝與組態指南》"。

資訊	必要？	您的價值
SVM名稱 SVM 的完整網域名稱（ FQDN ）。 此名稱必須在各叢集聯盟中都是唯一的名稱。	是的	

根Volume名稱 SVM根Volume的名稱。	是的	
Aggregate名稱 擁有SVM根磁碟區的集合體名稱。 此Aggregate必須存在。	是的	
安全風格 SVM根磁碟區的安全樣式。 可能的值包括* ntf*、* UNIX*和*混合*。	是的	
IPSpace名稱 指派SVM的IPspace。 此IPspace必須存在。	否	
SVM語言設定 SVM及其磁碟區的預設語言。 如果未指定預設語言、預設SVM語言會設為* 。UTF-8*。 SVM語言設定可決定用於顯示SVM中所有NAS磁碟區的檔案名稱和資料的字元集。 您可以在建立SVM之後修改語言。	否	

LIF 組態

SVM透過一或多個網路邏輯介面（LIF）、為用戶端和主機提供資料服務。

資訊	必要？	您的價值
SVM名稱 LIF的SVM名稱。	是的	
LIF 名稱 LIF 的名稱。 您可以為每個節點指派多個資料生命期、而且只要節點有可用的資料連接埠、就可以將生命期指派給叢集中的任何節點。 若要提供備援、您應該為每個子網路建立至少兩個資料生命期、並在不同節點上指派指派指派給特定子網路的生命期為主連接埠。 *重要事項：*如果您將SMB伺服器設定為以SMB代管Hyper-V或SQL Server、以提供不中斷營運的解決方案、則叢集中每個節點上的SVM必須至少有一個資料LIF。	是的	

服務原則 LIF 的服務原則。 服務原則會定義哪些網路服務可以使用LIF。內建的服務和服務原則可用於管理資料和系統SVM上的資料和管理流量。	是的	
允許的傳輸協定 IP 型的生命體不需要允許的通訊協定、請改用服務原則列。 指定在Fibre Channel連接埠上允許的SAN生命體傳輸協定。這些是可以使用該LIF的傳輸協定。在建立LIF之後、無法修改使用LIF的傳輸協定。設定LIF時、您應該指定所有的傳輸協定。	否	
主節點 LIF還原至其主連接埠時、LIF傳回的節點。 您應該記錄每個資料LIF的主節點。	是的	
主連接埠或廣播網域 請選擇下列其中一項： **Port** ：指定邏輯介面在 LIF 還原至其主連接埠時傳回的連接埠。這僅適用於IPspace子網路中的第一個LIF、否則不需要。 廣播網域：指定廣播網域、系統會在LIF還原至其主連接埠時、選取邏輯介面傳回的適當連接埠。	是的	
子網路名稱 要指派給SVM的子網路。 用於建立應用程式伺服器的持續可用SMB連線的所有資料生命期、必須位於相同的子網路上。	是（如果使用子網路）	

DNS 組態

在建立NFS或SMB伺服器之前、您必須在SVM上設定DNS。

資訊	必要？	您的價值
SVM名稱 您要在其中建立NFS或SMB伺服器的SVM名稱。	是的	
DNS網域名稱 執行主機對IP名稱解析時要附加到主機名稱的網域名稱清單。 請先列出本機網域、然後列出最常進行DNS查詢的網域名稱。	是的	

DNS 伺服器的 IP 位址 將為 NFS 或 SMB 伺服器提供名稱解析的 DNS 伺服器 IP 位址清單。 列出的DNS伺服器必須包含所需的服務位置記錄（SRV),才能找到SMB伺服器要加入之網域的Active Directory LDAP伺服器和網域控制器。 「服務」記錄用於將服務名稱對應至提供該服務之伺服器的DNS電腦名稱。如果ONTAP 無法透過本機DNS查詢取得服務位置記錄、則無法建立SMB伺服器。 確保ONTAP 功能完整的Active Directory SRVs記錄、最簡單的方法就是將Active Directory整合的DNS伺服器設定為SVM DNS伺服器。 您可以使用非Active Directory整合的DNS伺服器、前提是DNS管理員已手動將含有Active Directory網域控制器相關資訊的SRV記錄新增至DNS區域。 如需Active Directory整合式SRV記錄的相關資訊、請參閱主題 "Microsoft TechNet上的DNS Active Directory支援運作方式"。	是的	

動態**DNS**組態

您必須先在SVM上設定動態DNS（DDNS）、才能使用動態DNS自動將DNS項目新增至Active Directory整合的DNS伺服器。

系統會為SVM上的每個資料LIF建立DNS記錄。透過在SVM上建立多個資料LIF、您可以在用戶端連線與指派的資料IP位址之間取得負載平衡。DNS負載會以循環配置資源的方式、平衡使用主機名稱對指派IP位址所建立的連線。

資訊	必要？	您的價值
SVM名稱 您要在其中建立NFS或SMB伺服器的SVM。	是的	
是否使用DDNS 指定是否使用DDNS。 SVM上設定的DNS伺服器必須支援DDNS。預設會停用DDNS。	是的	

是否使用安全的DDNS 只有Active Directory整合的DNS才支援安全DDNS。 如果Active Directory整合的DNS只允許安全的DDNS更新、則此參數的值必須為true。 根據預設、安全DDNS會停用。 只有在為SVM建立SMB伺服器或Active Directory帳戶之後、才能啟用安全DDNS。	否	
DNS網域的FQDN DNS網域的FQDN。 您必須使用在SVM上為DNS名稱服務設定的相同網域名稱。	否	

網路連接埠

瞭解 **ONTAP** 網路連接埠組態

連接埠是實體連接埠（NIC）或虛擬化連接埠、例如介面群組或VLAN。

虛擬區域網路（VLAN）和介面群組構成虛擬連接埠。介面群組將多個實體連接埠視為單一連接埠、而VLAN則將實體連接埠細分為多個獨立的邏輯連接埠。

- 實體連接埠：可直接在實體連接埠上設定LIF。
- 介面群組：連接埠Aggregate、包含兩個以上的實體連接埠、做為單一主幹連接埠。介面群組可以是單一模式、多重模式或動態多重模式。
- VLAN：接收和傳送VLAN標記（IEEE 802.1Q標準）流量的邏輯連接埠。VLAN連接埠特性包括連接埠的VLAN ID。基礎實體連接埠或介面群組連接埠被視為VLAN主幹連接埠、且連接的交換器連接埠必須設定為主幹VLAN ID。

  VLAN連接埠的基礎實體連接埠或介面群組連接埠可繼續裝載傳輸區、以傳輸和接收無標記流量。

- 虛擬IP（VIP）連接埠：作為VIP LIF主連接埠的邏輯連接埠。VIP連接埠是由系統自動建立、僅支援有限數量的作業。支援VIP連接埠、從ONTAP 功能表9.5開始。

連接埠命名慣例為_enumberletter：

- 第一個字元說明連接埠類型。
  「E」代表乙太網路。
- 第二個字元表示連接埠介面卡所在的編號插槽。
- 第三個字元表示連接埠在多端口介面卡上的位置。
  「A」表示第一個連接埠、「b」表示第二個連接埠、依此類推。

例如、 `e0b` 表示乙太網路連接埠是節點主機板上的第二個連接埠。

VLAN 必須使用語法命名 `port_name-vlan-id`。

`port_name` 指定實體連接埠或介面群組。

`vlan-id` 指定網路上的 VLAN 識別。例如、 `e1c-80` 為有效的 VLAN 名稱。

設定網路連接埠

結合實體連接埠以建立 **ONTAP** 介面群組

介面群組也稱為「連結集合群組（ LAG ）」、是透過將同一個節點上的兩個或多個實體連接埠合併為單一邏輯連接埠而建立。邏輯連接埠可提供更高的恢復能力、更高的可用度和負載共享。

介面群組類型

儲存系統支援三種類型的介面群組：單一模式、靜態多重模式和動態多重模式。每個介面群組提供不同層級的容錯能力。多重模式介面群組提供負載平衡網路流量的方法。

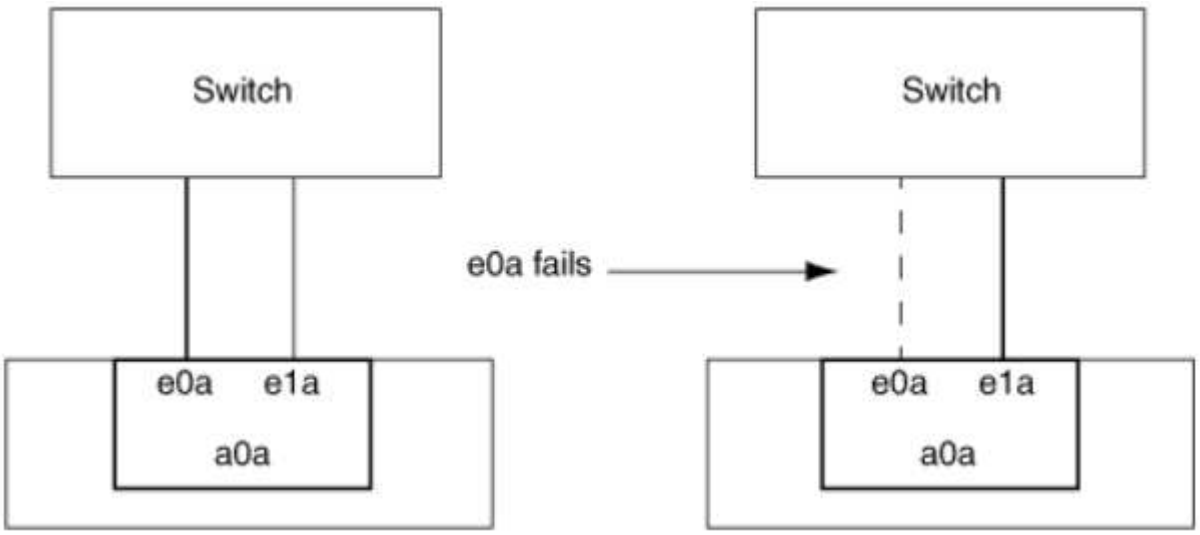
單一模式介面群組的特性

在單一模式介面群組中、介面群組中只有一個介面處於作用中狀態。其他介面處於待命狀態、可在作用中介面故障時接管。

單一模式介面群組的特性：

- 對於容錯移轉、叢集會監控主動式連結並控制容錯移轉。
  由於叢集會監控主動式連結、因此不需要交換器組態。
- 在單一模式介面群組中、待命的介面可以有多個。
- 如果單一模式介面群組橫跨多個交換器、則必須使用交換器間連結（ISL）來連接交換器。
- 對於單一模式介面群組、交換器連接埠必須位於相同的廣播網域中。
- 來源位址為0.00.0的連結監控Arp封包會透過連接埠傳送、以驗證連接埠是否位於同一個廣播網域中。

下圖是單一模式介面群組的範例。在圖中、e0a和e1a是a0a單一模式介面群組的一部分。如果作用中介面e0a故障、待命e1a介面會接管並維持與交換器的連線。



若要完成單一模式功能、建議改用容錯移轉群組。使用容錯移轉群組時、第二個連接埠仍可用於其他生命週期、不需保留未使用的狀態。此外、容錯移轉群組可跨越兩個以上的連接埠、並可跨越多個節點上的連接埠。

靜態多重模式介面群組的特性

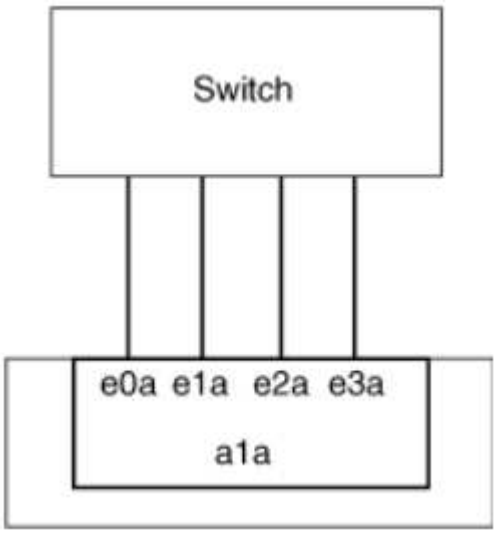
靜態多重模式介面群組實作ONTAP 功能符合IEEE 802.3ad（靜態）。任何支援Aggregate但沒有設定Aggregate的控制封包交換的交換器、都可以搭配靜態多重模式介面群組使用。

靜態多重模式介面群組不符合IEEE 802.3ad（動態）、也稱為「連結集合控制傳輸協定（LACP）」。LACP相當於連接埠集合傳輸協定（PAgP）、這是Cisco專屬的連結集合傳輸協定。

以下是靜態多重模式介面群組的特性：

- 介面群組中的所有介面都處於作用中狀態、並共用一個MAC位址。
  - 介面群組中的介面之間會分散多個個別連線。
  - 每個連線或工作階段都會在介面群組中使用一個介面。
    當您使用循序負載平衡方案時、所有工作階段都會以每個封包為基礎散佈在可用的連結之間、而且不會繫結到介面群組中的特定介面。
- 靜態多重模式介面群組最多可從「n-1」介面故障中恢復、其中n是組成介面群組的介面總數。
- 如果某個連接埠故障或拔除、則會自動將流經故障連結的流量重新分配至其餘的其中一個介面。
- 靜態多重模式介面群組可偵測到連結中斷、但無法偵測到與用戶端或交換器的連線中斷、進而影響連線能力和效能。
- 靜態多重模式介面群組需要支援多個交換器連接埠連結集合的交換器。
  交換器已設定成介面群組連結所連接的所有連接埠都是單一邏輯連接埠的一部分。某些交換器可能不支援設定用於巨型框架的連接埠連結集合。如需詳細資訊、請參閱交換器廠商的文件。
- 有多種負載平衡選項可供在靜態多重模式介面群組的介面之間分配流量。

下圖是靜態多重模式介面群組的範例。介面e0a、e1a、E2A和e3a是A1A多重模式介面群組的一部分。A1A多重模式介面群組中的所有四個介面都處於作用中狀態。



有幾項技術可讓單一集合式連結中的流量分散在多個實體交換器上。啟用此功能的技術因網路產品而異。靜態多

重模式介面群組ONTAP 的功能符合IEEE 802.3標準。如果某種特定的多重交換器連結集合技術據說可與IEEE 802.3標準互通或符合該標準、則應搭配ONTAP 使用。

IEEE 802.3標準指出、彙總連結中的傳輸裝置會決定傳輸的實體介面。因此ONTAP 、只有在分配傳出流量時、才能控制傳入訊框的傳入方式。如果您想要管理或控制集合式連結的傳入流量傳輸、則必須在直接連線的網路裝置上修改該傳輸。

動態多重模式介面群組

動態多重模式介面群組實作連結集合控制傳輸協定（LACP）、將群組成員資格與直接連接的交換器通訊。LACP可讓您偵測失去連結狀態、以及節點無法與直接附加交換器連接埠通訊。

Dynamic多重模式介面群組實作ONTAP 在整個過程中均符合IEEE 802.3 AD（802.1 AX）標準。不支援連接埠集合傳輸協定（PAgP）、這是Cisco專屬的連結集合傳輸協定。ONTAP

動態多重模式介面群組需要支援LACP的交換器。

在不可設定的主動模式中執行LACP、可與設定為主動或被動模式的交換器搭配運作。ONTAP根據IEEE 802.3 AD（802.1AX）的規定、執行長和短LACP定時器（搭配不可設定的值使用3秒和90秒）ONTAP 。

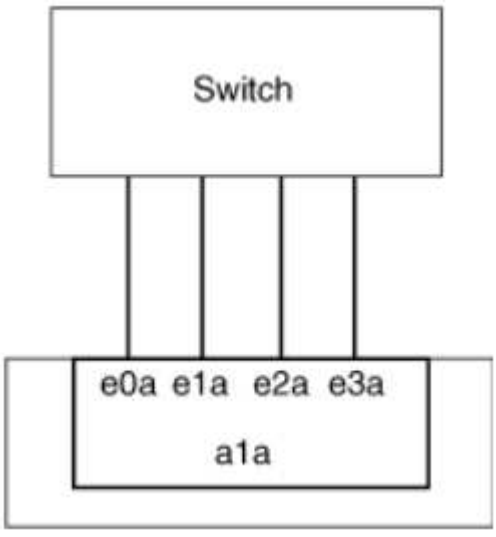
此功能可判斷用於傳輸傳出流量的成員連接埠、但無法控制接收傳入訊框的方式。ONTAP交換器會根據交換器連接埠通道群組中設定的負載平衡演算法、決定其連接埠通道群組的成員（個別實體連接埠）以供傳輸。因此、交換器組態會決定儲存系統的成員連接埠（個別實體連接埠）來接收流量。如需設定交換器的詳細資訊、請參閱交換器廠商的文件。

如果個別介面無法接收連續的LACP傳輸協定封包、則在「ifgrp STATUS」命令的輸出中、該個別介面會標示為「lid_inactive」。現有流量會自動重新路由至任何剩餘的作用中介面。

使用動態多重模式介面群組時、適用下列規則：

- 動態多重模式介面群組應設定為使用連接埠型、IP型、MAC型或循環配置資源負載平衡方法。
- 在動態多重模式介面群組中、所有介面都必須處於作用中狀態、並共用一個MAC位址。

下圖為動態多重模式介面群組的範例。介面e0a、e1a、E2A和e3a是A1A多重模式介面群組的一部分。A1A動態多重模式介面群組中的所有四個介面都處於作用中狀態。



多重模式介面群組中的負載平衡

您可以使用 IP 位址， MAC 位址，循序或連接埠型負載平衡方法，在多重模式介面群組的網路連接埠上平均分配網路流量，確保多重模式介面群組的所有介面都能用於傳出流量。

只有在建立介面群組時、才能指定多重模式介面群組的負載平衡方法。

最佳實務：建議盡可能使用連接埠型負載平衡。除非網路中有特定的原因或限制可防止負載平衡、否則請使用連接埠型負載平衡。

連接埠型負載平衡

建議使用連接埠型負載平衡。

您可以使用連接埠型負載平衡方法、根據傳輸層（TCP/IP）連接埠、將多重模式介面群組上的流量等化。

連接埠型負載平衡方法使用快速雜湊演算法來處理來源和目的地IP位址、以及傳輸層連接埠號碼。

IP位址和**MAC**位址負載平衡

IP位址和MAC位址負載平衡是在多重模式介面群組上平衡流量的方法。

這些負載平衡方法使用快速雜湊演算法來處理來源位址和目的地位址（IP位址和MAC位址）。如果雜湊演算法的結果對應到不在UP連結狀態的介面、則會使用下一個作用中介面。

> 在直接連線至路由器的系統上建立介面群組時、請勿選取MAC位址負載平衡方法。在這樣的設定中、每個傳出IP訊框的目的MAC位址都是路由器的MAC位址。因此、只會使用介面群組的一個介面。

IP位址負載平衡的運作方式與IPv6位址相同。

連續負載平衡

您可以使用循序負載平衡、使用循環配置資源演算法、在多個連結之間平均分配封包。您可以使用連續選項來平衡單一連線在多個連結之間的流量負載、以增加單一連線處理量。

不過、由於連續負載平衡可能導致封包交付順序不正常、因此可能導致效能極差。因此、一般不建議使用循序負載平衡。

建立介面群組或**LAG**

您可以建立介面群組或LAG（單一模式、靜態多重模式或動態多重模式（LACP））、結合彙總網路連接埠的功能、將單一介面呈現給用戶端。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式建立LAG *

步驟

1. 選擇*網路>乙太網路連接埠>+連結集合群組*以建立LAG。
2. 從下拉式清單中選取節點。
3. 請從下列選項中選擇：
   a. 自動選擇廣播網域（建議）。ONTAP
   b. 手動選取廣播網域。
4. 選擇要形成 LAG 的連接埠。
5. 選取模式：
   a. 單一：一次只使用一個連接埠。
   b. 多個：所有連接埠都可以同時使用。
   c. LACP：LACP傳輸協定決定可使用的連接埠。
6. 選擇負載平衡：
   a. IP型
   b. Mac型
   c. 連接埠
   d. 連續的
7. 儲存您的變更。

CLI

使用**CLI**建立介面群組

建立多重模式介面群組時、您可以指定下列任一種負載平衡方法：

- `port`：網路流量是根據傳輸層（ TCP/UDP ）連接埠來分配。這是建議的負載平衡方法。
- `mac`：網路流量是根據 MAC 位址來分配。
- `ip`：網路流量是根據 IP 位址來分配。
- `sequential`：網路流量會在收到時隨之分佈。

> ⓘ 介面群組的MAC位址取決於基礎連接埠的順序、以及這些連接埠在開機期間的初始化方式。因此、您不應假設在重新開機或ONTAP 進行升級時、ifgrp MAC位址會持續存在。

步驟

使用 `network port ifgrp create` 用於建立介面群組的命令。

介面群組必須使用語法命名 `a<number><letter>`。例如、a0a、a0b、a1C和a2a是有效的介面群組名稱。

如"指令參考資料ONTAP"需詳細 `network port ifgrp create`資訊，請參閱。

以下範例說明如何建立名為a0a的介面群組、其中包含連接埠的發佈功能和多重模式：

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

將連接埠新增至介面群組或**LAG**

您最多可將16個實體連接埠新增至介面群組或LAG、以獲得所有連接埠速度。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式將連接埠新增至LAG *

步驟

1. 選擇*網路>乙太網路連接埠> LAG*以編輯LAG。
2. 在同一個節點上選取其他連接埠以新增至LAG。
3. 儲存您的變更。

CLI

使用**CLI**將連接埠新增至介面群組

步驟

將網路連接埠新增至介面群組：

```
network port ifgrp add-port
```

下列範例說明如何將連接埠e0c新增至名為a0a的介面群組：

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

從ONTAP 功能更新到功能更新的版本開始、介面群組會在介面群組新增第一個實體連接埠約一分鐘後、自動放入適當的廣播網域。如果您不想讓 ONTAP 這麼做、而偏好手動將 ifgrp 放入廣播網域、請指定 `-skip -broadcast-domain-placement` 參數為的一部分 `ifgrp add-port` 命令。

深入瞭解 `network port ifgrp add-port`和設定中適用於連接埠介面群組"指令參考資料ONTAP"的限制。

從介面群組或**LAG**中移除連接埠

只要連接埠不是介面群組中的最後一個連接埠、您就可以從裝載lifs的介面群組中移除該連接埠。由於您並未從介面群組中移除最後一個連接埠、因此不需要介面群組不可裝載lifs、也不需要介面群組不可是LIF的主連接埠。不過、如果您要移除最後一個連接埠、則必須先移轉或移除介面群組中的LIF。

關於這項工作

您最多可從介面群組或LAG移除16個連接埠（實體介面）。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式從LAG *移除連接埠

步驟

1. 選擇*網路>乙太網路連接埠> LAG*以編輯LAG。
2. 從LAG中選取要移除的連接埠。
3. 儲存您的變更。

CLI

*使用CLI從介面群組*移除連接埠

步驟

從介面群組移除網路連接埠：

```
network port ifgrp remove-port
```

如"指令參考資料ONTAP"需詳細 `network port ifgrp remove-port`資訊，請參閱。

下列範例說明如何從名為a0a的介面群組移除連接埠e0c：

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

刪除介面群組或**LAG**

如果要直接在基礎實體連接埠上設定LIF、或決定變更介面群組、LAG模式或發佈功能、您可以刪除介面群組或LAG。

開始之前

- 介面群組或LAG不得裝載LIF。
- 介面群組或LAG不能是LIF的主連接埠或容錯移轉目標。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式刪除LAG *

步驟

1. 選擇*網路>乙太網路連接埠> LAG *以刪除LAG。
2. 選取您要移除的 LAG 。
3. 刪除 LAG 。

CLI

使用**CLI**刪除介面群組

步驟

使用 `network port ifgrp delete` 用於刪除介面群組的命令。

如"指令參考資料ONTAP"需詳細 `network port ifgrp delete`資訊，請參閱。

下列範例說明如何刪除名為a0b的介面群組：

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

透過實體連接埠設定 **ONTAP VLAN**

您可以在 ONTAP 中使用 VLAN 來提供網路的邏輯區段、方法是建立獨立的廣播網域、這些網域是以交換器連接埠為基礎定義、而非以實體邊界定義的傳統廣播網域。

一個VLAN可以跨越多個實體網路區段。屬於VLAN的終端站台會依功能或應用程式而定。

例如、VLAN中的終端站台可能會依部門（例如工程和會計）或專案（例如releasease1和release2）進行分組。由於終端站台的實體鄰近性在VLAN中並不重要、因此您可以將終端站台分散到不同的地理位置、並將廣播網域保留在交換式網路中。

在ONTAP 9.14.1 和 9.13.1 中，未被任何邏輯介面 (LIF) 使用且在所連接的交換器上缺少本機 VLAN 連線的未標記連接埠被標記為已降級。這有助於識別未使用的端口，並不表示中斷。本機 VLAN 允許 ifgrp 基本連接埠上未標記的流量，例如ONTAP CFM 廣播。在交換器上設定本機 VLAN 以防止阻止未標記的流量。

您可以建立、刪除或顯示有關VLAN的資訊來管理VLAN。

> 您不應該在網路介面上建立與交換器原生VLAN相同識別碼的VLAN。例如、如果網路介面e0b位於原生VLAN 10、則不應在該介面上建立VLAN e0b-10。

建立 **VLAN**

您可以使用 System Manager 或建立 VLAN 、以維護同一個網路網域內的個別廣播網域 `network port vlan create` 命令。

開始之前

確認已符合下列要求：

- 部署在網路中的交換器必須符合IEEE 802.1Q標準、或是具有廠商專屬的VLAN實作。
- 若要支援多個VLAN、端點必須靜態設定為屬於一個或多個VLAN。
- VLAN未附加至裝載叢集LIF的連接埠。
- VLAN未連接至指派給叢集IPspace的連接埠。
- VLAN並非在不含成員連接埠的介面群組連接埠上建立。

關於這項工作

建立VLAN會將VLAN附加至叢集中指定節點上的網路連接埠。

當您第一次透過連接埠設定VLAN時、連接埠可能會關閉、導致網路暫時中斷連線。後續新增至相同連接埠的VLAN不會影響連接埠狀態。

> 您不應該在網路介面上建立與交換器原生VLAN相同識別碼的VLAN。例如、如果網路介面e0b位於原生VLAN 10、則不應在該介面上建立VLAN e0b-10。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**建立**VLAN**

從ONTAP 功能更新9.12.0開始、您可以自動選取廣播網域、或從清單中手動選取。之前、廣播網域一律會根據第2層連線功能自動選取。如果您手動選取廣播網域、會出現一則警告訊息、指出手動選取廣播網域可能會導致連線中斷。

步驟

1. 選擇*網路>乙太網路連接埠>+ VLAN*。
2. 從下拉式清單中選取節點。
3. 請從下列選項中選擇：
   a. 自動選擇廣播網域（建議）。ONTAP
   b. 可從列表中手動選擇廣播域。
4. 選取要形成VLAN的連接埠。
5. 指定VLAN ID。
6. 儲存您的變更。

CLI

使用**CLI**建立**VLAN**

在某些情況下、如果您想要在效能降低的連接埠上建立 VLAN 連接埠、而不修正硬體問題或任何軟體組態錯誤、則可以設定 `-ignore-health-status` 的參數 `network port modify` 命令為 `true`。

如"指令參考資料ONTAP"需詳細 `network port modify`資訊，請參閱。

步驟

1. 使用 `network port vlan create` 建立 VLAN 的命令。
2. 您必須指定 `vlan-name` 或 `port` 和 `vlan-id` 建立 VLAN 的選項。
   VLAN名稱是連接埠（或介面群組）名稱與網路交換器VLAN識別碼的組合、中間有連字號。例如、`e0c-24` 和 `e1c-80` 為有效的 VLAN 名稱。

以下範例說明如何建立 VLAN `e1c-80` 已連接至網路連接埠 `e1c` 在節點上 `cluster-1-01`：

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

從ONTAP 功能更新到功能更新的版本開始、VLAN會在建立後約一分鐘自動放入適當的廣播網域。如果您不想讓 ONTAP 這麼做、而偏好手動將 VLAN 放入廣播網域、請指定 `-skip-broadcast-domain-placement` 參數為的一部分 `vlan create` 命令。

如"指令參考資料ONTAP"需詳細 `network port vlan create`資訊，請參閱。

編輯 VLAN

您可以變更廣播網域或停用VLAN。

使用System Manager編輯VLAN

從ONTAP 功能更新9.12.0開始、您可以自動選取廣播網域、或從清單中手動選取。先前的廣播網域一律會根據第2層連線功能自動選取。如果您手動選取廣播網域、會出現一則警告訊息、指出手動選取廣播網域可能會導致連線中斷。

步驟

1. 選擇*網路>乙太網路連接埠> VLAN*。
2. 選取編輯圖示。
3. 執行下列其中一項：
   - 從清單中選取不同的廣播網域、以變更廣播網域。
   - 清除*已啟用*核取方塊。
4. 儲存您的變更。

刪除 VLAN

從插槽中移除NIC之前、您可能必須先刪除VLAN。當您刪除VLAN時、它會自動從所有使用它的容錯移轉規則和群組中移除。

開始之前

請確定沒有任何與VLAN相關的生命里數。

關於這項工作

從連接埠刪除最後一個VLAN可能會導致網路暫時中斷與連接埠的連線。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**刪除**VLAN**

步驟

1. 選擇*網路>乙太網路連接埠> VLAN*。
2. 選取您要移除的VLAN。
3. 按一下*刪除*。

CLI

使用**CLI**刪除**VLAN**

步驟

使用 `network port vlan delete` 刪除 VLAN 的命令。

以下範例說明如何刪除 VLAN `e1c-80` 從網路連接埠 `e1c` 在節點上 `cluster-1-01`：

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

如"指令參考資料ONTAP"需詳細 `network port vlan delete`資訊，請參閱。

修改 **ONTAP** 網路連接埠屬性

您可以修改實體網路連接埠的自動協商、雙工、流程控制、速度和健全狀況設定。

開始之前

您要修改的連接埠不得裝載任何LIF。

關於這項工作

- 不建議修改100 GbE、40 GbE、10 GbE或1 GbE網路介面的管理設定。

  您為雙工模式和連接埠速度設定的值稱為管理設定。視網路限制而定、管理設定可能會與操作設定有所不同（亦即、雙工模式和連接埠實際使用的速度）。

- 不建議修改介面群組中基礎實體連接埠的管理設定。

  。 `-up-admin` 參數（可在進階權限層級使用）會修改連接埠的管理設定。

- 不建議設定 `-up-admin` 對於節點上的所有連接埠、或是節點上最後一個可運作叢集 LIF 所在的連接埠、系統管理設定為 false 。
- 不建議修改管理連接埠的 MTU 大小、 `e0M`。
- 廣播網域中連接埠的MTU大小無法從為廣播網域設定的MTU值變更。
- VLAN的MTU大小不得超過其基礎連接埠的MTU大小值。

步驟

1. 修改網路連接埠的屬性：

   `network port modify`

2. 您可以設定 `-ignore-health-status` 欄位為 true 、指定系統可以忽略指定連接埠的網路連接埠健全狀況狀態。

   網路連接埠健全狀況狀態會自動從降級變更為健全狀態、而此連接埠現在可用於裝載lifs。您應該將叢集連接埠的流量控制設定為 `none`。依預設、流程控制設定為 `full`。

下列命令會將流程控制項設定為「無」、以停用連接埠e0b上的流程控制：

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

如"指令參考資料ONTAP"需詳細 `network port modify`資訊，請參閱。

轉換 **40GbE NIC** 連接埠，為 **ONTAP** 網路建立 **10GbE** 連接埠

您可以將X1144A-R6和X91440A-R6 40GbE網路介面卡（NIC）轉換成支援四個10GbE連接埠。

如果您要將支援其中一個NIC的硬體平台連接至支援10GbE叢集互連和客戶資料連線的叢集、則必須轉換NIC以提供必要的10GbE連線。

開始之前

您必須使用支援的中斷連接線。

關於這項工作

如需支援NIC的平台完整清單、請參閱 "Hardware Universe"。

> 在X1144A-R6 NIC上、只能轉換連接埠A來支援四個10GbE連線。轉換連接埠A後、連接埠e便無法使用。

步驟

1. 進入維護模式。
2. 將NIC從40GbE支援轉換為10GbE支援。

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. 使用convert命令後、停止節點。
4. 安裝或更換纜線。
5. 視硬體機型而定、請使用SP（服務處理器）或BMC（基礎板管理控制器）將節點關機後再開機、以使轉換生效。

為 **ONTAP** 網路設定 **UTA X1143A-R6** 連接埠

根據預設， X1143A-R6 統一化目標介面卡是以 FC 目標模式設定，但您可以將其連接埠設定為 10 Gb 乙太網路和 FCoE （ CNA ）連接埠，或設定為 16 Gb FC 啟動器或目標連接埠。這需要不同的SFP+介面卡。

當X1143A-R6介面卡設定為乙太網路和FCoE時、可在相同的10-GbE連接埠上支援並行NIC和FCoE目標流量。如果設定為FC、則可針對FC目標或FC啟動器模式個別設定每個共用相同ASIC的雙埠配對。這表示單一X1143A-R6介面卡可在一個雙埠配對上支援FC目標模式、在另一個雙埠配對上支援FC啟動器模式。 連接至相同ASIC的連接埠配對必須設定為相同模式。

在FC模式中、X1143A-R6介面卡的運作速度就像任何現有的FC裝置一樣、最高可達16 Gbps。在CNA模式中、您可以使用X1143A-R6介面卡來同時處理NIC和FCoE流量、並共用相同的10 GbE連接埠。CNA模式僅支援FC目標模式的FCoE功能。

若要設定統一化目標介面卡（X1143A-R6）、您必須在相同的特性設定模式下、在同一個晶片上設定兩個鄰近的連接埠。

步驟

1. 檢視連接埠組態：

```
system hardware unified-connect show
```

2. 視需要設定光纖通道（ FC ）或融合式網路介面卡（ CNA ）的連接埠：

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. 連接FC或10 Gb乙太網路適用的纜線。
4. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該使用8 GB SFP或16 GB SFP、視所連接的FC架構而定。

轉換 **UTA2** 連接埠以用於 **ONTAP** 網路

您可以將 UTA2 連接埠從融合式網路介面卡（ CNA ）模式轉換為光纖通道（ FC ）模式，反之亦然。

當您需要變更連接埠與其網路的實體媒體，或是支援 FC 啟動器和目標時，您應該將 UTA2 特性設定從 CNA 模式變更為 FC 模式。

從 **CNA** 模式到 **FC** 模式

步驟

1. 使介面卡離線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 變更連接埠模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. 重新啟動節點、然後將介面卡上線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 請通知您的管理員或VIF管理程式、視情況刪除或移除連接埠：
   - 如果連接埠作為LIF的主連接埠、介面群組（ifgrp）或主機VLAN的成員、則管理員應執行下列動作：
     - 移動LIF、從ifgrp移除連接埠、或分別刪除VLAN。
     - 執行命令以手動刪除連接埠 `network port delete`。如果 `network port delete`命令失敗，系統管理員應解決錯誤，然後再次執行命令。
   - 如果連接埠不是LIF的主連接埠、不是ifgrp的成員、也不是主控VLAN、則VIF管理程式應在重新開機時從記錄中移除連接埠。如果 VIF 管理程式未移除連接埠，則管理員必須在重新開機後使用命令手動移除該連接埠 `network port delete`。

     如"指令參考資料ONTAP"需詳細 `network port delete`資訊，請參閱。

5. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

   對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該先使用8 GB SFP或16 GB SFP、再變更節點上的組態。

從 **FC** 模式到 **CNA** 模式

步驟

1. 使介面卡離線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 變更連接埠模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. 重新啟動節點
4. 確認您已安裝正確的 SFP+ 。

   對於CNA、您應該使用10Gb乙太網路SFP。

轉換 **ONTAP** 網路的 **CNA/UTA2** 光學模組

您應該變更統一化目標介面卡（CNA/UTA2）上的光學模組、以支援您為介面卡選取的特性設定模式。

步驟

1. 驗證卡中使用的目前SFP+。接著、將目前的SFP+替換為適當的SFP+、以符合偏好的特性設定（FC或CNA）。
2. 從X1143A-R6介面卡移除目前的光纖模組。
3. 針對您偏好的個人化模式（FC或CNA）光纖插入正確的模組。
4. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

支援的SFP+模組和Cisco品牌銅線（雙軸纜線）纜線列於中 "NetApp Hardware Universe"。

從 **ONTAP** 叢集節點移除 **NIC**

您可能必須從插槽中移除故障的NIC、或將NIC移至其他插槽以進行維護。

移除 NIC 的程序與 ONTAP 9.7 和舊版不同。如果需要從運行 ONTAP 9.7 及更早版本的 ONTAP 羣集節點中刪除 NIC ，請參閱過程"從節點移除 NIC （ ONTAP 9.7 或更早版本）"。

步驟

1. 關閉節點電源。
2. 從插槽中實際移除NIC。
3. 開啟節點電源。
4. 確認連接埠已刪除：

```
network port show
```

自動從任何介面群組移除連接埠。ONTAP如果連接埠是介面群組的唯一成員、介面群組就會刪除。如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

5. 如果連接埠上已設定任何VLAN、就會被取代。您可以使用下列命令來檢視已移出的VLAN：

```
cluster controller-replacement network displaced-vlans show
```

。 `displaced-interface show`、 `displaced-vlans show`和 `displaced-vlans restore` 命令是唯一的，不需要以開頭的完整命令名稱 `cluster controller-replacement network`。

6. 這些VLAN會被刪除、但可以使用下列命令還原：

```
displaced-vlans restore
```

7. 如果連接埠上已設定任何LIF、ONTAP 則在同一個廣播網域的另一個連接埠上、會自動為這些LIF選擇新的主連接埠。如果在同一個檔案管理器上找不到合適的主連接埠、則這些生命區會被視為已取代。您可以使用下列命令來檢視已移出的LIF：

   `displaced-interface show`

8. 將新連接埠新增至同一個節點上的廣播網域時、便會自動還原該LIF的主連接埠。或者、您也可以使用設定主連接埠 `network interface modify -home-port -home-node or use the displaced-interface restore` 命令。

相關資訊

- "叢集控制器更換網路置換介面刪除"
- "修改網路介面"

監控網路連接埠

監控 **ONTAP** 網路連接埠的健全狀況

網路連接埠的支援管理包括自動健全狀況監控和一組健全狀況監控、可協助您識別可能不適合裝載生命設備的網路連接埠。ONTAP

關於這項工作

如果健全狀況監視器判定網路連接埠不健全、它會透過EMS訊息警告系統管理員、或將連接埠標記為降級。如果該LIF有健全的替代容錯移轉目標、則可避免在降級的網路連接埠上裝載LIF。ONTAP連接埠可能會因為軟性故障事件而降級、例如連結跳轉（上下快速跳轉連結）或網路分割：

- 當叢集IPspace中的網路連接埠遇到連結Flapping或失去與廣播網域中其他網路連接埠的第2層（L2）連線能力時、它們會標示為降級。

- 非叢集IPspaces中的網路連接埠遇到連結Flapping時、會標示為降級。

您必須瞭解降級連接埠的下列行為：

- 降級的連接埠無法包含在VLAN或介面群組中。

  如果介面群組的成員連接埠已標示為降級、但介面群組仍標示為健全、則該介面群組可裝載lifs。

- LIF會自動從降級的連接埠移轉至正常的連接埠。
- 在容錯移轉事件期間、降級的連接埠不會被視為容錯移轉目標。如果沒有可用的正常連接埠、則降級的連接埠會根據正常的容錯移轉原則來主機生命期。
- 您無法建立、移轉LIF或將其還原為降級連接埠。

  您可以修改 `ignore-health-status` 將網路連接埠設定為 `true`。然後、您可以在健全的連接埠上裝載LIF。

步驟

1. 登入進階權限模式：

   ```
   set -privilege advanced
   ```

2. 檢查啟用哪些健全狀況監視器來監控網路連接埠健全狀況：

   ```
   network options port-health-monitor show
   ```

   連接埠的健全狀況狀態取決於健全狀況監視器的值。

   下列健全狀況監視器預設ONTAP 可在支援中使用：

   - 連結Flapping健全狀況監視器：監控連結Flapping

     如果連接埠在五分鐘內有一次以上的連結Flapping、則此連接埠會標示為降級。

   - L2可到達性健全狀況監視器：監控同一個廣播網域中設定的所有連接埠是否彼此具有L2可到達性

     此健全狀況監視器會報告所有IPspace中的L2可連線性問題、但只會將叢集IPspace中的連接埠標記為降級。

   - crc監控：監控連接埠上的crc統計資料

     此健全狀況監視器不會將連接埠標記為降級、但會在觀察到極高的CRC故障率時產生EMS訊息。

   如"指令參考資料ONTAP"需詳細 `network options port-health-monitor show`資訊，請參閱。

3. 使用啟用或停用 IPspace 的任何健全狀況監視器 `network options port-health-monitor modify` 命令。

   如"指令參考資料ONTAP"需詳細 `network options port-health-monitor modify`資訊，請參閱。

4. 檢視連接埠的詳細健全狀況：

```
network port show -health
```

命令輸出會顯示連接埠的健全狀況狀態、 `ignore health status` 設定、以及連接埠標示為降級的原因清單。

連接埠健全狀況狀態可以是 `healthy` 或 `degraded`。

如果是 `ignore health status` 設定為 `true`、表示連接埠健全狀況狀態已從修改 `degraded` 至 `healthy` 由管理員提供。

如果是 `ignore health status` 設定為 `false`，連接埠健全狀況狀態會由系統自動決定。

如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

監控 **ONTAP** 網路連接埠的連線能力

可到達性監控功能已內建ONTAP 於更新版本的更新版本中。使用此監控功能來識別實體網路拓撲與ONTAP 該功能組態不相符的情況。在某些情況下ONTAP 、無法連線的連接埠可修復。在其他情況下、需要採取其他步驟。

關於這項工作

使用這些命令來驗證、診斷及修復ONTAP 因不符合實體纜線或網路交換器組態的物件組態而產生的網路錯誤組態。

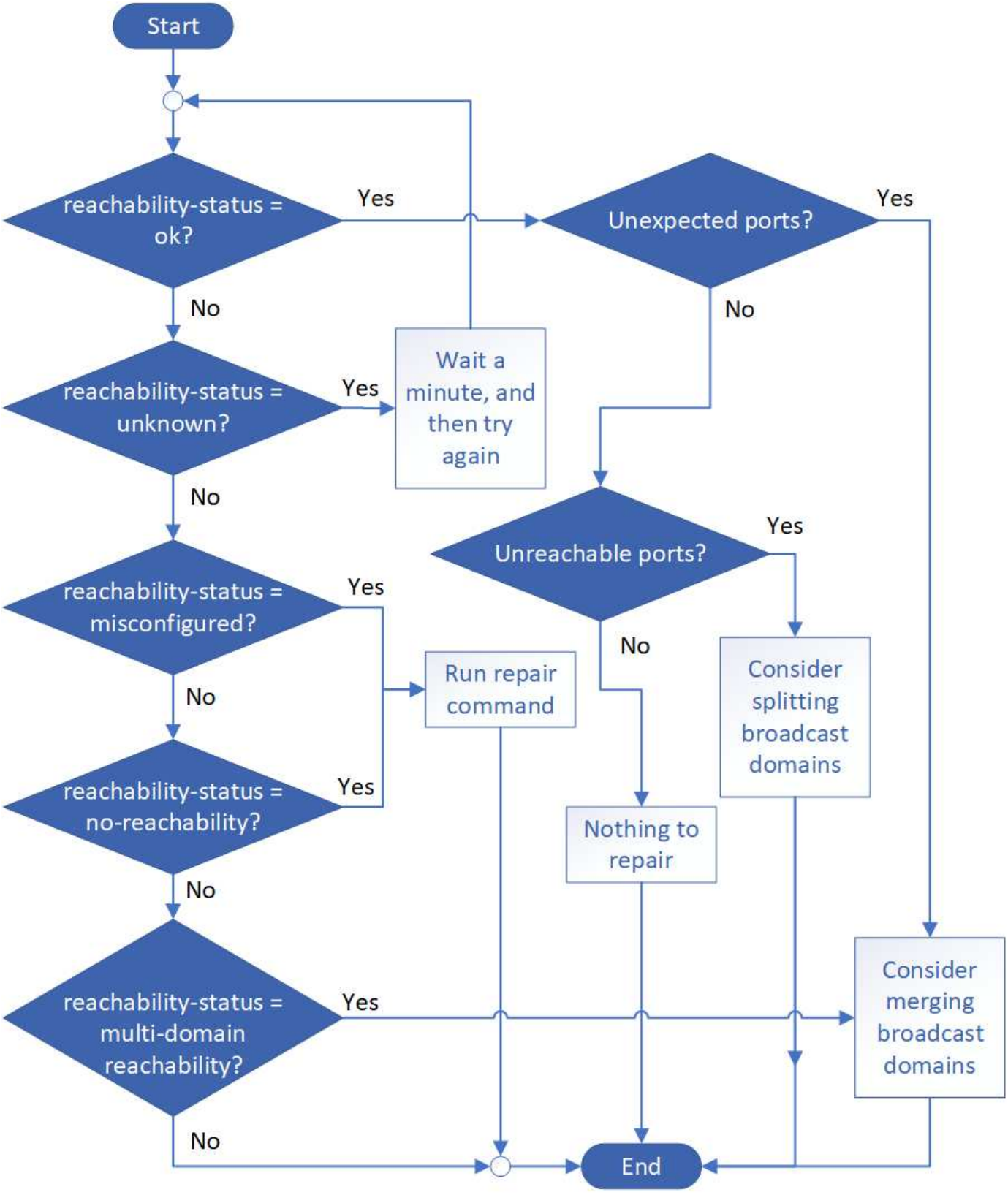
步驟

1. 檢視連接埠連線性：

```
network port reachability show
```

   如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

2. 請使用下列決策樹狀結構和表格來判斷下一個步驟（如果有）。


Start
reachability-status = ok?
Yes
Unexpected ports?
Yes
No
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
No
reachability-status = no-reachability?
Yes
Nothing to repair
No
reachability-status = multi-domain reachability?
Yes
Consider merging broadcast domains
No
End

連線狀態	說明

好的	連接埠可連線至其指派的廣播網域的第2層。 如果連線狀態為「正常」、但有「非預期的連接埠」、請考慮合併一或多個廣播網域。如需詳細資訊、請參閱下列_Unexpected連接埠_資料列。 如果連線狀態為「正常」、但有「無法連線的連接埠」、請考慮分割一或多個廣播網域。如需詳細資訊、請參閱下列_Unreachable連接埠_資料列。 如果連線狀態為「正常」、而且沒有非預期或無法連線的連接埠、表示您的組態正確。
非預期的連接埠	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷其是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
無法連線的連接埠	如果單一廣播網域已分割成兩個不同的連線能力集、您可以分割廣播網域、將ONTAP 此功能與實體網路拓撲進行同步。 一般而言、無法連線的連接埠清單會定義在您確認實體和交換器組態正確之後、應分割成另一個廣播網域的一組連接埠。 如需詳細資訊、請參閱 "分割廣播網域"。
設定錯誤的連線能力	連接埠無法連線至其指派的廣播網域的第2層；不過連接埠確實可連線至不同的廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給可連線的廣播網域： `network port reachability repair -node -port` 如需詳細資訊、請參閱 "修復連接埠連線能力"。
不可到達性	連接埠無法連線至任何現有廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給預設IPspace中自動建立的新廣播網域： `network port reachability repair -node -port`如需更多資訊"修復連接埠連線能力"，請參閱。如"指令參考資料ONTAP"需詳細 `network port reachability repair`資訊，請參閱。
多網域連線能力	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷其是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域" 或 "修復連接埠連線能力"。

不明	如果連線狀態為「未知」、請稍候幾分鐘、然後再試一次命令。

修復連接埠之後、您需要檢查並解決已移轉的LIF和VLAN。如果連接埠是介面群組的一部分、您也需要瞭解該介面群組發生了什麼事。如需詳細資訊、請參閱 "修復連接埠連線能力"。

瞭解 **ONTAP** 網路上的連接埠使用情形

有幾個知名連接埠是專為 ONTAP 與特定服務的通訊所保留。如果儲存網路環境中的連接埠值與 ONTAP 連接埠上的值相同，就會發生連接埠衝突。

傳入流量

ONTAP 儲存設備上的傳入流量使用下列通訊協定和連接埠：

傳輸協定	連接埠	目的
所有 ICMP	全部	Ping 執行個體
TCP	22	安全 Shell 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	80	網頁存取叢集管理 LIF 的 IP 位址
TCP/UDP	111.	rpcbind ，遠端程序呼叫 NFS
UDP	123.	NTP ，網路時間傳輸協定
TCP	135.	MSRPC ， Microsoft 遠端程序呼叫
TCP	139.	NetBIOS-SSN ，適用於 CIFS 的 NetBios 服務工作階段
TCP/UDP	161-162	SNMP ，簡易網路管理傳輸協定
TCP	443.	安全的網頁存取叢集管理 LIF 的 IP 位址
TCP	445.	MS Active Domain Services ， Microsoft SMB/CIFS over TCP 搭配 NetBIOS 架構
TCP/UDP	635	NFS 裝載可與遠端檔案系統互動，就像是本機檔案系統一樣
TCP	749.	Kerberos
UDP	953.	名稱精靈
TCP/UDP	2049.	NFS 伺服器精靈
TCP	2050.	NRV ， NetApp 遠端 Volume 傳輸協定
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP/UDP	4045	NFS 鎖定精靈
TCP/UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS RPC Rquotad
UDP	4444.	KRB524 ， Kerberos 524

UDP	5353.	多點傳送DNS
TCP	10000.	使用網路資料管理傳輸協定（ NDMP ）進行備份
TCP	11104.	叢集對等，雙向管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	叢集對等，雙向 SnapMirror 資料傳輸，使用叢集間的生命週期
SSL/TLS	30000	透過安全通訊端 (SSL/TLS) 接受 DMA 和 NDMP 伺服器之間的 NDMP 安全控制連線。安全掃描器可以報告連接埠 30000 上的漏洞。

傳出流量

您可以根據業務需求，使用基本或進階規則來設定 ONTAP 儲存設備上的輸出流量。

基本傳出規則

所有連接埠都可用於透過 ICMP ， TCP 和 UDP 傳輸協定的所有輸出流量。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的輸出流量規則，可以使用下列資訊，只開啟 ONTAP 輸出通訊所需的連接埠。

Active Directory

傳輸協定	連接埠	來源	目的地	目的
TCP	88.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ， iSCSI ）	Active Directory 樹系	Kerberos V 驗證
UDP	137.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 名稱服務
UDP	138.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 資料報服務
TCP	139.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 服務工作階段
TCP	389.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	LDAP
UDP	389.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	LDAP
TCP	445.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構

TCP	464	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	變更並設定 Kerberos V 密碼（ set_change ）
UDP	464	節點管理 LIF ， Data LIF （ NFS ， CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
TCP	749.	節點管理 LIF ， Data LIF （ NFS ， CIFS ）	Active Directory 樹系	變更並設定 Kerberos V 密碼（ RPCSEC_GSS ）

AutoSupport

傳輸協定	連接埠	來源	目的地	目的
TCP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP時、AutoSupport

SNMP

傳輸協定	連接埠	來源	目的地	目的
TCP/UDP	162.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控

SnapMirror

傳輸協定	連接埠	來源	目的地	目的
TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段

其他服務

傳輸協定	連接埠	來源	目的地	目的
TCP	25.	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
UDP	67.	節點管理 LIF	DHCP	DHCP伺服器
UDP	68.	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息
TCP	5010.	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業
TCP	18600 至 18699	節點管理 LIF	目的地伺服器	NDMP 複本

瞭解 **ONTAP** 內部連接埠

下表列出了 ONTAP 內部使用的連接埠及其功能。 ONTAP使用這些連接埠執行各種功能，

例如建立叢集內 LIF 通訊。

此列表並不詳盡，並且可能在不同環境中有所不同。

連接埠/傳輸協定	組件/功能
514	系統記錄
900	NetApp叢集RPC
902.	NetApp叢集RPC
904	NetApp叢集RPC
905)	NetApp叢集RPC
910	NetApp叢集RPC
911	NetApp叢集RPC
913	NetApp叢集RPC
914	NetApp叢集RPC
159.15	NetApp叢集RPC
918	NetApp叢集RPC
920	NetApp叢集RPC
921.	NetApp叢集RPC
924	NetApp叢集RPC
925	NetApp叢集RPC
927	NetApp叢集RPC
928	NetApp叢集RPC
929	NetApp叢集RPC
930	核心服務與管理功能（KSMF）
931	NetApp叢集RPC
932.	NetApp叢集RPC
933	NetApp叢集RPC
934	NetApp叢集RPC
935	NetApp叢集RPC
936.	NetApp叢集RPC
937	NetApp叢集RPC
939	NetApp叢集RPC
940	NetApp叢集RPC
951.	NetApp叢集RPC
954	NetApp叢集RPC

95	NetApp叢集RPC
956.	NetApp叢集RPC
958	NetApp叢集RPC
961.	NetApp叢集RPC
963,	NetApp叢集RPC
969.64	NetApp叢集RPC
9666	NetApp叢集RPC
967	NetApp叢集RPC
975	金鑰管理互通性傳輸協定（KMIP）
982.	NetApp叢集RPC
983.	NetApp叢集RPC
5125.	磁碟的備用控制連接埠
5133	磁碟的備用控制連接埠
51444.	磁碟的備用控制連接埠
65502	節點範圍SSH
65503	LIF共用
7700	叢集會話管理器 (CSM)
7810.	NetApp叢集RPC
7811.	NetApp叢集RPC
7812.	NetApp叢集RPC
7813.	NetApp叢集RPC
7814	NetApp叢集RPC
（—	NetApp叢集RPC
7816	NetApp叢集RPC
7817.	NetApp叢集RPC
7818.	NetApp叢集RPC
7819	NetApp叢集RPC
7820	NetApp叢集RPC
7821	NetApp叢集RPC
7822.	NetApp叢集RPC
7823	NetApp叢集RPC
7824	NetApp叢集RPC
7835-7839 及 7845-7849	用於集群內通訊的 TCP 連接埠
8023.	節點範圍Telnet

8443	適用於 Amazon FSx 的 ONTAP S3 NAS 連接埠
8514.	節點範圍RSH
9877	KMIP用戶端連接埠（僅限內部本機主機）
10006	用於 HA 互連通訊的 TCP 連接埠

IPspaces

瞭解 **ONTAP IPspace** 組態

IPspaces可讓您設定單ONTAP 一的支援叢集、讓用戶端從多個管理性獨立的網路網域存取、即使這些用戶端使用相同的IP位址子網路範圍也一樣。如此可將用戶端流量區隔、以確保隱私與安全。

IPspace可定義儲存虛擬機器（SVM）所在的獨特IP位址空間。為IPspace定義的連接埠和IP位址僅適用於該IPspace。IPspace內的每個SVM都會有一個不同的路由表、因此不會發生跨SVM或跨IPspace流量路由傳送。

IPspace可在其路由網域上同時支援IPv6位址。

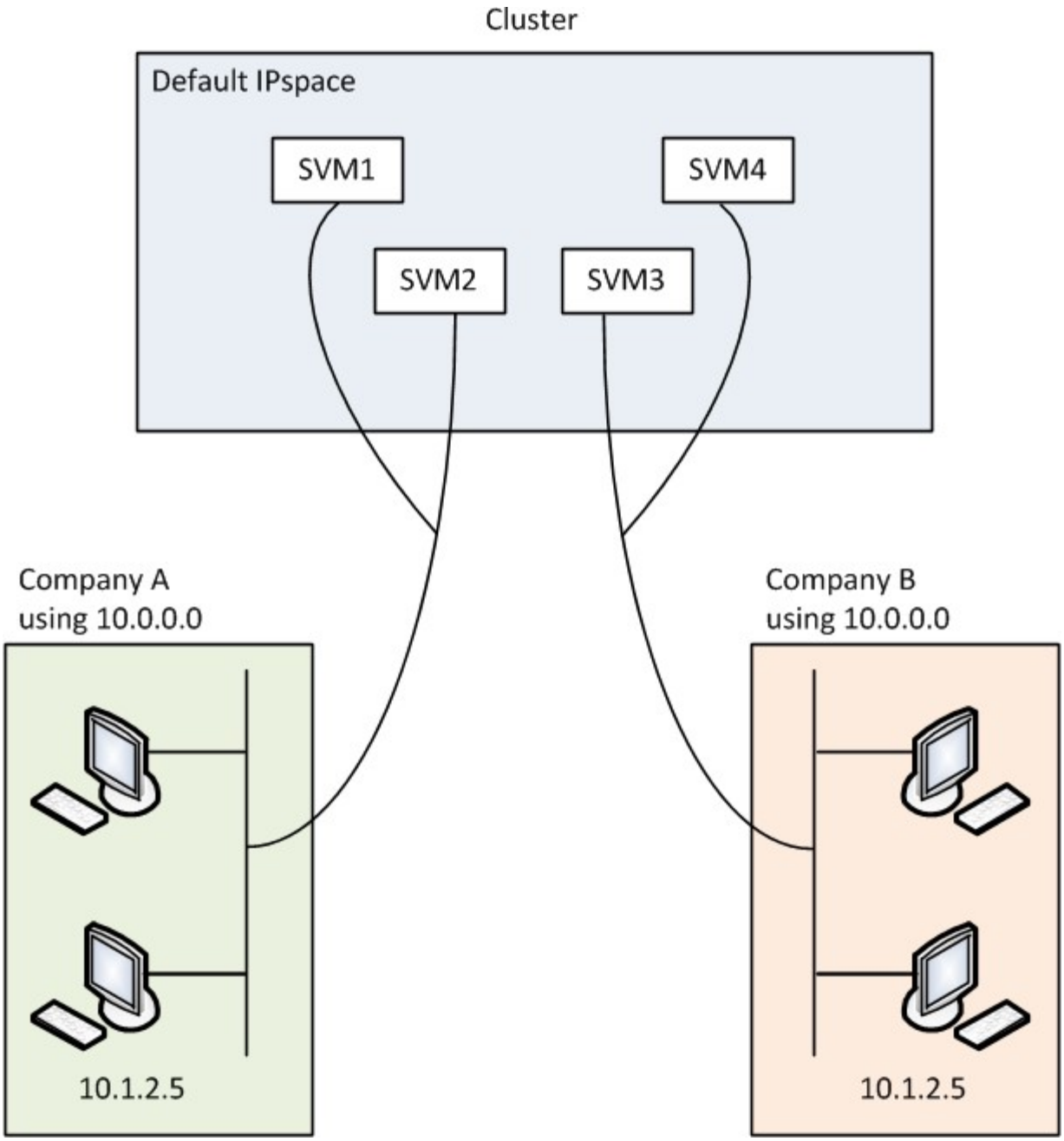
如果您要管理單一組織的儲存設備、則不需要設定IPspaces。如果您要在單ONTAP 一的一套叢集上管理多家公司的儲存設備、而且您確定您的客戶都沒有衝突的網路組態、那麼您也不需要使用IPspaces。在許多情況下、使用儲存虛擬機器（SVM）及其各自獨特的IP路由表、可用來分隔獨特的網路組態、而非使用IPspace。

使用**IPspaces**的範例

使用IPspaces的常見應用程式、是儲存服務供應商（SSP）需要將公司A和B的客戶連接ONTAP 到SSP內部部署上的一個支援叢集、而兩家公司都使用相同的私有IP位址範圍。

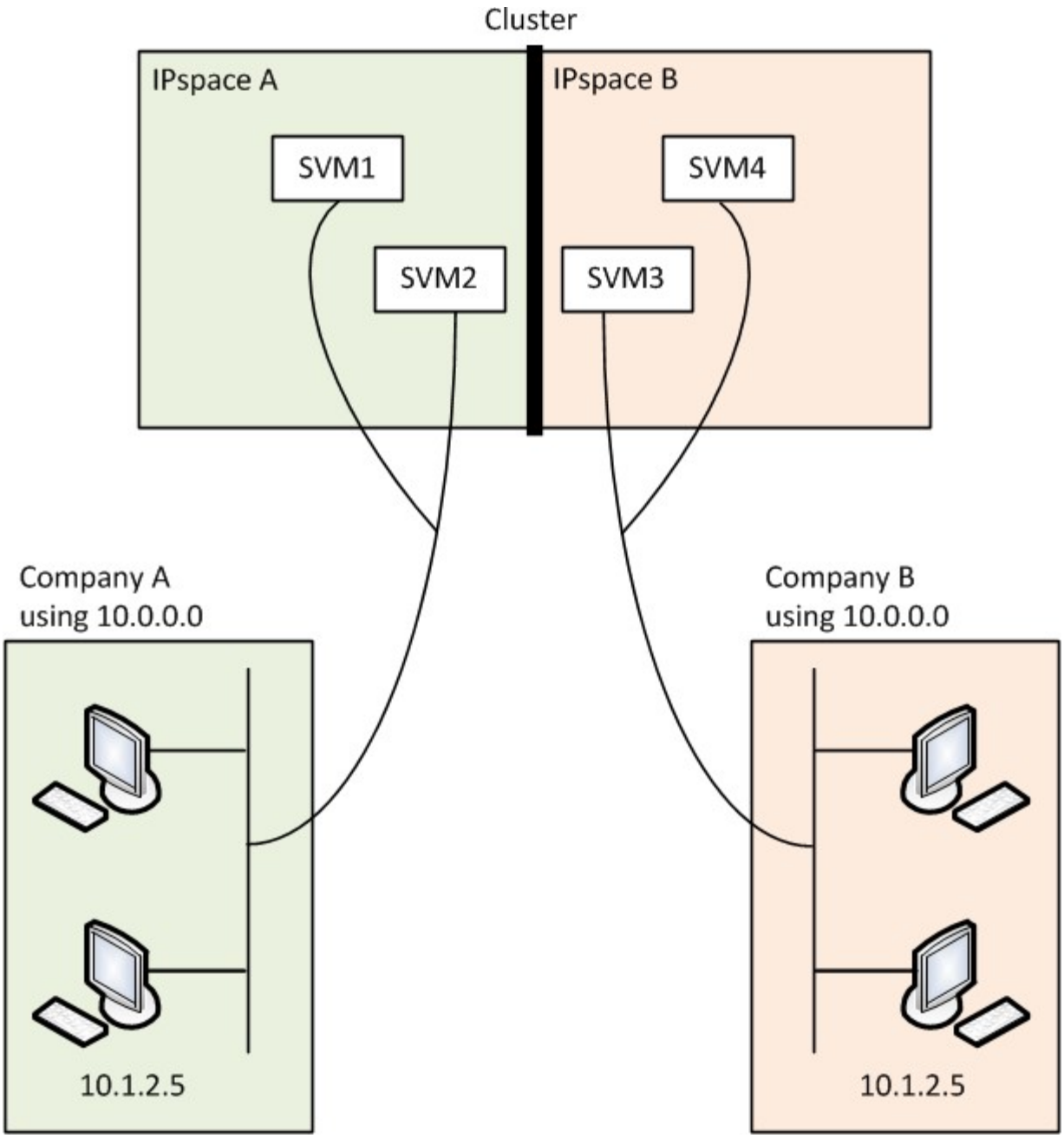
SSP會在叢集上為每位客戶建立SVM、並提供從兩個SVM到公司A網路的專用網路路徑、以及從其他兩個SVM到公司B網路的專用網路路徑。

下圖顯示這種部署類型、如果兩家公司都使用非私有IP位址範圍、就能正常運作。不過、圖例顯示兩家公司使用相同的私有IP位址範圍、這會造成問題。



兩家公司都使用私有IP位址子網路10.0.0.0、造成下列問題：

- 如果兩家公司決定為其各自的SVM使用相同的IP位址、則位於SSP位置之叢集中的SVM會有衝突的IP位址。
- 即使兩家公司同意使用不同的IP位址來處理SVM、也可能發生問題。
- 例如，如果網路中的任何用戶端與B網路中的用戶端具有相同的IP位址，則發往A位址空間中用戶端的封包可能會路由傳送到B位址空間中的用戶端，反之亦然。
- 如果兩家公司決定使用互不相容的位址空間（例如、A使用10.0.0.0、網路遮罩為255.128.0.0、B使用10.128.0.0、網路遮罩為255.128.8.0）、 SSP需要在叢集上設定靜態路由、以便將流量適當路由傳送到A和B的網路。
- 此解決方案既不可擴充（因為靜態路由）、也不安全（廣播流量會傳送至叢集的所有介面）。為了克服這些問題、SSP會在叢集上定義兩個IPspace、每個公司一個。由於不路由跨IP空間的流量、因此即使所有SVM都設定在10.0.0.0位址空間中、每家公司的資料仍會安全地路由至其各自的網路、如下圖所示：



此外、各種組態檔案（例如）所參照的 IP 位址 `/etc/ hosts` 檔案 `/etc/hosts.equiv` 檔案、和 `the /etc/rc` 檔案、與該 IPspace 相關。因此、IPspaces可讓SSP針對多個SVM的組態和驗證資料、設定相同的IP位址、而不會發生衝突。

IPspaces的標準屬性

首次建立叢集時、預設會建立特殊的IPspaces。此外、還會針對每個IPspace建立特殊的儲存虛擬機器（SVM）。

初始化叢集時會自動建立兩個IPspace：

- 「預設」IPspace

  此IPspace是連接埠、子網路和SVM的容器、用於提供資料。如果您的組態不需要用戶端個別的IPspace、則可在此IPspace中建立所有SVM。此IPspace也包含叢集管理和節點管理連接埠。

- 「叢集」IPspace

  此IPspace包含叢集中所有節點的所有叢集連接埠。它會在建立叢集時自動建立。可連線至內部私有叢集網路。當其他節點加入叢集時、這些節點的叢集連接埠會新增至「叢集」IPspace。

每個IPspace都有一個「系統」SVM。當您建立IPspace時、會建立名稱相同的預設系統SVM：

- 「叢集」IPspace的系統SVM會在內部私有叢集網路上的叢集節點之間傳輸叢集流量。

  它由叢集管理員管理、名稱為「叢集」。

- 「預設」IPspace的系統SVM會傳輸叢集和節點的管理流量、包括叢集之間的叢集間流量。

  它由叢集管理員管理、使用與叢集相同的名稱。

- 您所建立的自訂IPspace系統SVM會承載該SVM的管理流量。

  它由叢集管理員管理、使用與IPspace相同的名稱。

一個IPspace中可以存在一個或多個用於用戶端的SVM。每個用戶端SVM都有自己的資料磁碟區和組態、並獨立管理其他SVM。

為 ONTAP 網路建立 IPspace

IPspaces是儲存虛擬機器（SVM）所在的不同IP位址空間。當您需要SVM擁有自己的安全儲存、管理和路由時、可以建立IPspaces。您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

關於這項工作

整個叢集的IP空間上限為512個。對於包含具有 6 GB RAM 的節點的叢集、叢集範圍限制會減至 256 個 IPspace 。請參閱Hardware Universe 《參考資訊（英文）：判斷您的平台是否有其他限制。

"NetApp Hardware Universe"

IPspace名稱不能為「ALL」、因為「ALL」是系統保留的名稱。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立IPspace：

   ```
   network ipspace create -ipspace ipspace_name
   ```

   `ipspace_name` 為您要建立的 IPspace 名稱。下列命令會在叢集上建立IPspace ipspace1：

```
network ipspace create -ipspace ipspace1
```

如"指令參考資料ONTAP"需詳細 `network ipspace create`資訊，請參閱。

2. 顯示 IPspaces ：

   `network ipspace show`

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ----------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

IPspace隨系統SVM一起建立、用於IPspace。系統SVM可傳輸管理流量。

完成後

如果您在MetroCluster 具有不含任何組態的叢集中建立IPspace、則必須手動將IPspace物件複寫到合作夥伴叢集。在IPspace複寫之前建立並指派給IPspace的任何SVM、將不會複寫到合作夥伴叢集。

廣播網域會自動在「預設」IPspace中建立、並可使用下列命令在IPspaces之間移動：

```
network port broadcast-domain move
```

例如、如果您想要使用下列命令、將廣播網域從「預設」移至「ips1」：

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

檢視 **ONTAP** 網路上的 **IPspace**

您可以顯示叢集中存在的IPspaces清單、也可以檢視指派給每個IPspace的儲存虛擬機器（SVM）、廣播網域和連接埠。

步驟

顯示叢集中的IPspaces和SVM：

```
network ipspace show [-ipspace ipspace_name]
```

下列命令會顯示叢集中的所有IPspaces、SVM和廣播網域：

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  ------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

下列命令會顯示屬於IPspace ipspace1的節點和連接埠：

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

如"指令參考資料ONTAP"需詳細 `network ipspace show`資訊，請參閱。

從 ONTAP 網路刪除 IPspace

如果不再需要IPspace、您可以將其刪除。

開始之前

不得有廣播網域、網路介面或SVM與您要刪除的IPspace相關聯。

系統定義的「預設」和「叢集」IPspaces無法刪除。

步驟

刪除IPspace：

```
network ipspace delete -ipspace ipspace_name
```

下列命令會從叢集刪除IPspace ipspace1：

```
network ipspace delete -ipspace ipspace1
```

如"指令參考資料ONTAP"需詳細 `network ipspace delete`資訊，請參閱。

廣播網域

瞭解 ONTAP 廣播網域

廣播網域的目的是將屬於同一層網路的網路連接埠分組。然後、儲存虛擬機器（SVM）便可使用群組中的連接埠來處理資料或管理流量。

ONTAP 9.7 和舊版中的廣播網域管理方式有所不同。如果您需要在運行 ONTAP 9.7 及更早版本的網絡上管理廣播域，請"廣播網域總覽（ ONTAP 9.7 及更早版本）"參閱。

廣播網域位於IPspace中。在叢集初始化期間、系統會建立兩個預設廣播網域：

- 「預設」廣播網域包含「預設」IPspace中的連接埠。

  這些連接埠主要用於提供資料。叢集管理和節點管理連接埠也位於此廣播網域中。

- 「叢集」廣播網域包含「叢集」IPspace中的連接埠。

  這些連接埠用於叢集通訊、並包含叢集中所有節點的所有叢集連接埠。

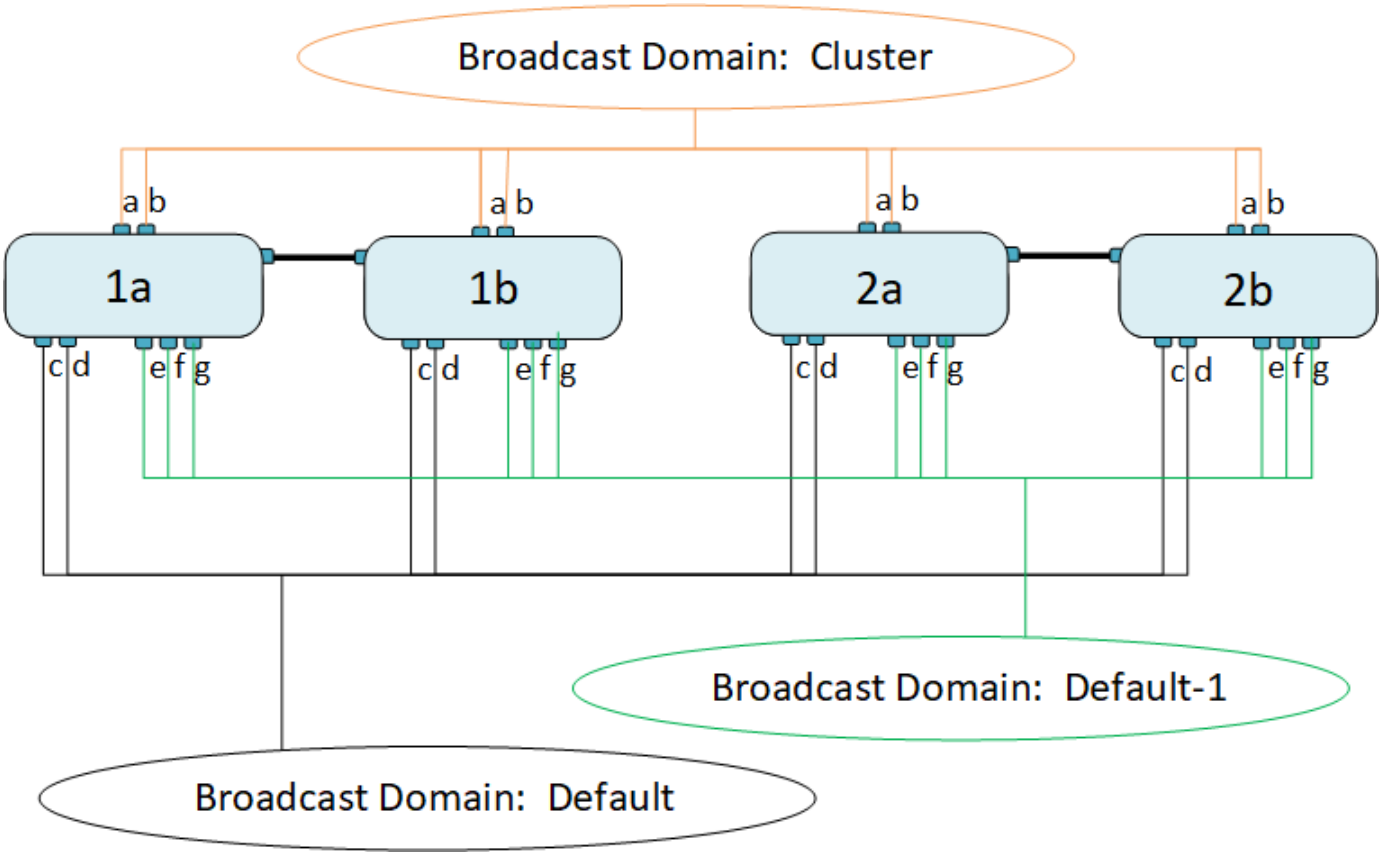
  必要時、系統會在預設IPspace中建立額外的廣播網域。「預設」廣播網域包含管理LIF的主連接埠、以及任何其他連接埠具有該連接埠第2層可連線性的連接埠。其他廣播網域的名稱為「預設值-1」、「預設值-2」等。

使用廣播網域的範例

廣播網域是同一個IPspace中的一組網路連接埠、也能彼此連接第2層、通常包括叢集中許多節點的連接埠。

下圖顯示指派給四節點叢集中三個廣播網域的連接埠：

- 叢集初始化期間會自動建立「叢集」廣播網域、其中包含叢集中每個節點的連接埠a和b。
- 叢集初始化期間也會自動建立「預設」廣播網域、其中包含叢集中每個節點的連接埠c和d。
- 系統會根據第2層網路連線能力、在叢集初始化期間自動建立任何其他廣播網域。這些額外的廣播網域命名為「預設-1」、「預設-2」等。



系統會自動建立名稱相同且與每個廣播網域具有相同網路連接埠的容錯移轉群組。此容錯移轉群組是由系統自動管理、也就是說、當連接埠從廣播網域新增或移除時、它們會自動從這個容錯移轉群組中新增或移除。

建立 ONTAP 廣播網域

廣播網域會將叢集中屬於同一個第2層網路的網路連接埠分組。然後、SVM便可使用這些連接埠。

廣播網域會在叢集建立或加入作業期間自動建立。從ONTAP 功能更新9.12.0開始、除了自動建立的廣播網域之外、您也可以在System Manager中手動新增廣播網域。

建立廣播網域的程序與 ONTAP 9.7 和舊版不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上創建廣播域，請"建立廣播網域（ ONTAP 9.7 及更早版本）"參閱。

開始之前

您打算新增至廣播網域的連接埠不得屬於其他廣播網域。如果您要使用的連接埠屬於另一個廣播網域、但未使用、請從原始廣播網域移除這些連接埠。

關於這項工作

- 所有廣播網域名稱在IPspace內必須是唯一的。
- 新增至廣播網域的連接埠可以是實體網路連接埠、VLAN或連結集合群組/介面群組（LAG / ifgrps）。
- 如果您要使用的連接埠屬於另一個廣播網域、但未使用、請先將它們從現有的廣播網域中移除、再將它們新增至新的廣播網域。
- 新增至廣播網域之連接埠的最大傳輸單元（MTU）會更新為廣播網域中設定的MTU值。

- MTU值必須符合連接至該層2網路的所有裝置、但e0M連接埠處理管理流量除外。
- 如果您未指定IPspace名稱、則會在「預設」IPspace中建立廣播網域。

為了簡化系統組態、系統會自動建立同名的容錯移轉群組、其中包含相同的連接埠。

系統管理員

步驟

1. 選擇*網路>總覽>廣播網域*。
2. 按一下 + Add
3. 命名廣播網域。
4. 設定MTU。
5. 選取IPspace。
6. 儲存廣播網域。

您可以在新增廣播網域之後編輯或刪除該網域。

CLI

如果您使用的是 ONTAP 9.8 及更新版本、則會根據第 2 層的連線能力、自動建立廣播網域。如需詳細資訊、請參閱 "修復連接埠連線能力"。

您也可以手動建立廣播網域。

步驟

1. 檢視目前未指派給廣播網域的連接埠：

   ```
   network port show
   ```

   如果顯示器很大、請使用 `network port show -broadcast-domain` 僅檢視未指派連接埠的命令。

2. 建立廣播網域：

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` 是您要建立的廣播網域名稱。

   b. `mtu_value` 為 IP 封包的 MTU 大小； 1500 和 9000 為典型值。

      此值會套用至新增至此廣播網域的所有連接埠。

   c. `ipspace_name` 是要新增此廣播網域的 IPspace 名稱。

      除非您指定此參數的值、否則會使用「預設」IPspace。

   d. `ports_list` 是要新增至廣播網域的連接埠清單。

      連接埠會以格式新增 `node_name:port_number`例如、 `node1:e0c`。

3. 確認已視需要建立廣播網域：

   ```
   network port show -instance -broadcast-domain new_domain
   ```

如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

範例

下列命令會在預設IPspace中建立廣播網域bcast1、將MTU設為1500、並新增四個連接埠：

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain create`資訊，請參閱。

完成後

您可以透過建立子網路來定義廣播網域中可用的IP位址集區、或是現在可以將SVM和介面指派給IPspace。如需更多資訊、請參閱 "叢集與SVM對等關係"。

如果您需要變更現有廣播網域的名稱、請使用 `network port broadcast-domain rename` 命令。

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain rename`資訊，請參閱。

從 ONTAP 廣播網域新增或移除連接埠

廣播網域會在叢集建立或加入作業期間自動建立。您不需要從廣播網域手動移除連接埠。

如果網路連接埠連線能力已變更、無論是透過實體網路連線或交換器組態、而且網路連接埠屬於不同的廣播網域、請參閱下列主題：

"修復連接埠連線能力"

新增或移除廣播網域連接埠的程序與 ONTAP 9.7 和舊版不同。如果您需要在執行 ONTAP 9.7 及更早版本的網路上，從廣播網域新增或移除連接埠"從廣播網域新增或移除連接埠（ ONTAP 9.7 及更早版本）"，請參閱。

系統管理員

從 ONTAP 9.14.1 開始、您可以使用系統管理員在廣播網域之間重新指派乙太網路連接埠。建議您將每個乙太網路連接埠指派給廣播網域。因此、如果您從廣播網域取消指派乙太網路連接埠、則必須將其重新指派給不同的廣播網域。

步驟

若要重新指派乙太網路連接埠、請執行下列步驟：

1. 選擇 * 網路 > 總覽 * 。
2. 在 * 廣播網域 * 區段中、選取 ⋮ 網域名稱旁的。
3. 在下拉式功能表中、選取*編輯*。
4. 在 * 編輯廣播網域 * 頁面上、取消選取您要重新指派給其他網域的乙太網路連接埠。
5. 對於每個取消選取的連接埠、會顯示 * 重新指派乙太網路連接埠 * 視窗。選取您要重新指派連接埠的廣播網域，然後選取 * 重新指派 * 。
6. 選取您要指派給目前廣播網域的所有連接埠、然後儲存變更。

CLI

如果網路連接埠連線能力已變更、無論是透過實體網路連線或交換器組態、而且網路連接埠屬於不同的廣播網域、請參閱下列主題：

"修復連接埠連線能力"

或者、您也可以使用手動新增或移除廣播網域的連接埠 `network port broadcast-domain add-ports` 或 `network port broadcast-domain remove-ports` 命令。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您打算新增至廣播網域的連接埠不得屬於其他廣播網域。
- 已屬於介面群組的連接埠無法個別新增至廣播網域。

關於這項工作

新增和移除網路連接埠時、適用下列規則：

新增連接埠時…	移除連接埠時…
連接埠可以是網路連接埠、VLAN或介面群組（ifgrps）。	不適用
這些連接埠會新增至廣播網域的系統定義容錯移轉群組。	這些連接埠會從廣播網域中的所有容錯移轉群組中移除。
連接埠的MTU會更新為廣播網域中設定的MTU值。	連接埠的MTU不變。
連接埠的IPspace會更新為廣播網域的IPspace值。	這些連接埠會移至「預設」IPspace、且不含廣播網域屬性。

如果使用命令移除介面群組的最後一個成員連接埠 `network port ifgrp remove-port`，則會導致介面群組連接埠從廣播網域中移除，因為廣播網域中不允許使用空的介面群組連接埠。如"指令參考資料ONTAP"需詳細 `network port ifgrp remove-port`資訊，請參閱。

步驟

1. 使用顯示目前指派或未指派給廣播網域的連接埠 `network port show` 命令。
2. 從廣播網域新增或移除網路連接埠：

如果您想要…	使用…
新增連接埠至廣播網域	`network port broadcast-domain add-ports`
從廣播網域移除連接埠	`network port broadcast-domain remove-ports`

3. 確認已從廣播網域新增或移除連接埠：

   `network port show`

   如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

新增和移除連接埠的範例

下列命令會將節點叢集上的連接埠e0g與節點叢集上的連接埠e0g新增至預設IPspace中的廣播網域bcast1：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

下列命令會在叢集IPspace中新增兩個叢集連接埠以廣播網域叢集：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

下列命令會從預設IPspace的廣播網域bcast1中移除節點叢集1上的連接埠e0e：

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain remove-ports`資訊，請參閱。

相關資訊

- "指令參考資料ONTAP"

修復 ONTAP 連接埠連線能力

系統會自動建立廣播網域。但是、如果連接埠已重新標記、或交換器組態變更、則可能需要將連接埠修復至不同的廣播網域（新的或現有的）。

根據廣播網域成員（乙太網路連接埠）的第2層連通性、可自動偵測並建議網路線路問題的解決方案。ONTAP

錯誤的佈線可能會導致非預期的廣播網域連接埠指派。從ONTAP 版本號《21：1：2》（《2：2：2）開始、叢集會在叢集設定後或新節點加入現有叢集時、透過驗證連接埠可連線性、自動檢查網路配線問題。

系統管理員

如果偵測到連接埠連線性問題、System Manager會建議您執行修復作業來解決問題。

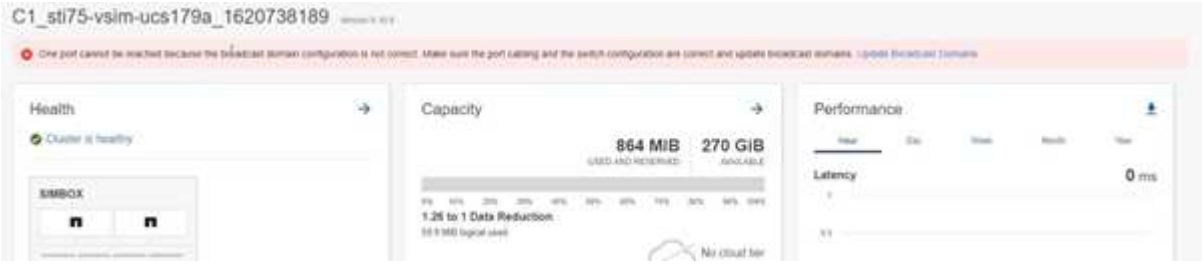
設定叢集之後、儀表板上會報告網路配線問題。

將新節點加入叢集之後、「節點」頁面上會出現網路配線問題。

您也可以在網路圖上檢視網路配線健全狀況。連接埠連線能力問題會在網路圖中以紅色的錯誤圖示表示。

叢集後設定

設定叢集之後、如果系統偵測到網路配線問題、儀表板上會出現一則訊息。



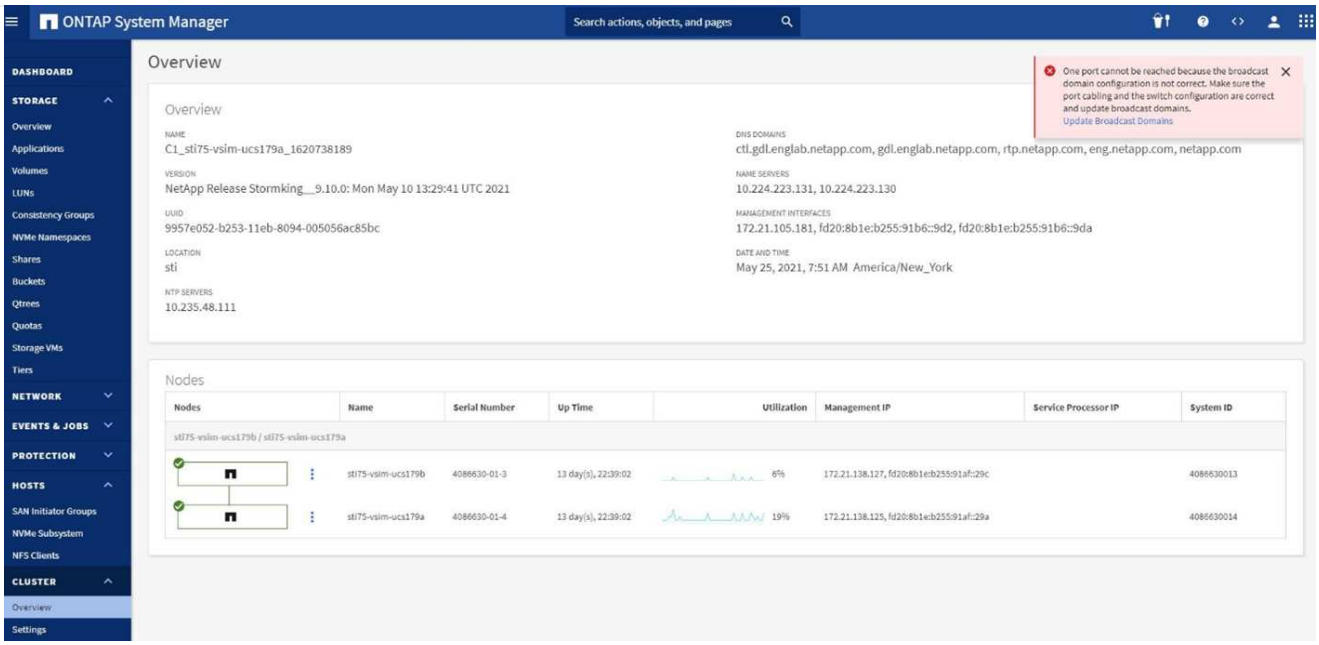
步驟

1. 按照訊息中的建議修正線路。
2. 按一下連結以啟動「更新廣播網域」對話方塊。
   「更新廣播網域」對話方塊隨即開啟。

3. 檢閱連接埠的相關資訊、包括節點、問題、目前的廣播網域及預期的廣播網域。
4. 選取您要修復的連接埠、然後按一下「修復」。
   系統會將連接埠從目前的廣播網域移至預期的廣播網域。

POST節點加入

將新節點加入叢集之後、如果系統偵測到網路配線問題、節點頁面上會出現一則訊息。



步驟

1. 按照訊息中的建議修正線路。
2. 按一下連結以啟動「更新廣播網域」對話方塊。
   「更新廣播網域」對話方塊隨即開啟。

3. 檢閱連接埠的相關資訊、包括節點、問題、目前的廣播網域及預期的廣播網域。
4. 選取您要修復的連接埠、然後按一下「修復」。
   系統會將連接埠從目前的廣播網域移至預期的廣播網域。

CLI

開始之前

您必須是叢集管理員才能執行此工作。

關於這項工作

您可以使用命令、根據ONTAP 由停止偵測到的第2層可到達性、自動修復連接埠的廣播網域組態。

步驟

1. 檢查交換器組態和纜線。

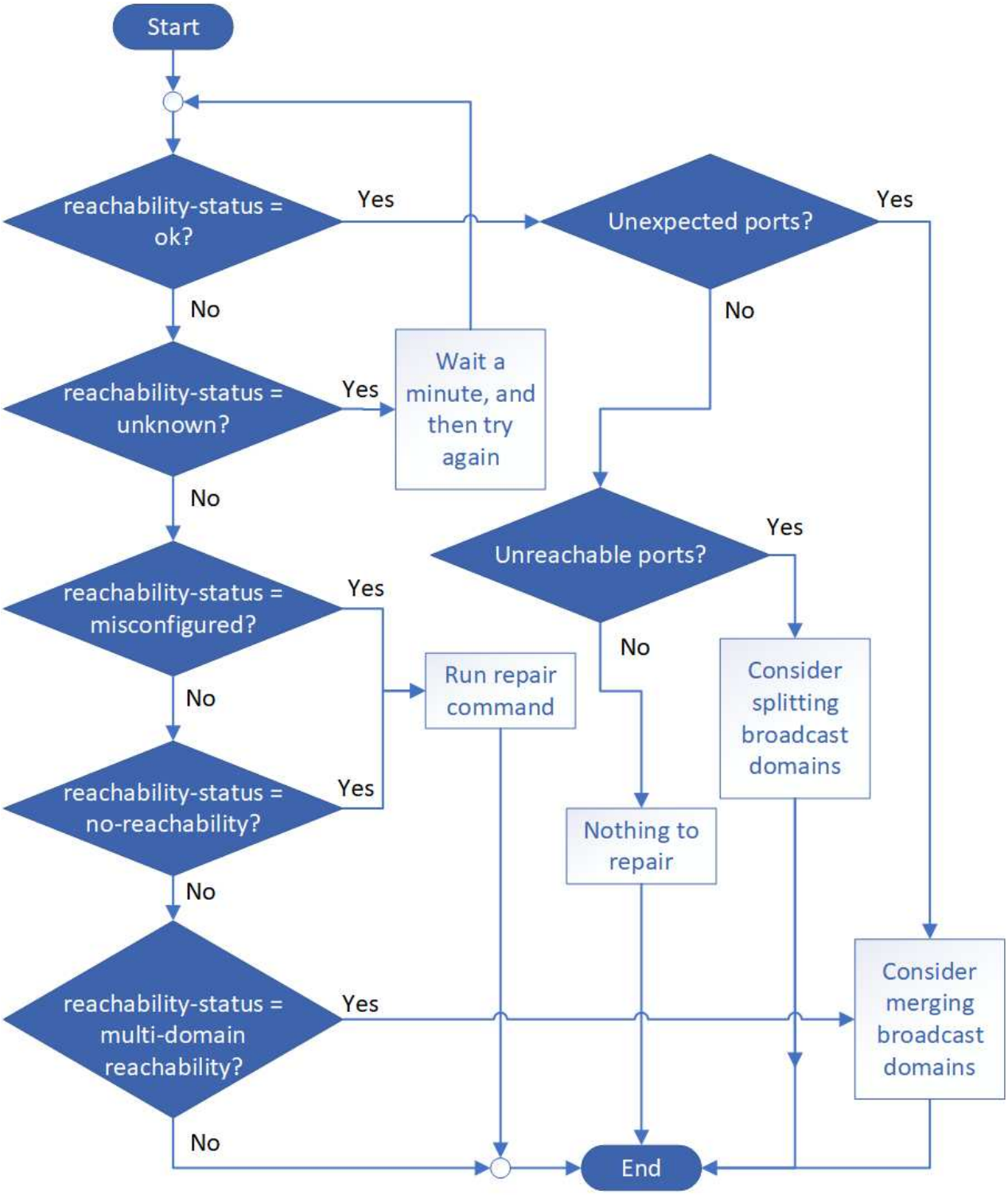
2. 檢查連接埠的可連線性：

   `network port reachability show -detail -node -port`

   命令輸出包含可到達性結果。

   如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

3. 請使用下列決策樹狀結構和表格來瞭解可連線性結果、並判斷接下來要做什麼（如果有的話）。



連線狀態	說明
好的	連接埠可連線至其指派的廣播網域的第2層。 如果連線狀態為「正常」、但有「非預期的連接埠」、請考慮合併一或多個廣播網域。如需詳細資訊、請參閱下列_Unexpected連接埠_資料列。 如果連線狀態為「正常」、但有「無法連線的連接埠」、請考慮分割一或多個廣播網域。如需詳細資訊、請參閱下列_Unreachable連接埠_資料列。 如果連線狀態為「正常」、而且沒有非預期或無法連線的連接埠、表示您的組態正確。
非預期的連接埠	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
無法連線的連接埠	如果單一廣播網域已分割成兩個不同的連線能力集、您可以分割廣播網域、 將ONTAP 此功能與實體網路拓撲進行同步。 一般而言、無法連線的連接埠清單會定義在您確認實體和交換器組態正確之後、應分割成另一個廣播網域的一組連接埠。 如需詳細資訊、請參閱 "分割廣播網域"。
設定錯誤的連線能力	連接埠無法連線至其指派的廣播網域的第2層；不過連接埠確實可連線至不同的廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給可連線的廣播網域： `network port reachability repair -node -port`
不可到達性	連接埠無法連線至任何現有廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給預設IPspace中自動建立的新廣播網域： `network port reachability repair -node -port` • 注意：* 如果所有介面群組（ ifgrp ）成員連接埠都報告 `no-reachability`、執行 `network port reachability repair` 每個成員連接埠上的命令都會導致從 ifgrp 移除每個連接埠、並置入新的廣播網域、最後導致移除 ifgrp 本身。執行之前 `network port reachability repair` 命令、根據實體網路拓撲、確認連接埠的可連線廣播網域符合您的預期。 如"指令參考資料ONTAP"需詳細 `network port reachability repair`資訊，請參閱。

多網域連線能力	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
不明	如果連線狀態為「未知」、請稍候幾分鐘、然後再試一次命令。

修復連接埠之後、請檢查是否有已移位的LIF和VLAN。如果連接埠是介面群組的一部分、您也需要瞭解該介面群組發生了什麼事。

生命

當某個連接埠修復並移至不同的廣播網域時、在修復連接埠上設定的任何LIF都會自動指派新的主連接埠。如果可能、該主連接埠會從同一個節點上的相同廣播網域中選取。或者、也會選取另一個節點的主連接埠、或者、如果沒有適當的主連接埠、主連接埠就會清除。

如果 LIF 的主連接埠移至另一個節點、或已清除、則 LIF 會被視為「已移轉」。您可以使用下列命令來檢視這些已移出的LIF：

```
displaced-interface show
```

如果有任何需要更換的生命、您必須：

- 還原已移出的LIF的主場：

  ```
  displaced-interface restore
  ```

- 手動設定LIF的主目錄：

  ```
  network interface modify -home-port -home-node
  ```

  如"指令參考資料ONTAP"需詳細 `network interface modify`資訊，請參閱。

- 如果您對LIF目前設定的主目錄感到滿意、請從「失所介面」表格中移除該項目：

  ```
  displaced-interface delete
  ```

VLAN

如果修復的連接埠有VLAN、這些VLAN會自動刪除、但也會記錄為「已移除」。您可以檢視這些已移離的VLAN：

```
displaced-vlans show
```

如果有任何已被取代的VLAN、您必須：

- 將VLAN還原至其他連接埠：

  ```
  displaced-vlans restore
  ```

- 從「Valler-VLANs」表中移除項目：

```
displaced-vlans delete
```

介面群組

如果修復的連接埠是介面群組的一部分、則會從該介面群組中移除。如果它是唯一指派給介面群組的成員連接埠、則介面群組本身就會移除。

相關資訊

- "升級後驗證您的網路組態"
- "監控網路連接埠的連線能力"
- "指令參考資料ONTAP"

將 ONTAP 廣播網域移至 IPspace

從 ONTAP 9.8 開始，您可以將系統根據第 2 層連線能力所建立的廣播網域移至您建立的 IPspace 。

在移動廣播網域之前、您必須確認廣播網域中連接埠的可連線性。

自動掃描連接埠可判斷哪些連接埠可以彼此連線、並將它們放在同一個廣播網域中、但此掃描無法判斷適當的IPspace。如果廣播網域屬於非預設IPspace、則您必須使用本節中的步驟手動移動它。

開始之前

廣播網域會自動設定為叢集建立和加入作業的一部分。此「預設」廣播網域定義為連接第2層連接至叢集第一個節點上管理介面的主連接埠的連接埠集。ONTAP如有必要、會建立其他廣播網域、並命名為*預設值-1*、*預設值-2*等。

當節點加入現有叢集時、其網路連接埠會根據其第2層可到達性自動加入現有的廣播網域。如果連接埠無法連線至現有的廣播網域、則連接埠會放置在一個或多個新的廣播網域中。

關於這項工作

- 具有叢集生命的連接埠會自動置入「叢集」IPspace。
- 可連線至節點管理LIF主連接埠的連接埠、會置於「預設」廣播網域中。
- 其他廣播網域則由ONTAP 不受限制的功能自動建立、作為叢集建立或加入作業的一部分。
- 當您新增VLAN和介面群組時、這些VLAN和介面群組會在建立後約一分鐘自動放入適當的廣播網域。

步驟

1. 驗證廣播網域中連接埠的可連線性。自動監控第2層連線能力。ONTAP使用下列命令來驗證每個連接埠是否已新增至廣播網域、且具有「OK」連線能力。

   ```
   network port reachability show -detail
   ```

   如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

2. 如有必要、請將廣播網域移至其他IPspaces：

```
network port broadcast-domain move
```

例如、如果您要將廣播網域從「預設」移至「ips1」：

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default
-to-ipspace ips1
```

相關資訊

- "網路連接埠廣播網域移動"

分割 ONTAP 廣播網域

如果透過實體網路連線或交換器組態變更了網路連接埠連線能力、 先前在單一廣播網域中設定的一組網路連接埠已分割成兩個不同的連線能力集、您可以分割廣播網域、將ONTAP此「更新」組態與實體網路拓撲進行同步。

分割廣播網域的程序與 ONTAP 9.7 和舊版不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上分割廣播域，請"分割廣播網域（ ONTAP 9.7 或更早版本）"參閱。

若要判斷網路連接埠廣播網域是否分割成多個連線能力集，請使用 `network port reachability show -details`命令並注意哪些連接埠無法彼此連線（「無法連線的連接埠」）。一般而言、無法連線的連接埠清單會在您確認實體和交換器組態正確之後、定義應分割成另一個廣播網域的連接埠集。如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

步驟

將廣播網域分割成兩個廣播網域：

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` 是廣播網域所在 IPSpace 的名稱。
- `-broadcast-domain` 是要分割的廣播網域名稱。
- `-new-broadcast-domain` 是要建立的新廣播網域名稱。
- `-ports` 是要新增至新廣播網域的節點名稱和連接埠。

相關資訊

- "網路連接埠廣播網域分割"

合併 ONTAP 廣播網域

如果網路連接埠可連線性已變更、無論是透過實體網路連線或交換器組態、或是先前在多個廣播網域中設定的兩組網路連接埠、現在都能共用可連線性、則可以使用合併兩個廣播網域、將ONTAP 此二元組態與實體網路拓撲進行同步。

ONTAP 9.7 和舊版中的廣播網域合併程序不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上合併廣播域，請"合併廣播網域（ ONTAP 9.7 或更早版本）"參閱。

若要確定多個廣播域是否屬於可達性集，請使用 `network port reachability show -details`命令並注意在另一個廣播網域中配置的哪些連接埠實際上彼此具有連接（“意外連接埠”）。通常、非預期連接埠清單會定義在您驗證實體和交換器組態是否正確之後、應合併到廣播網域的連接埠集。

如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

步驟

將一個廣播網域的連接埠合併到現有的廣播網域：

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` 是廣播網域所在 IPSpace 的名稱。
- `-broadcast-domain` 是要合併的廣播網域名稱。
- `-into-broadcast-domain` 是將接收其他連接埠的廣播網域名稱。

相關資訊

- "網路連接埠 broadcast-domain-merge"

變更 ONTAP 廣播網域中連接埠的 MTU 值

您可以修改廣播網域的MTU值、以變更該廣播網域中所有連接埠的MTU值。這可以用來支援網路中的拓撲變更。

在 ONTAP 9.7 和更早版本中，變更廣播網域連接埠 MTU 值的程序有所不同。如果您需要變更執行 ONTAP 9.7 及更早版本之網路上廣播網域連接埠的 MTU 值，請參閱"變更廣播網域中連接埠的 MTU 值（ ONTAP 9.7 及更早版本）"。

系統管理員

從 ONTAP 9.12.0 開始，您可以使用 System Manager 修改廣播網域的 MTU 值，從而變更該廣播網域中所有連接埠的 MTU 值。

步驟

1. 選擇 **Network > Broadcast Domains** 。
2. 在 **Broadcast Domains** 部分，選擇要變更 MTU 值的廣播網域的名稱。
3. 系統會彈出提示，詢問您是否要變更廣播網域中所有連接埠的 MTU 值。按一下 **Yes** 繼續變更。
4. 根據需要修改 MTU 值並儲存變更。

   系統會將新的 MTU 值套用至廣播網域中的所有連接埠，這會導致這些連接埠的流量短暫中斷。

CLI

開始之前

MTU值必須符合連接至該層2網路的所有裝置、但e0M連接埠處理管理流量除外。

關於這項工作

更改 MTU 值會導致受影響連接埠上的流量短暫中斷。系統會顯示提示，您必須輸入 **y** 才能變更 MTU。

步驟

變更廣播網域中所有連接埠的MTU值：

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

其中：

- `broadcast_domain` 是廣播網域的名稱。
- `mtu` 為 IP 封包的 MTU 大小； 1500 和 9000 為典型值。
- `ipspace` 是此廣播域所在的 IPspace 的名稱。除非您為此選項指定值，否則將使用「Default」IPspace。

  以下命令將廣播網域 bcast1 中所有連接埠的 MTU 變更為 9000：

  ```
  network port broadcast-domain modify -broadcast-domain <Default-1>
  -mtu < 9000 >
  Warning: Changing broadcast domain settings will cause a momentary
  data-serving interruption.
  Do you want to continue? {y|n}: <y>
  ```

相關資訊

- "修改網路連接埠廣播網域"

檢視 ONTAP 廣播網域

您可以顯示叢集中每個IPspace內的廣播網域清單。輸出也會顯示每個廣播網域的連接埠清單和MTU值。

ONTAP 9.7 和舊版中顯示廣播網域的程序有所不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上顯示廣播域，請"顯示廣播網域（ ONTAP 9.7 或更早版本）"參閱。

步驟

顯示叢集中的廣播網域和相關連接埠：

```
network port broadcast-domain show
```

下列命令會顯示叢集中的所有廣播網域和相關連接埠：

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                            cluster-1-01:e0a       complete
                            cluster-1-01:e0b       complete
                            cluster-1-02:e0a       complete
                            cluster-1-02:e0b       complete
Default Default      1500
                            cluster-1-01:e0c       complete
                            cluster-1-01:e0d       complete
                            cluster-1-02:e0c       complete
                            cluster-1-02:e0d       complete
        Default-1    1500
                            cluster-1-01:e0e       complete
                            cluster-1-01:e0f       complete
                            cluster-1-01:e0g       complete
                            cluster-1-02:e0e       complete
                            cluster-1-02:e0f       complete
                            cluster-1-02:e0g       complete
```

下列命令會顯示預設廣播網域中的連接埠、其更新狀態為「錯誤」、表示連接埠無法正確更新：

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

相關資訊

- "網路連接埠廣播網域show"

刪除 ONTAP 廣播網域

如果不再需要廣播網域、您可以將其刪除。這會將與該廣播網域相關的連接埠移至「預設」IPspace。

開始之前

不得有任何子網路、網路介面或SVM與您要刪除的廣播網域相關聯。

關於這項工作

- 無法刪除系統建立的「叢集」廣播網域。
- 刪除廣播網域時、會移除與廣播網域相關的所有容錯移轉群組。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**刪除廣播網域

當廣播網域包含連接埠或與子網路相關聯時、不會顯示刪除選項。

步驟

1. 選擇*網路>總覽>廣播網域*。
2. 在您要移除的廣播網域旁邊選取 ⋮ * > 刪除 * 。

CLI

使用**CLI**刪除廣播網域

步驟

刪除廣播網域：

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

下列命令會刪除IPspace ipspace1中的廣播網域預設值1：

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

相關資訊

- "網路連接埠廣播網域刪除"

容錯移轉群組和原則

瞭解 ONTAP 網路上的 LIF 容錯移轉

LIF容錯移轉是指自動將LIF移轉至不同的網路連接埠、以因應LIF目前連接埠上的連結故障。這是提供高可用度以連線至SVM的關鍵元件。設定LIF容錯移轉包括建立容錯移轉群組、修改LIF以使用容錯移轉群組、以及指定容錯移轉原則。

容錯移轉群組包含一組來自叢集中一或多個節點的網路連接埠（實體連接埠、VLAN和介面群組）。容錯移轉群組中的網路連接埠可定義LIF可用的容錯移轉目標。容錯移轉群組可以指派叢集管理、節點管理、叢集間及NAS資料生命期給它。

如果LIF設定為沒有有效的容錯移轉目標、則LIF嘗試容錯移轉時會發生中斷。您可以使用 `network interface show -failover`命令來驗證容錯移轉組態。如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

建立廣播網域時、系統會自動建立同名的容錯移轉群組、其中包含相同的網路連接埠。此容錯移轉群組是由系統自動管理、也就是說、當連接埠從廣播網域新增或移除時、它們會自動從這個容錯移轉群組中新增或移除。對於不想管理自己的容錯移轉群組的系統管理員而言、這是一種效率。

建立 ONTAP 容錯移轉群組

您可以建立網路連接埠的容錯移轉群組、以便LIF在LIF的目前連接埠發生連結故障時、自動移轉至不同的連接埠。這可讓系統將網路流量重新路由至叢集中的其他可用連接埠。

關於這項工作

您可以使用 `network interface failover-groups create` 命令以建立群組並將連接埠新增至群組。

- 新增至容錯移轉群組的連接埠可以是網路連接埠、VLAN或介面群組（ifgrps）。
- 新增至容錯移轉群組的所有連接埠都必須屬於同一個廣播網域。
- 單一連接埠可位於多個容錯移轉群組中。
- 如果您在不同的VLAN或廣播網域中有LIF、則必須為每個VLAN或廣播網域設定容錯移轉群組。
- 容錯移轉群組不適用於SAN iSCSI或FC環境。

步驟

建立容錯移轉群組：

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* 是可以使用容錯移轉群組的 SVM 名稱。
- *`failover_group_name`* 為您要建立的容錯移轉群組名稱。
- *`ports_list`* 是要新增至容錯移轉群組的連接埠清單。
  連接埠的新增格式為_node_name>:<port_number>_、例如node1:e0c。

下列命令會針對SVM VS3建立容錯移轉群組fg3、並新增兩個連接埠：

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

完成後

- 在建立容錯移轉群組之後、您應該將容錯移轉群組套用至LIF。
- 套用不為LIF提供有效容錯移轉目標的容錯移轉群組、會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 如"指令參考資料ONTAP"需詳細 `network interface failover-groups create`資訊，請參閱。

在 LIF 上設定 ONTAP 容錯移轉設定

您可以將容錯移轉原則和容錯移轉群組套用至LIF、將LIF設定為容錯移轉至特定的網路連接埠群組。您也可以停用LIF、使其無法容錯移轉至其他連接埠。

關於這項工作

- 建立LIF時、預設會啟用LIF容錯移轉、可用的目標連接埠清單則由預設的容錯移轉群組和容錯移轉原則根據LIF類型和服務原則來決定。

  從9.5開始、您可以為LIF指定服務原則、以定義哪些網路服務可以使用LIF。有些網路服務會對LIF強制容錯移轉限制。

  如果LIF的服務原則變更後會進一步限制容錯移轉、則系統會自動更新LIF的容錯移轉原則。

- 您可以在network interface modify命令中指定-容 錯移轉群組和-容 錯移轉原則參數的值、以修改I生命 體的容錯移轉行為。
- 修改LIF會導致LIF沒有有效的容錯移轉目標、因此會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 從 ONTAP 9.11.1 開始、在 All Flash SAN Array （ASA）平台上、 iSCSI LIF 容錯移轉會自動在新建立的儲存 VM 上、於新建立的 iSCSI 生命週期中啟用。

  此外、您也可以 "在預先存在的 iSCSI 生命體上手動啟用 iSCSI LIF 容錯移轉"、意指在升級至 ONTAP 9.11.1 或更新版本之前建立的生命。

- 下列清單說明容錯移轉原則設定如何影響從容錯移轉群組選取的目標連接埠：

  對於 iSCSI LIF 容錯移轉、只有容錯移轉原則 `local-only`、 `sfo-partner-only` 和 `disabled` 支援。

- `broadcast-domain-wide` 適用於容錯移轉群組中所有節點上的所有連接埠。
- `system-defined` 僅適用於 LIF 主節點上的連接埠、以及叢集中的另一個節點、通常是非 SFO 合作夥伴（如果存在）。
- `local-only` 僅適用於 LIF 主節點上的連接埠。
- `sfo-partner-only` 僅適用於 LIF 主節點及其 SFO 合作夥伴上的連接埠。
- `disabled` 表示 LIF 未設定為容錯移轉。

步驟

設定現有介面的容錯移轉設定：

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

設定容錯移轉設定及停用容錯移轉的範例

下列命令會將容錯移轉原則設定為廣播網域範圍、並使用容錯移轉群組fg3中的連接埠做為SVM VS3上LIF資料1的容錯移轉目標：

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

下列命令會停用SVM VS3上LIF資料1的容錯移轉：

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

相關資訊

- "網路介面"

用於管理容錯移轉群組和原則的 ONTAP 命令

您可以使用 `network interface failover-groups` 管理容錯移轉群組的命令。您可以使用 `network interface modify` 用於管理套用至 LIF 的容錯移轉群組和容錯移轉原則的命令。

如果您想要...	使用此命令...
將網路連接埠新增至容錯移轉群組	`network interface failover-groups add-targets`
從容錯移轉群組移除網路連接埠	`network interface failover-groups remove-targets`
修改容錯移轉群組中的網路連接埠	`network interface failover-groups modify`
顯示目前的容錯移轉群組	`network interface failover-groups show`
在LIF上設定容錯移轉	`network interface modify -failover -group -failover-policy`
顯示每個LIF所使用的容錯移轉群組和容錯移轉原則	`network interface show -fields failover-group, failover-policy`

重新命名容錯移轉群組	`network interface failover-groups rename`
刪除容錯移轉群組	`network interface failover-groups delete`

修改容錯移轉群組、使其無法為叢集中的任何LIF提供有效的容錯移轉目標、可能會在LIF嘗試容錯移轉時造成中斷。

相關資訊

- "網路介面"

子網路（僅限叢集管理員）

瞭解 ONTAP 網路的子網路

子網路可讓您分配特定區塊或集區IP位址、以供ONTAP 您進行支援所需的網路組態。這可讓您指定子網路名稱、而不必指定IP位址和網路遮罩值、更輕鬆地建立lifs。

子網路是在廣播網域內建立、其中包含屬於同一第3層子網路的IP位址集區。子網路中的IP位址會在建立LIF時分配給廣播網域中的連接埠。移除LIF時、IP位址會傳回子網路集區、可供未來的LIF使用。

建議您使用子網路、因為子網路可讓IP位址的管理更輕鬆、而且能簡化生命週期的建立程序。此外、如果您在定義子網路時指定閘道、則當使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。

為 ONTAP 網路建立子網路

您可以建立子網路、以配置稍後為SVM建立LIF時所使用的特定IPv4或IPv6位址區塊。

這可讓您更輕鬆地建立lifs、方法是指定子網路名稱、而非為每個LIF指定IP位址和網路遮罩值。

開始之前

您必須是叢集管理員才能執行此工作。

您要新增子網路的廣播網域和IPspace必須已經存在。

關於這項工作

- 所有子網路名稱在IPspace內必須是唯一的。
- 將IP位址範圍新增至子網路時、您必須確保網路中沒有重疊的IP位址、以免不同的子網路或主機嘗試使用相同的IP位址。
- 如果您在定義子網路時指定閘道、則當使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。如果您不使用子網路、或是定義子網路時未指定閘道、則需要使用 `route create` 手動將路由新增至 SVM 的命令。
- NetApp 建議為資料 SVM 上的所有生命建立子網路物件。這對 MetroCluster 組態尤其重要，因為每個子網路物件都有相關的廣播網域，因此子網路物件可讓 ONTAP 判斷目的地叢集上的容錯移轉目標。

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 建立子網路。

系統管理員

從ONTAP 功能性版本的0：9.12.0開始、您可以使用System Manager建立子網路。

步驟

1. 選擇*網路>總覽>子網路*。
2. 按一下 + Add 以建立子網路。
3. 命名子網路。
4. 指定子網路IP位址。
5. 設定子網路遮罩。
6. 定義組成子網路的IP位址範圍。
7. 如果有用、請指定閘道。
8. 選取子網路所屬的廣播網域。
9. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

使用CLI建立子網路。

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 為您要建立的第 3 層子網路名稱。

  名稱可以是像「Mgmt」這樣的文字字串、也可以是特定的子網路IP值、例如192.0/24。

- `broadcast_domain_name` 是子網路所在的廣播網域名稱。
- `ipspace_name` 是廣播網域所屬的 IPspace 名稱。

  除非您指定此選項的值、否則會使用「預設」IPspace。

- `subnet_address` 是子網路的 IP 位址和遮罩、例如 192.0.2.0/24 。
- `gateway_address` 是子網路預設路由的閘道、例如 192.0.2.1 。
- `ip_address_list` 是將分配給子網路的 IP 位址清單或範圍。

  IP位址可以是個別位址、IP位址範圍、或是以逗號分隔的清單組合。

- 價值 `true` 可設定為 `-force-update-lif-associations` 選項。

  如果任何服務處理器或網路介面目前正在使用指定範圍內的IP位址、則此命令會失敗。將此值設為true、可將任何手動定址的介面與目前子網路建立關聯、並允許命令成功執行。

下列命令會在預設IPspace的廣播網域預設-1中建立子網路子網路1。它會新增一個IPV4子網路IP位址和遮罩、閘道和一系列IP位址：

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

下列命令會在「預設」IPspace的廣播網域預設中建立子網路子網路2。它新增多種IPv6位址：

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

完成後

您可以使用子網路中的位址、將SVM和介面指派給IPspace。

如果您需要變更現有子網路的名稱、請使用 `network subnet rename` 命令。

如"指令參考資料ONTAP"需詳細 `network subnet rename`資訊，請參閱。

從 **ONTAP** 網路的子網路新增或移除 **IP** 位址

您可以在最初建立子網路時新增IP位址、或是將IP位址新增至已存在的子網路。您也可以從現有子網路移除IP位址。如此一來、您只能為SVM分配所需的IP位址。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*從ONTAP 版本S59.12.0開始、您可以使用System Manager在子網路*中新增或移除IP位址

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要變更的子網路旁選取 ⋮ * > 編輯 * 。
3. 新增或移除IP位址。
4. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

*使用CLI在子網路*中新增或移除IP位址

關於這項工作

新增IP位址時、如果有任何服務處理器或網路介面使用所新增範圍內的IP位址、您將會收到錯誤訊息。如果您想要將任何手動定址的介面與目前的子網路建立關聯、您可以設定 `-force-update-lif-associations` 選項 `true`。

移除IP位址時、如果有任何服務處理器或網路介面使用要移除的IP位址、您將會收到錯誤訊息。如果您希望介面在從子網路移除後繼續使用 IP 位址、您可以設定 `-force-update-lif-associations` 選項 `true`。

步驟

新增或移除子網路中的IP位址：

如果您想要…	使用此命令…
新增IP位址至子網路	網路子網路新增範圍
從子網路移除IP位址	網路子網路移除範圍

下列命令會將IP位址192.0.2.82到192.0.2.85新增至子網路子網路1：

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

下列命令會從子網路子網路3移除IP位址198.51.1009：

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

如果目前範圍包括1到10、20到40、而您想要新增11到19、41到50（基本上允許1到50）、您可以使用下列命令來重疊現有的位址範圍。此命令只會新增新位址、不會影響現有位址：

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

深入瞭解 `network subnet add-ranges`及 `network subnet remove-ranges` "指令參考資料ONTAP"。

變更 ONTAP 網路的子網路內容

您可以變更現有子網路中的子網路位址和遮罩值、閘道位址或IP位址範圍。

關於這項工作

- 修改IP位址時、您必須確保網路中沒有重疊的IP位址、以免不同的子網路或主機嘗試使用相同的IP位址。
- 如果您新增或變更閘道IP位址、當使用子網路在新的SVM中建立LIF時、修改的閘道會套用至新的SVM。如果路由尚未存在、則會為SVM建立通往閘道的預設路由。變更閘道IP位址時、您可能需要手動新增新路由至SVM。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**來變更子網路內容

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要變更的子網路旁選取 * > 編輯 * 。
3. 進行變更。
4. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

使用**CLI**變更子網路內容

步驟

修改子網路內容：

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 是您要修改的子網路名稱。
- `ipspace` 是子網路所在 IPspace 的名稱。
- `subnet` 為子網路的新位址和遮罩（如果適用）、例如 192.0.2.0/24 。
- `gateway` 是子網路的新閘道（如果適用）、例如 192.0.2.1 。輸入*「*」*會移除閘道項目。
- `ip_ranges` 為 IP 位址的新清單或範圍、如果適用、將會分配給子網路。IP位址可以是個別位址、範圍或IP位址、或是以逗號分隔的清單組合。此處指定的範圍會取代現有的IP位址。
- `force-update-lif-associations` 變更 IP 位址範圍時為必填。修改IP位址範圍時、您可以將此選項的值設為* true*。如果任何服務處理器或網路介面使用指定範圍內的IP位址、則此命令會失敗。將此值設為* true*可將任何手動定址的介面與目前的子網路建立關聯、並允許命令成功執行。

下列命令會修改子網路子網路3的閘道IP位址：

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

如"指令參考資料ONTAP"需詳細 `network subnet modify`資訊，請參閱。

檢視 ONTAP 網路的子網路

您可以顯示IP空間內分配給每個子網路的IP位址清單。輸出也會顯示每個子網路可用的IP位址總數、以及目前使用的位址數目。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**來顯示子網路

步驟

1. 選擇*網路>總覽>子網路*。
2. 檢視子網路清單。

CLI

使用**CLI**顯示子網路

步驟

顯示子網路清單及這些子網路中使用的相關IP位址範圍：

```
network subnet show
```

下列命令會顯示子網路和子網路內容：

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name    Subnet          Domain    Gateway       Total    Ranges
------  --------------- --------- ------------ --------
------------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1     5/9      192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

如"指令參考資料ONTAP"需詳細 `network subnet show`資訊，請參閱。

從 ONTAP 網路刪除子網路

如果您不再需要子網路、而想要取消分配指派給子網路的IP位址、您可以將其刪除。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**刪除子網路

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要移除的子網路旁選取 ⋮ * > 刪除 * 。
3. 儲存您的變更。

CLI

使用**CLI**刪除子網路

關於這項工作

如果任何服務處理器或網路介面目前使用指定範圍內的IP位址、您將會收到錯誤訊息。如果希望介面在刪除子網路之後仍繼續使用IP位址、您可以將-force-update-lif-associations-true選項設定為true、以移除子網路與lifs的關聯。

步驟

刪除子網路：

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

下列命令會刪除IPspace ipspace1中的子網路子網路1：

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

如"指令參考資料ONTAP"需詳細 `network subnet delete`資訊，請參閱。

為 ONTAP 網路建立 SVM

您必須建立SVM、才能將資料提供給用戶端。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須知道SVM根磁碟區的安全樣式。

  如果您計畫在此SVM上實作Hyper-V或SQL Server over SMB解決方案、則根磁碟區應該使用NTFS安全樣式。包含Hyper-V檔案或SQL資料庫檔案的磁碟區在建立時必須設定為NTFS安全性。將根磁碟區安全樣式設定為NTFS、可確保您不會不慎建立UNIX或混合式安全型資料磁碟區。

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

系統管理員

您可以使用System Manager來建立儲存VM。

步驟

1. 選擇*儲存VMS*。
2. 按一下 + Add 以建立儲存 VM 。
3. 命名儲存VM。
4. 選取存取傳輸協定：
   - SMB/CIFS、NFS
   - iSCSI
   - FC
   - NVMe
     i. 如果您選取*啟用SMB/CIFS*、請完成下列組態：

欄位或核取方塊	說明
系統管理員名稱	指定SMB/CIFS儲存VM的系統管理員使用者名稱。
密碼	指定SMB/CIFS儲存VM的管理員密碼。
伺服器名稱	指定SMB/CIFS儲存VM的伺服器名稱。
Active Directory網域	指定Active Directory網域、為SMB/CIFS儲存VM提供使用者驗證。
組織單位	指定Active Directory網域中與SMB/CIFS伺服器相關聯的組織單位。「cn=computers"是預設值、可以修改。
存取儲存VM中的共享區時、加密資料	選取此核取方塊可使用SMB 3.0加密資料、以防止對SMB/CIFS儲存VM中共用區的未授權檔案存取。
網域	新增、移除或重新排列SMB / CIFS儲存VM所列的網域。
名稱伺服器	新增、移除或重新排序SMB/CIFS儲存VM的名稱伺服器。
預設語言	指定儲存VM及其磁碟區的預設語言編碼設定。使用CLI變更儲存VM內個別磁碟區的設定。

網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用NFS*、請完成下列組態：

欄位或核取方塊	說明
允許NFS用戶端存取核取方塊	如果NFS儲存VM上建立的所有磁碟區都應該使用根磁碟區路徑「/」來掛載及周遊、請選取此核取方塊。將規則新增至匯出原則「預設」、以允許不中斷的掛載周遊。
規則	按一下 + Add 以建立規則。 • 用戶端規格：指定主機名稱、IP位址、網路群組或網域。 • 存取傳輸協定：選取下列選項的組合： ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3. ▪ NFSv4. • 存取詳細資料：針對每種類型的使用者、指定存取層級（唯讀、讀取/寫入器或超級使用者）。使用者類型包括： ◦ 全部 ◦ 全部（匿名使用者） ◦ UNIX ◦ Kerberos 5. ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM 儲存規則。

預設語言	指定儲存VM及其磁碟區的預設語言編碼設定。使用CLI變更儲存VM內個別磁碟區的設定。
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用iSCSI*、請完成下列組態：

欄位或核取方塊	說明
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取 * 啟用 FC* 、請完成下列組態：

欄位或核取方塊	說明
設定FC連接埠	在要納入儲存VM的節點上選取網路介面。建議每個節點使用兩個網路介面。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用NVMe/FC*、請完成下列組態：

欄位或核取方塊	說明

設定FC連接埠	在要納入儲存VM的節點上選取網路介面。建議每個節點使用兩個網路介面。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取 * 啟用 NVMe / TCP * 、請完成下列組態：

欄位或核取方塊	說明
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 儲存您的變更。

CLI

使用ONTAP CLI建立子網路。

步驟

1. 判斷哪些Aggregate是包含SVM根磁碟區的候選集合體。

   ```
   storage aggregate show -has-mroot false
   ```

   您必須選擇至少有1 GB可用空間的集合體、才能包含根磁碟區。如果您打算在SVM上設定NAS稽核、則必須在根Aggregate上至少有3 GB的額外可用空間、並在啟用稽核功能時、使用額外空間來建立稽核接移磁碟區。

   > 如果已在現有SVM上啟用NAS稽核、則會在成功完成集合建立之後、立即建立Aggregate的接移Volume。

2. 記錄您要在其上建立SVM根Volume的集合體名稱。
3. 如果您打算在建立SVM時指定語言、但不知道要使用的值、請識別並記錄您要指定的語言值：

   ```
   vserver create -language ?
   ```

4. 如果您計畫在建立 SVM 時指定快照原則，但不知道原則名稱，請列出可用的原則，並識別並記錄您要

使用的快照原則名稱：

```
volume snapshot policy show -vserver vserver_name
```

5. 如果您打算在建立SVM時指定配額原則、但不知道原則名稱、請列出可用的原則、並識別並記錄您要使用的配額原則名稱：

```
volume quota policy show -vserver vserver_name
```

6. 建立SVM：

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. 驗證SVM組態是否正確。

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

在此範例中、命令會在IPspace「ipspace1」中建立名為「VS1」的SVM。根磁碟區的名稱為「VS1_root」、建立於具有NTFS安全樣式的aggr3上。

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

邏輯介面（LIF）

LIF 總覽

瞭解 ONTAP 叢集的 LIF 組態

LIF（邏輯介面）代表叢集中節點的網路存取點。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。

叢集管理員可以建立、檢視、修改、移轉、還原、 或刪除lifs。SVM管理員只能檢視與SVM相關聯的LIF。

LIF是具有相關特性的IP位址或WWPN、例如服務原則、主連接埠、主節點、容錯移轉至的連接埠清單、以及防

火牆原則。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。

> 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

LIF可裝載於下列連接埠：

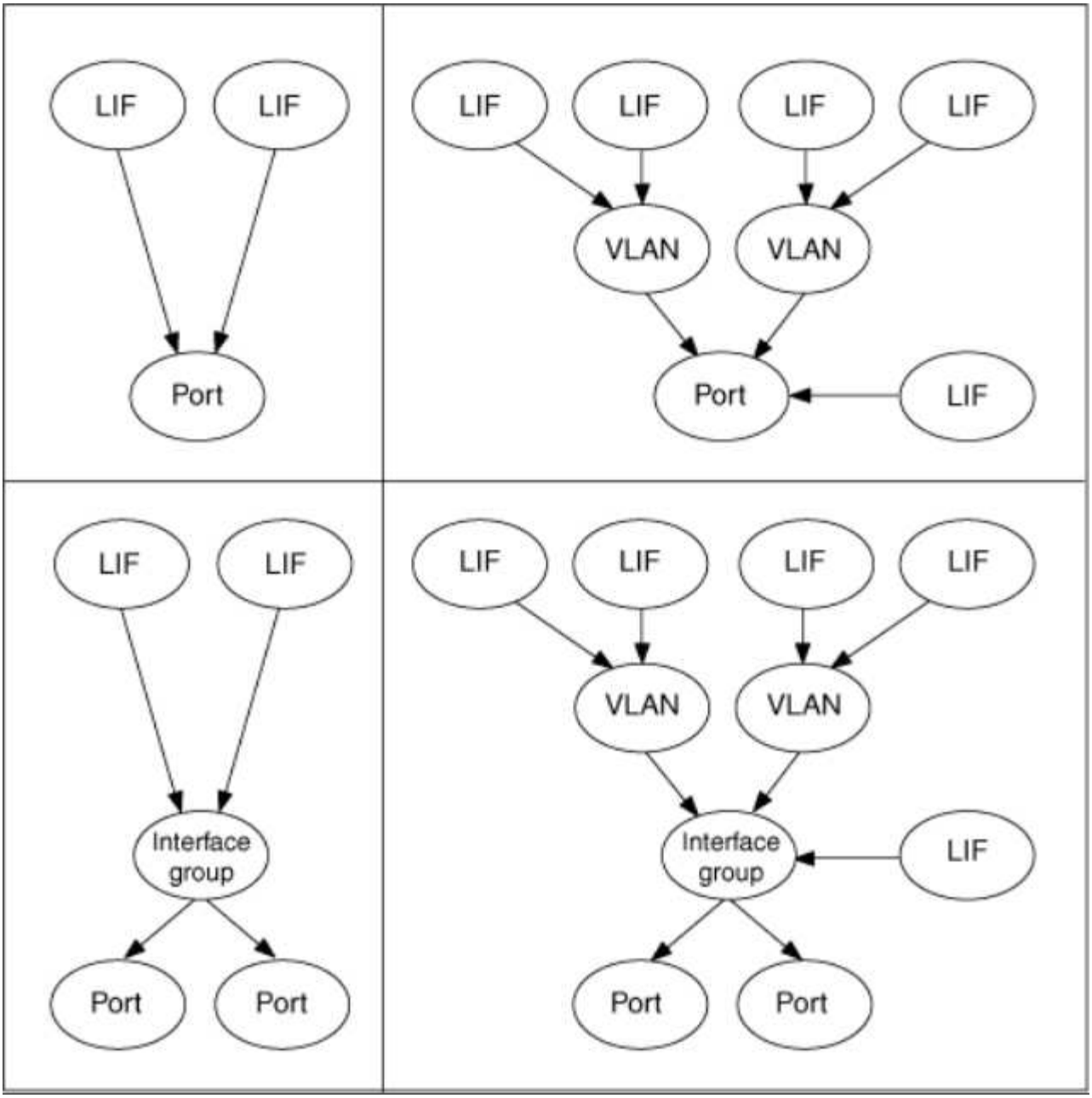
- 不屬於介面群組的實體連接埠
- 介面群組
- VLAN
- 裝載VLAN的實體連接埠或介面群組
- 虛擬IP（VIP）連接埠

  從支援的版本起、VIP LIF就會在VIP連接埠上提供支援。ONTAP

在LIF上設定FC等SAN傳輸協定時、它會與WWPN相關聯。

"SAN管理"

下圖說明ONTAP 了一個作業系統中的連接埠階層架構：



LIF 容錯移轉與恢復

LIF 會在 LIF 從其主節點或連接埠移至其 HA 合作夥伴節點或連接埠時進行容錯移轉。LIF 容錯移轉可由 ONTAP 自動觸發、或由叢集管理員手動針對某些事件觸發、例如實體乙太網路連結中斷或節點從複寫資料庫（ RDB ）仲裁中刪除。發生 LIF 容錯移轉時、 ONTAP 會繼續在合作夥伴節點上執行正常作業、直到容錯移轉的原因解決為止。當主節點或連接埠恢復健全狀況時、 LIF 會從 HA 合作夥伴還原回其主節點或連接埠。 此還原稱為贈品。

對於 LIF 容錯移轉和恢復、每個節點的連接埠都必須屬於同一個廣播網域。若要檢查每個節點上的相關連接埠是否屬於同一個廣播網域、請參閱下列內容：

- ONTAP 9.8 及更新版本： "修復連接埠連線能力"
- ONTAP 9.7 及更早版本："新增或移除廣播網域中的連接埠"

若為已啟用 LIF 容錯移轉的生命（自動或手動）、則適用下列項目：

- 對於使用資料服務原則的生命、您可以檢查容錯移轉原則限制：
  - ONTAP 9.6 及更新版本： "更新版本中的生命與服務政策ONTAP"
  - ONTAP 9.5 及更早版本："LIF角色在ONTAP 更新版本的版本中"
- 當自動還原設定為時、會自動還原生命 `true` 當 LIF 的主連接埠健全且能夠裝載 LIF 時、
- 在計畫性或非計畫性節點接管上、接管節點上的 LIF 會容錯移轉至 HA 合作夥伴。LIF容錯移轉的連接埠由VIF Manager決定。
- 容錯移轉完成後、 LIF 會正常運作。
- 啟動恢復時、如果將自動還原設定為、 LIF 會還原回其主節點和連接埠 `true`。
- 當乙太網路連結在裝載一或多個生命體的連接埠上中斷時、 VIF Manager 會將生命體從停機連接埠移轉到同一個廣播網域中的不同連接埠。新連接埠可能位於同一個節點或其HA合作夥伴中。連結還原後、如果自動還原設為 `true`、 VIF Manager 會將生命恢復回其主節點和主連接埠。
- 當節點從複寫資料庫（ RDB ）仲裁中移出時、 VIF Manager 會將生命從仲裁節點移出移轉至其 HA 合作夥伴。當節點恢復為仲裁、且自動還原設為時 `true`、 VIF Manager 會將生命恢復回其主節點和主連接埠。

瞭解 **ONTAP LIF** 與連接埠類型的相容性

LIF可以具有不同的特性、以支援不同的連接埠類型。

當叢集間和管理生命體設定在同一個子網路中時、外部防火牆可能會封鎖管理流量、AutoSupport而且可能會導致無法透過不中斷的功能進行。您可以執行來恢復系統 `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` 切換叢集間 LIF 的命令。不過、您應該在不同的子網路中設定叢集間LIF和管理LIF、以避免此問題。

LIF	說明
資料LIF	與儲存虛擬機器（SVM）相關聯的LIF、用於與用戶端通訊。 您可以在一個連接埠上擁有多個資料生命量。這些介面可在整個叢集內進行移轉或容錯移轉。您可以將資料LIF修改成SVM管理LIF、將其防火牆原則修改為管理。 建立至NIS、LDAP、Active Directory、WINS和DNS伺服器的工作階段會使用資料生命期。
叢集LIF	LIF用於在叢集中的節點之間傳輸叢集內的流量。必須始終在叢集連接埠上建立叢集LIF。 叢集LIF可在同一個節點上的叢集連接埠之間容錯移轉、但無法移轉或容錯移轉至遠端節點。當新節點加入叢集時、會自動產生IP位址。不過、如果您想要手動指派IP位址給叢集LIF、則必須確保新的IP位址與現有的叢集LIF位於相同的子網路範圍內。
叢集管理LIF	LIF可為整個叢集提供單一管理介面。 叢集管理LIF可容錯移轉至叢集中的任何節點。它無法容錯移轉至叢集或叢集間連接埠

叢集間 LIF	用於跨叢集通訊、備份和複寫的LIF。您必須在叢集中的每個節點上建立叢集間LIF、才能建立叢集對等關係。 這些LIF只能容錯移轉至同一個節點中的連接埠。它們無法移轉或容錯移轉至叢集中的其他節點。
節點管理 LIF	提供專屬IP位址以管理叢集中的特定節點的LIF。節點管理生命期是在建立或加入叢集時建立的。例如、當節點無法從叢集存取時、這些生命量會用於系統維護。
VIP LIF	VIP LIF是在VIP連接埠上建立的任何資料LIF。若要深入瞭解"設定虛擬IP（VIP）LIF"、請參閱。

相關資訊

- "修改網路介面"

ONTAP 版本支援的 **LIF** 服務原則和角色

隨著時間的推移、 ONTAP 管理生命負載所支援流量類型的方式也隨之改變。

- ONTAP 9 的同一版本和更早的版本使用 LIF 角色和防火牆服務。
- ONTAP 9 6 及更新版本使用 LIF 服務原則：
  - ONTAP 9 簡介推出 LIF 服務原則。
  - ONTAP 9 6 中以 LIF 服務原則取代 LIF 角色。
  - ONTAP 9 。 10.1 以 LIF 服務原則取代防火牆服務。

您設定的方法取決於您所使用的 ONTAP 版本。

若要深入瞭解：

- 防火牆原則請"命令： firewall-police-show"參閱。
- LIF 角色、請參閱"LIF 角色（ ONTAP 9.5 及更早版本）"。
- LIF 服務原則，請"生命與服務原則（ ONTAP 9.6 及更新版本）"參閱。

瞭解 **ONTAP** 生命與服務原則

您可以將服務原則（而非LIF角色或防火牆原則）指派給生命期、以決定生命期所支援的流量類型。服務原則定義LIF支援的網路服務集合。提供一組可與LIF相關聯的內建服務原則。ONTAP

ONTAP 9.7 和舊版的網路流量管理方法不同。如果您需要管理運行 ONTAP 9.7 及更早版本的網絡上的流量，請"LIF 角色（ ONTAP 9.5 及更早版本）"參閱。

FCP 和 NVMe/FCP 協定目前不需要服務原則。

您可以使用下列命令來顯示服務原則及其詳細資料：

```
network interface service-policy show
```

如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。

未繫結至特定服務的功能、將會使用系統定義的行為來選取輸出連線的生命。

具有空服務原則的 LIF 上的應用程式可能會在非預期的情況下運作。

系統**SVM**的服務原則

管理SVM和任何系統SVM都包含可用於該SVM中的LIF的服務原則、包括管理和叢集間LIF。系統會在建立IPspace時自動建立這些原則。

下表列出從 ONTAP 9.12.1 開始的系統 SVM 中生命週期的內建原則。對於其他版本、請使用下列命令顯示服務原則及其詳細資料：

```
network interface service-policy show
```

原則	隨附服務	等效角色	說明
預設叢集間	叢集間核心、管理-https	叢集間	用於傳輸叢集間流量的lifs。 附註：ONTAP 服務叢集間核心可從名稱為net-intercluster服務原則的版本中取得。
default-route-聲明	管理- BGP	-	由承載 BGP 對等連線的生命所使用 附註：可從 ONTAP 9.5 取得、名稱為 net-route-note 服務原則。
預設管理	管理核心、管理https、管理http、管理ssh、管理自動支援、 管理- EMS、管理- DNS用戶端、管理- ad用戶端、管理-LDAP用戶端、管理-NIS用戶端、 管理層NTP用戶端、管理層記錄轉送	節點管理或叢集管理	使用此系統範圍內的管理原則、建立系統SVM擁有的節點和叢集範圍管理生命期。這些LIF可用於連往DNS、AD、LDAP或NIS伺服器的傳出連線、以及一些額外連線、以支援代表整個系統執行的應用程式。從 ONTAP 9.12.1 開始，您可以使用該 `management-log-forwarding`服務來控制將稽核記錄轉送到遠端系統記錄伺服器的生命週期。

下表列出從 ONTAP 9.11.1 開始，在系統 SVM 上可使用的服務：

服務	容錯移轉限制	說明
叢集間核心	僅限主節點	核心叢集間服務
管理核心	-	核心管理服務
管理- ssh	-	SSH管理存取服務
管理-http	-	HTTP 管理存取服務

管理- https	-	HTTPS 管理存取服務
管理自動支援	-	發佈AutoSupport 功能的相關服務
管理- BGP	僅限主連接埠	與BGP對等互動相關的服務
備份NDMP控制	-	NDMP備份控制服務
管理- EMS	-	管理訊息存取服務
管理- NTP用戶端	-	推出於本文件的版本。ONTAP NTP用戶端存取服務。
管理- NTP伺服器	-	推出於本文件的版本。ONTAP NTP伺服器管理存取服務
管理-連接埠對應	-	portmap管理服務
管理伺服器	-	rsh伺服器管理服務
管理SNMP伺服器	-	SNMP伺服器管理服務
管理- Telnet-server	-	用於Telnet伺服器管理的服務
管理記錄轉送	-	推出於本文件的版本為ONTAP 稽核記錄轉送服務

資料**SVM**的服務原則

所有資料SVM都包含服務原則、可供該SVM中的LIF使用。

下表列出以 ONTAP 9.11.1 開頭的資料 SVM 中的生命週期內建原則。對於其他版本、請使用下列命令顯示服務原則及其詳細資料：

```
network interface service-policy show
```

原則	隨附服務	等效資料傳輸協定	說明
預設管理	資料核心，管理-https ，管理 -http ，管理 -ssh ，管理 -DNS-Client ，管理 -ad-Client ，管理 -LDAP-Client ，管理 -NIS-Client	無	使用此SVM範圍內的管理原則來建立資料SVM擁有的SVM管理生命期。這些LIF可用於提供SSH或HTTPS存取給SVM管理員。必要時、這些LIF可用於連往外部DNS、AD、LDAP或NIS伺服器的傳出連線。

預設資料區塊	資料核心、資料iSCSI	iSCSI	用於傳輸區塊導向SAN資料流量的生命體。從 ONTAP 9.10.1 開始，「 default-data-blocks 」原則已過時。改用「預設資料iSCSI」服務原則。
預設資料檔案	資料核心， data-fpolice-client ， data-dnS-server ， FlexCache ， data-CIFS ， data-nfs ， management -dnS -client ， management -ad -client ， management -ldap -client ， management -nis 用戶端	NFS、CIFS、fcache	使用預設資料檔案原則來建立支援檔案型資料傳輸協定的NAS lifs。有時SVM中只有一個LIF、因此此原則允許LIF用於外部DNS、AD、LDAP或NIS伺服器的傳出連線。如果您偏好這些連線只使用管理階層的生命，則可以從此原則移除這些服務。
預設資料iSCSI	資料核心、資料iSCSI	iSCSI	用於傳輸iSCSI資料流量的LIF。
預設資料-NVMe -TCP	資料核心、資料 -NVMe-TCP	NVMe TCP	用於傳輸NVMe/TCP資料流量的生命生命量。

下表列出可用於資料 SVM 的服務，以及從 ONTAP 9.11.1 開始的 LIF 容錯移轉原則所施加的任何限制：

服務	容錯移轉限制	說明
管理- ssh	-	SSH管理存取服務
管理-http	-	在 ONTAP 9.10.1 中推出 HTTP 管理存取服務
管理- https	-	HTTPS 管理存取服務
管理-連接埠對應	-	portmap管理存取服務
管理SNMP伺服器	-	在 ONTAP 9.10.1 中推出 用於 SNMP 伺服器管理存取的服務
資料核心	-	核心資料服務
資料NFS	-	NFS資料服務
資料CIFS	-	CIFS 資料服務

資料FlexCache	-	資料服務FlexCache
資料iSCSI	僅適用於 AFF/FAS 的主連接埠；僅適用於 ASA 的 SFO 合作夥伴	iSCSI資料服務
備份NDMP控制	-	在 ONTAP 9.10.1 中推出 備份NDMP可控制資料服務
資料DNS伺服器	-	在 ONTAP 9.10.1 中推出 DNS伺服器資料服務
資料fpolice-client	-	檔案篩選原則資料服務
資料-NVMe-TCP	僅限主連接埠	在 ONTAP 9.10.1 中推出 NVMe TCP資料服務
資料S3伺服器	-	簡易儲存服務（S3）伺服器資料服務

您應該瞭解如何將服務原則指派給資料SVM中的LIF：

- 如果使用資料服務清單建立資料SVM、則會使用指定的服務來建立該SVM中的內建「預設資料檔案」和「預設資料區塊」服務原則。
- 如果在建立資料SVM時未指定資料服務清單、則會使用預設的資料服務清單來建立該SVM中的內建「預設資料檔案」和「預設資料區塊」服務原則。

  預設的資料服務清單包括iSCSI、NFS、NVMe、SMB及FlexCache 支援服務。

- 如果LIF是以資料傳輸協定清單建立、則會將相當於指定資料傳輸協定的服務原則指派給LIF。
- 如果不存在等效的服務原則、則會建立自訂服務原則。
- 如果在沒有服務原則或資料傳輸協定清單的情況下建立LIF、預設會將預設資料檔案服務原則指派給LIF。

資料核心服務

資料核心服務可讓先前使用LIF搭配資料角色的元件、在已升級的叢集上正常運作、以使用服務原則來管理LIF角色（ONTAP 在S32 9.6中已過時）。

將資料核心指定為服務並不會開啟防火牆中的任何連接埠、但該服務應包含在資料SVM的任何服務原則中。例如、預設的資料檔案服務原則會包含下列服務：

- 資料核心
- 資料NFS
- 資料CIFS
- 資料FlexCache

資料核心服務應包含在原則中、以確保使用LIF的所有應用程式都能如預期般運作、但其他三項服務則可視需要

移除。

用戶端LIF服務

從推出支援支援多種應用程式的支援服務起、支援客戶端LIF服務。ONTAP ONTAP這些服務可控制代表每個應用程式用於傳出連線的LIF。

下列新服務可讓系統管理員控制哪些LIF是用於特定應用程式的來源位址。

服務	SVM限制	說明
管理-廣告用戶端	-	從《支援支援》9.11.1開始ONTAP 、ONTAP 支援Active Directory用戶端服務、以進行外部AD伺服器的傳出連線。
管理DNS用戶端	-	從功能支援的版本起、功能支援DNS用戶端服務、以便連線至外部DNS伺服器。ONTAP ONTAP
管理- LDAP用戶端	-	從功能支援的版本起、支援LDAP用戶端服務、以進行外部LDAP伺服器的傳出連線。ONTAP ONTAP
管理NIS用戶端	-	從功能支援的版本起、功能支援NIS用戶端服務、以進行外部NIS伺服器的傳出連線。ONTAP ONTAP
管理- NTP用戶端	僅限系統	從功能支援的版本起、支援NTP用戶端服務、以便連線至外部NTP伺服器。ONTAP ONTAP
資料fpolice-client	純資料	從功能不全的9.8開始ONTAP 、支援用戶端服務輸出FPolicy連線。ONTAP

某些內建服務原則會自動包含每項新服務、但系統管理員可以將其從內建原則中移除、或將其新增至自訂原則中、以控制代表每個應用程式用於傳出連線的LIF。

相關資訊

- "網路介面服務原則顯示"

管理生命

設定 ONTAP 叢集的 LIF 服務原則

您可以設定LIF服務原則、以識別將使用LIF的單一服務或服務清單。

為lifs建立服務原則

您可以為lifs建立服務原則。您可以將服務原則指派給一或多個LIF、讓LIF能夠傳輸單一服務或服務清單的流量。

您需要進階權限才能執行 `network interface service-policy create` 命令。

關於這項工作

內建的服務和服務原則可用於管理資料和系統SVM上的資料和管理流量。大部分的使用案例都是使用內建服務原則而非建立自訂服務原則來滿足。

您可以視需要修改這些內建服務原則。

步驟

1. 檢視叢集中可用的服務：

```
network interface service show
```

服務代表LIF存取的應用程式、以及叢集所服務的應用程式。每項服務都包含零個或多個應用程式正在偵聽的TCP和udp連接埠。

提供下列額外的資料與管理服務：

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. 檢視叢集中的服務原則：

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. 建立服務原則：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- 「service_name」指定應包含在原則中的服務清單。
- "ip_address/mask"指定允許存取服務原則中服務之位址的子網路遮罩清單。根據預設、所有指定的服務都會新增預設允許位址清單0.00.0.0/0、以允許來自所有子網路的流量。如果提供了非預設允許的位址清單、則使用該原則的LIF會設定為封鎖所有來源位址不符合任何指定遮罩的要求。

  下列範例說明如何針對包含_NFS_和_SMB_服務的SVM建立資料服務原則（*svm1_data_policy_*）：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  下列範例顯示如何建立叢集間服務原則：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. 確認已建立服務原則。

```
cluster1::> network interface service-policy show
```

  下列輸出顯示可用的服務原則：

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
--------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

完成後

在建立時或修改現有LIF、將服務原則指派給LIF。

將服務原則指派給LIF

您可以在建立LIF時或修改LIF、將服務原則指派給LIF。服務原則會定義可與LIF搭配使用的服務清單。

關於這項工作

您可以在管理VM和資料SVM中指派生命權的服務原則。

步驟

視您要將服務原則指派給LIF的時間而定、請執行下列其中一項動作：

如果您...	指派服務原則...
建立LIF	網路介面create -vserver Svm_name -lIF <lif_name>-home-node<node_name>-home-port <port_name> ｛（-address <ip_address>-netMask<ip_address>）-subnet-name <subnet_name>-service-policy <service_policy_name>
修改LIF	網路介面修改-vserver <Svm_name>-lif<lif_name>-service-policy <service_policy_name>

當您為LIF指定服務原則時、不需要指定LIF的資料傳輸協定和角色。也支援透過指定角色和資料傳輸協定來建立LIF。

服務原則只能由建立服務原則時所指定之相同SVM中的LIF使用。

範例

下列範例說明如何修改LIF的服務原則、以使用預設管理服務原則：

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

管理LIF服務原則的命令

使用 `network interface service-policy` 管理 LIF 服務原則的命令。

如"指令參考資料ONTAP"需詳細 `network interface service-policy`資訊，請參閱。

開始之前

在主動 SnapMirror 關係中修改 LIF 的服務原則會中斷複寫排程。如果您將 LIF 從叢集間轉換為非叢集間（反之亦然）、則這些變更不會複寫至對等叢集。若要在修改 LIF 服務原則之後更新對等叢集、請先執行 `snapmirror abort` 然後操作 重新同步複寫關係。

如果您想要...	使用此命令...
建立服務原則（需要進階權限）	`network interface service-policy create`
新增其他服務項目至現有的服務原則（需要進階權限）	`network interface service-policy add-service`

如果您想要...	使用此命令...
複製現有的服務原則（需要進階權限）	`network interface service-policy clone`
修改現有服務原則中的服務項目（需要進階權限）	`network interface service-policy modify-service`
從現有的服務原則移除服務項目（需要進階權限）	`network interface service-policy remove-service`
重新命名現有的服務原則（需要進階權限）	`network interface service-policy rename`
刪除現有的服務原則（需要進階權限）	`network interface service-policy delete`
將內建服務原則還原為原始狀態（需要進階權限）	`network interface service-policy restore-defaults`
顯示現有的服務原則	`network interface service-policy show`

相關資訊

- "網路介面服務展示"
- "網路介面服務原則"
- "SnapMirror中止"

建立 **ONTAP** 生命

SVM透過一或多個網路邏輯介面（LIF）、為用戶端提供資料服務。您必須在您要用來存取資料的連接埠上建立LIF。LIF （網路介面）是與實體或邏輯連接埠相關聯的 IP 位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

最佳實務做法

連接至 ONTAP 的交換器連接埠應設定為跨距樹狀目錄邊緣連接埠、以減少 LIF 移轉期間的延遲。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 基礎實體或邏輯網路連接埠必須設定為管理UP狀態。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用 System Manager 或建立的 `network subnet create` 命令。

  如"指令參考資料ONTAP"需詳細 `network subnet create`資訊，請參閱。

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您無法將NAS和SAN傳輸協定指派給相同的LIF。

  支援的傳輸協定包括SMB、NFS、FlexCache 支援功能、iSCSI和FC； iSCSI和FC無法與其他傳輸協定結合使用。不過、NAS和乙太網路型SAN傳輸協定可以存在於同一個實體連接埠上。

  - 您不應設定承載SMB流量的生命期、以自動還原至其主節點。如果SMB伺服器要裝載解決方案、以便透過Hyper-V或SQL Server透過SMB進行不中斷營運、則此建議為必填。
- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- SVM使用的所有名稱對應和主機名稱解析服務、例如DNS、NIS、LDAP和Active Directory、 必須至少有一個LIF處理SVM的資料流量。
- 處理節點之間叢集內流量的LIF、不應與處理管理流量的LIF或處理資料流量的LIF位於相同的子網路上。
- 建立沒有有效容錯移轉目標的LIF會產生警告訊息。
- 如果叢集中有大量的生命量、您可以驗證叢集上支援的LIF容量：
  - System Manager：從ONTAP 功能完善的9.12.0,開始檢視網路介面網格的處理量。
  - CLI ：使用 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

    深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。
- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他LIF。ONTAP

  從ONTAP 支援FFC-NVMe的支援功能到支援的功能表9.4開始。如果您要建立FC-NVMe LIF、應該注意下列事項：

  - NVMe傳輸協定必須受到建立LIF的FC介面卡支援。
  - FC-NVMe是資料生命中唯一的資料傳輸協定。
- 必須為每個支援SAN的儲存虛擬機器（SVM）設定一個LIF處理管理流量。
- NVMe LIF和命名空間必須裝載在同一個節點上。
- 每個 SVM 每個節點最多可設定兩個處理資料流量的 NVMe 生命。
- 當您建立具有子網路的網路介面時ONTAP 、ENetApp會自動從所選子網路選取可用的IP位址、並將其指派給網路介面。如果有多個子網路、您可以變更子網路、但無法變更IP位址。
- 建立（新增）SVM時、您無法為網路介面指定位於現有子網路範圍內的IP位址。您會收到子網路衝突錯誤。此問題發生在網路介面的其他工作流程中、例如在SVM設定或叢集設定中建立或修改叢集間網路介面。
- 從 ONTAP 9.10.1 開始， `network interface` CLI 命令包含 `-rdma-protocols`透過 RDMA 組態的 NFS 參數。從 ONTAP 9.12.1 開始，系統管理員支援透過 RDMA 組態建立 NFS 的網路介面。如需更多資訊、請參閱 透過RDMA設定NFS的LIF。
- 從 ONTAP 9.11.1 開始、全快閃 SAN 陣列（ASA）平台可自動進行 iSCSI LIF 容錯移轉。

iSCSI LIF 容錯移轉會自動啟用（容錯移轉原則設為 `sfo-partner-only` 且自動還原值設為 `true`）如果指定 SVM 中不存在 iSCSI 生命負載、或指定 SVM 中所有現有的 iSCSI 生命負載均已透過 iSCSI LIF 容錯移轉啟用、則新建立的 iSCSI 生命負載。

如果您升級至 ONTAP 9.11.1 或更新版本後、 SVM 中現有的 iSCSI 生命體尚未啟用 iSCSI LIF 容錯移轉功能、且您在同一個 SVM 中建立新的 iSCSI 生命體、則新的 iSCSI 生命體將採用相同的容錯移轉原則 (`disabled`） SVM 中現有的 iSCSI 生命。

"適用於ASA 各種平台的iSCSI LIF容錯移轉"

從ONTAP 支援支援的版本9.7開始、ONTAP 只要IPspace的同一子網路中至少已存在一個LIF、則該產品就會自動選擇LIF的主連接埠。在同一個廣播網域中選擇一個主連接埠、以作為該子網路中的其他LIF。ONTAP您仍可指定主連接埠、但不再需要主連接埠（除非該子網路在指定的IPspace中尚不存在任何生命區）。

從ONTAP 功能性的9.12.0開始、您所遵循的程序取決於您所使用的介面-系統管理員或CLI：

系統管理員

使用**System Manager**新增網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 選取 + Add 。
3. 選取下列其中一個介面角色：
   a. 資料
   b. 叢集間
   c. SVM管理
4. 選取傳輸協定：
   a. SMB/CIFS與NFS
   b. iSCSI
   c. FC
   d. NVMe / FC
   e. NVMe / TCP
5. 命名LIF或接受先前選擇所產生的名稱。
6. 接受主節點、或使用下拉式選單選取一個節點。
7. 如果在所選SVM的IPspace中至少設定一個子網路、則會顯示子網路下拉式清單。
   a. 如果您選取子網路、請從下拉式清單中選擇該子網路。
   b. 如果您在沒有子網路的情況下繼續、則會顯示「廣播網域」下拉式清單：
      i. 指定IP位址。如果IP位址正在使用中、則會顯示警告訊息。
      ii. 指定子網路遮罩。
8. 從廣播網域中選取主連接埠、可以是自動（建議）或從下拉式功能表中選取一個。主連接埠控制項會根據廣播網域或子網路選擇來顯示。
9. 儲存網路介面。

CLI

- 使用 CLI 建立 LIF*

步驟

1. 確定要用於LIF的廣播網域連接埠。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain show`資訊，請參閱。

2. 驗證要用於lifs的子網路是否包含足夠的未使用IP位址。

   `network subnet show -ipspace` *`ipspace1`*

   如"指令參考資料ONTAP"需詳細 `network subnet show`資訊，請參閱。

3. 在您要用來存取資料的連接埠上建立一個或多個生命體。

   NetApp 建議為資料 SVM 上的所有生命建立子網路物件。這對 MetroCluster 組態尤其重要，因為每個子網路物件都有相關的廣播網域，因此子網路物件可讓 ONTAP 判斷目的地叢集上的容錯移轉目標。有關說明，請參閱"建立子網路"。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

     您也可以使用-autom-revert選項、指定LIF是否應自動還原為主節點和主連接埠。

   如"指令參考資料ONTAP"需詳細 `network interface revert`資訊，請參閱。

   - `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
   - 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
   - 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
   - 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。如"指令參考資料ONTAP"需詳細 `network route create`資訊，請參閱。
   - `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下

自動還原至其主節點。預設設定為 `false`但您可以將其設定為 `true` 視環境中的網路管理原則而定。

- `-service-policy` 從 ONTAP 9.5 開始、您可以使用指派 LIF 的服務原則 `-service-policy` 選項。
  當為LIF指定服務原則時、該原則會用來建構LIF的預設角色、容錯移轉原則和資料傳輸協定清單。在支援的過程中、服務原則僅適用於叢集間和BGP對等服務。ONTAP在NetApp 9.6中ONTAP 、您可以建立多種資料與管理服務的服務原則。
- `-data-protocol` 可讓您建立支援 FCP 或 NVMe / FC 傳輸協定的 LIF 。建立IP LIF時不需要此選項。

4. 選用：在-address選項中指派IPv6位址：

   a. 使用 `network ndp prefix show` 用於查看在各種接口上學習的 RA 前綴列表的命令。

      - `network ndp prefix show` 命令可在進階權限層級使用。

      如"指令參考資料ONTAP"需詳細 `network ndp prefix show`資訊，請參閱。

   b. 使用格式 `prefix::id` 手動建構 IPv6 位址。

      `prefix` 是在各種介面上學習的首碼。

   用於導出 `id`，選擇隨機 64 位元十六進位數字。

5. 驗證LIF介面組態是否正確。

   ```
   network interface show -vserver vs1
   ```

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1       up/up      10.0.0.128/24    node1     e0d
   true
   ```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

6. 確認容錯移轉群組組態符合需求。

   ```
   network interface show -failover -vserver vs1
   ```

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
--------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	網路ping
IPv6位址	網路ping6.

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

下列命令會建立一個 NVMe / FC LIF 並指定 `nvme-fc` 資料傳輸協定：

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

修改 **ONTAP** 生命

您可以變更主節點或目前節點、管理狀態、IP位址、網路遮罩、容錯移轉原則、 防火牆原則和服務原則。您也可以將LIF的位址系列從IPV4變更為IPV6。

關於這項工作

- 將LIF的管理狀態修改為「關機」時、任何未完成的NFSv4鎖定都會保留、直到LIF的管理狀態恢復為「開機」為止。

為了避免其他生命週期嘗試存取鎖定檔案時發生鎖定衝突、您必須先將NFSv4用戶端移至不同的LIF、再將管理狀態設為向下。

- 您無法修改FC LIF所使用的資料傳輸協定。不過、您可以修改指派給服務原則的服務、或變更指派給IP LIF的服務原則。

  若要修改FC LIF所使用的資料傳輸協定、您必須刪除並重新建立LIF。若要變更IP LIF的服務原則、更新期間會短暫中斷。

- 您無法修改主節點或節點範圍管理LIF的目前節點。
- 使用子網路變更LIF的IP位址和網路遮罩值時、會從指定的子網路分配IP位址；如果LIF的先前IP位址來自不同的子網路、則IP位址會傳回該子網路。
- 若要將 LIF 的位址系列從 IPv4 修改為 IPv6 、您必須使用冒號表示法來表示 IPv6 位址、並為新增值 `-netmask-length` 參數。
- 您無法修改自動設定的連結本機IPv6位址。
- 修改LIF會導致LIF沒有有效的容錯移轉目標、因此會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 從功能介紹9.5開始ONTAP 、您可以修改與LIF相關的服務原則。

  在支援的過程中、服務原則僅適用於叢集間和BGP對等服務。ONTAP在NetApp 9.6中ONTAP 、您可以建立多種資料與管理服務的服務原則。

- 從 ONTAP 9.11.1 開始、自動 iSCSI LIF 容錯移轉功能可在 All Flash SAN Array （ASA）平台上使用。

  對於預先存在的 iSCSI 生命體（即升級至 9.11.1 或更新版本之前建立的生命體）、您可以將容錯移轉原則修改為 "啟用自動 iSCSI LIF 容錯移轉"。

- ONTAP利用網路時間協定 (NTP) 來同步整個叢集的時間。變更 LIF IP 位址後，您可能需要更新 NTP 設定以防止同步失敗。欲了解更多信息，請參閱"NetApp知識庫：LIF IP 變更後 NTP 同步失敗"。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**編輯網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁選取 ⋮ * > 編輯 * 。
3. 變更一或多個網路介面設定。如需詳細資訊、請參閱 "建立LIF"。
4. 儲存您的變更。

CLI

使用**CLI**修改**LIF**

步驟

1. 使用修改 LIF 屬性 `network interface modify` 命令。

   下列範例說明如何使用IP位址和子網路client1_sub的網路遮罩值來修改LIF datalif2的IP位址和網路遮罩：

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   下列範例說明如何修改LIF的服務原則。

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   如"指令參考資料ONTAP"需詳細 `network interface modify`資訊，請參閱。

2. 驗證IP位址是否可連線。

如果您使用…	然後使用…
IPV4位址	`network ping`
IPv6位址	`network ping6`

   如"指令參考資料ONTAP"需詳細 `network ping`資訊，請參閱。

移轉 **ONTAP** 生命

如果連接埠故障或需要維護、您可能必須將LIF移轉至同一個節點或叢集中的不同節點上的不同連接埠。移轉LIF與LIF容錯移轉類似、但LIF移轉是手動作業、而LIF容錯移轉則是LIF

的自動移轉、以因應LIF目前網路連接埠上的連結故障。

開始之前

- 必須已為lifs設定容錯移轉群組。
- 目的地節點和連接埠必須正常運作、而且必須能夠存取與來源連接埠相同的網路。

關於這項工作

- BGP LIF位於主連接埠上、無法移轉至任何其他節點或連接埠。
- 從節點移除NIC之前、您必須先將屬於NIC的連接埠上裝載的LIF移轉至叢集中的其他連接埠。
- 您必須執行命令、從裝載叢集LIF的節點移轉叢集LIF。
- 節點範圍的LIF（例如節點範圍管理LIF、叢集LIF、叢集間LIF）無法移轉至遠端節點。
- 當NFSv4 LIF在節點之間移轉時、新連接埠上的LIF可用前、延遲最多可達45秒。

  若要解決此問題、請在沒有延遲的情況下使用NFSv4.1。

- 您可以在執行 ONTAP 9.11.1 或更新版本的 All Flash SAN Array （ ASA ）平台上移轉 iSCSI 生命體。

  移轉iSCSI LIF僅限於主節點或HA合作夥伴上的連接埠。

- 如果您的平台不是執行 ONTAP 9.11.1 版或更新版本的 All Flash SAN Array （ ASA ）平台、則無法將 iSCSI 生命體從一個節點移轉至另一個節點。

  若要解決此限制、您必須在目的地節點上建立iSCSI LIF。瞭解 "建立iSCSI LIF"。

- 如果您想要透過RDMA移轉LIF（網路介面）for NFS、則必須確保目的地連接埠具有RoCE功能。您必須執行ONTAP 版本S廳9.10.1或更新版本、才能使用CLI移轉LIF、ONTAP 或使用System Manager移轉版本。在System Manager中、一旦您選取了具備RoCE功能的目的地連接埠、就必須勾選*使用roce連接埠*旁的方塊、才能成功完成移轉。深入瞭解 "透過RDMA設定NFS的LIF"。
- 當您移轉來源或目的地LIF時、VMware VAAI複製卸載作業會失敗。深入瞭解卸載複本：
  - "NFS 環境"
  - "SAN環境"

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**移轉網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁邊選取 ⋮ * > Migrate* 。

   對於 iSCSI LIF 、請在 * 移轉介面 * 對話方塊中、選取 HA 合作夥伴的目的地節點和連接埠。

   如果您要永久移轉 iSCSI LIF 、請選取核取方塊。iSCSI LIF 必須先離線、才能永久移轉。此外、一旦iSCSI LIF永久移轉、就無法復原。沒有還原選項。

3. 按一下*移轉*。
4. 儲存您的變更。

CLI

使用**CLI**移轉**LIF**

步驟

視您要移轉特定LIF或所有LIF而定、請執行適當的動作：

如果您想要移轉...	輸入下列命令...
特定LIF	`network interface migrate`
節點上的所有資料和叢集管理生命體	`network interface migrate-all`
連接埠上的所有生命	`network interface migrate-all -node <node> -port <port>`

下列範例說明如何移轉名為的LIF `datalif1` 在SVM上 `vs0` 連接埠 `e0d` 開啟 `node0b`：

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

以下範例說明如何從目前（本機）節點移轉所有資料與叢集管理生命週期：

```
network interface migrate-all -node local
```

相關資訊

- "網路介面移轉"

在 **ONTAP** 節點容錯移轉或連接埠移轉之後，將 **LIF** 還原至其主連接埠

您可以在LIF容錯移轉或手動或自動移轉至其他連接埠之後、將其還原至主連接埠。如果特定LIF的主連接埠無法使用、則LIF會保留在目前的連接埠、不會還原。

關於這項工作

- 如果您在設定自動還原選項之前、以管理方式將LIF的主連接埠移至「UP」狀態、則LIF不會傳回主連接埠。
- 除非「自動回復」選項的值設為true、否則LIF不會自動回復。
- 您必須確保已啟用「自動還原」選項、以便讓I生命 回復到主連接埠。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**將網路介面還原為其主連接埠

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁選取 ⋮ * > Revert * 。
3. 選取*還原*可將網路介面還原至其主連接埠。

CLI

使用**CLI**將**LIF**還原為其主連接埠

步驟

手動或自動將LIF還原至主連接埠：

如果您想要將LIF還原至其主連接埠…	然後輸入下列命令…
手動	`network interface revert -vserver vserver_name -lif lif_name`
自動	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

如"指令參考資料ONTAP"需詳細 `network interface`資訊，請參閱。

恢復設定不正確的 **ONTAP LIF**

叢集網路連線至交換器時、無法建立叢集、但叢集IPspace中設定的所有連接埠、都無法連線至叢集IPspace中設定的其他連接埠。

關於這項工作

在交換式叢集中、如果叢集網路介面（ LIF ）設定在錯誤的連接埠上、或是叢集連接埠連接到錯誤的網路、則為

`cluster create` 命令可能會失敗、並出現下列錯誤：

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

如"指令參考資料ONTAP"需詳細 `cluster create`資訊，請參閱。

命令的結果 `network port show`可能會顯示數個連接埠已新增至叢集 IPspace ，因為它們已連線至使用叢集 LIF 設定的連接埠。然而， `network port reachability show -detail`指令顯示哪些連接埠彼此之間沒有連線。

如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

若要從連接埠上設定的叢集LIF還原、而該連接埠無法連線至使用叢集lifs設定的其他連接埠、請執行下列步驟：

步驟

1. 將叢集LIF的主連接埠重設為正確的連接埠：

   ```
   network port modify -home-port
   ```

   如"指令參考資料ONTAP"需詳細 `network port modify`資訊，請參閱。

2. 從叢集廣播網域中移除未設定叢集lifs的連接埠：

   ```
   network port broadcast-domain remove-ports
   ```

   如"指令參考資料ONTAP"需詳細 `network port broadcast-domain remove-ports`資訊，請參閱。

3. 建立叢集：

   ```
   cluster create
   ```

結果

當您完成叢集建立時、系統會偵測到正確的組態、並將連接埠放入正確的廣播網域。

相關資訊

- "網路連接埠連線能力顯示"

刪除 **ONTAP** 生命

您可以刪除不再需要的網路介面（LIF）。

開始之前

要刪除的生命期不得在使用中。

步驟

1. 使用以下命令將要刪除的生命期標記爲管理性關閉：

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. 使用 `network interface delete` 刪除一或所有生命的命令：

如果您要刪除...	輸入命令...
特定LIF	`network interface delete -vserver vserver_name -lif lif_name`
所有生命	`network interface delete -vserver vserver_name -lif *`

如"指令參考資料ONTAP"需詳細 `network interface delete`資訊，請參閱。

下列命令會刪除LIF mgmtlif2：

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. 使用 `network interface show` 確認 LIF 已刪除的命令。

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

設定 ONTAP 虛擬 IP （ VIP ）生命

有些新一代資料中心使用第 3 層（ IP ）網路機制，需要在子網路之間容錯移轉。ONTAP 支援虛擬 IP （ VIP ）資料生命體，以及相關的路由傳輸協定，邊界閘道傳輸協定（ BGP ），以滿足這些新一代網路的容錯移轉需求。

關於這項工作

VIP資料LIF並非任何子網路的一部分、可從以相同IPspace裝載BGP LIF的所有連接埠存取。VIP資料LIF可消除主機對個別網路介面的相依性。由於多個實體介面卡會傳輸資料流量、因此整個負載不會集中在單一介面卡和相關子網路上。VIP資料LIF是透過路由傳輸協定邊界閘道傳輸協定（BGP）通告給對等路由器。

VIP資料生命量具備下列優點：

- LIF可攜性超越廣播網域或子網路：VIP資料LIF可透過BGP向路由器宣告每個VIP資料LIF的目前位置、容錯移轉至網路中的任何子網路。
- Aggregate處理量：VIP資料生命量可支援超過任何個別連接埠頻寬的Aggregate處理量、因為VIP生命量可以同時從多個子網路或連接埠傳送或接收資料。

設定邊界閘道傳輸協定（**BGP**）

在建立VIP生命期之前、您必須先設定BGP、這是用於向對等路由器宣告VIP LIF存在的路由傳輸協定。

從 ONTAP 9 9.1 開始， VIP 提供選用的預設路由自動化功能，使用 BGP 對等群組來簡化組態。

當BGP對等端點位於同一子網路時、使用BGP對等端點做為下一跳路由器、即可輕鬆學習預設路由。ONTAP若要使用此功能、請設定 `-use-peer-as-next-hop` 屬性至 `true`。依預設、此屬性為 `false`。

如果您已設定靜態路由、則這些路由仍會優先於這些自動預設路由。

開始之前

對等路由器必須設定為接受來自BGP LIF的BGP連線、以取得所設定的自治系統編號（ASN）。

> 不處理來自路由器的任何傳入路由宣告、因此您應該設定對等路由器、使其不傳送任何路由更新到叢集。ONTAP如此可縮短與對等通訊完全正常運作所需的時間，並減少 ONTAP 內部的記憶體使用量。

關於這項工作

設定BGP包括選擇性地建立BGP組態、建立BGP LIF、以及建立BGP對等群組。當在指定節點上建立第一個BGP對等群組時、使用預設值自動建立預設BGP組態。ONTAP

BGP LIF用於與對等路由器建立BGP TCP工作階段。對於對等路由器而言、BGP LIF是下一跳、可到達VIP LIF。BGP LIF已停用容錯移轉。BGP 對等群組會在對等群組使用的 IPspace 中，為所有 SVM 通告 VIP 路由。對等群組使用的 IPspace 是從 BGP LIF 繼承而來。

從 ONTAP 9 。 16.1 開始， BGP 對等群組支援 MD5 驗證，以保護 BGP 工作階段。啟用 MD5 時， BGP 工作階段只能在獲授權的對等點之間建立和處理，以防止未獲授權的使用者可能中斷工作階段。

下列欄位已新增至 `network bgp peer-group create`和 `network bgp peer-group modify`命令：

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

這些參數可讓您使用 MD5 簽章來設定 BGP 對等群組，以增強安全性。下列需求適用於使用 MD5 驗證：

- 您只能在參數設定為 `true`**時指定** `-md5-secret`**參數** `-md5-enabled`。
- 您必須先全域啟用 IPsec ，才能啟用 MD5 BGP 驗證。BGP LIF 不一定要有作用中的 IPsec 組態。請參閱 "透過有線加密設定IP安全性（IPsec）"。
- NetApp 建議您先在路由器上設定 MD5, 然後再在 ONTAP 控制器上進行設定。

從功能變數9.9開始ONTAP 、新增了下列欄位：

- `-asn`**或** `-peer-asn`（ 4 位元組值）屬性本身不是新的，但現在使用 4 位元組整數。
- `-med`
- `-use-peer-as-next-hop`

您可以利用多重出口鑑別器（MED-）支援、針對路徑優先順序進行進階路由選擇。BGP更新訊息中的選用屬性Medion、可讓路由器為流量選取最佳路由。MEDA是無符號32位元整數（0 - 4294967295）、偏好較低的

值。

從 ONTAP 9.8 開始、這些欄位已新增至 `network bgp peer-group` 命令：

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

這些BGP屬性可讓您設定BGP對等群組的AS路徑和社群屬性。

雖然 ONTAP 支援上述 BGP 屬性，但路由器不需要遵守這些屬性。NetApp 強烈建議您確認路由器支援哪些屬性，並據此設定 BGP 對等群組。如需詳細資料、請參閱路由器提供的BGP文件。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 選用：執行下列其中一項動作、建立BGP組態或修改叢集的預設BGP組態：

   a. 建立BGP組態：

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   - 此 `-routerid`參數接受點分十進制 `32` 位元值，只需在 `AS` 網域內唯一即可。`NetApp` 建議您使用保證唯一性的節點管理 `IP` （ `v4` ）位址 `<router_id>`。
   - 雖然 ONTAP BGP 支援 32 位元 ASN 數字，但僅支援標準十進位標記法。不支援私有 ASN 的點狀 ASN 表示法，例如 65000.1 ，而非 4259840001 。

   2位元組ASN的範例：

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

   使用4位元組ASN的範例：

   ```
   network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
   1.1.1.1
   ```

   a. 修改預設BGP組態：

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>`指定 ASN 編號。從支援BGP的ASN 9.8開始ONTAP 、支援2位元組非負整數。這是一個 16 位元數字（ 1 到 65534 個可用值）。從 ONTAP 9 9.1 開始， BGP 的 ASN 支援 4 位元組非負整數（ 1 至 4294967295 ）。預設ASN為65501。ASN 23456保留用於ONTAP 建立不宣告4位元組ASN功能的對等端點、以供建立不含
- `<hold_time>`指定保留時間（以秒為單位）。預設值為 180s 。

ONTAP 僅支援一個全域 `<asn_number>`， `<hold_time>`，和 `<router_id>`，即使您為多個 IPspace 設定 BGP 也一樣。BGP 和所有 IP 路由資訊完全隔離在一個 IPspace 內。IPspace 相當於虛擬路由和轉送（ VRF ）執行個體。

3. 為系統SVM建立BGP LIF：

   對於預設 IPspace ， SVM 名稱是叢集名稱。對於其他 IPspace ， SVM 名稱與 IPspace 名稱相同。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

   您可以使用 `default-route-announce` BGP LIF 的服務原則或任何包含「管理 BGP 」服務的自訂服務原則。

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. 建立BGP對等群組、用於與遠端對等路由器建立BGP工作階段、並設定通告給對等路由器的VIP路由資訊：

   範例1：建立沒有自動預設路由的對等群組

   在這種情況下，管理員需要建立通往 BGP 對等點的靜態路由。

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

範例2：使用自動預設路由建立對等群組

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

範例 3 ：建立啟用 MD5 的對等群組

a. 啟用IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

b. 建立啟用 MD5 的 BGP 對等群組：

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
   ```

   使用十六進位金鑰的範例：

   ```
   network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
   -lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
   0x746573742073656372657
   ```

   使用字串的範例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

建立 BGP 對等群組之後，執行命令時會列出虛擬乙太網路連接埠（以 v0a.v0z ， v1a… 開頭）`network port show`。此介面的 MTU 一律以 1500 報告。用於流量的實際 MTU 是從實體連接埠（ BGP LIF ）衍生而來，此連接埠是在流量傳送時決定的。如"指令參考資料ONTAP"需詳細`network port show`資訊，請參閱。

建立虛擬IP（VIP）資料LIF

VIP資料LIF是透過路由傳輸協定邊界閘道傳輸協定（BGP）通告給對等路由器。

開始之前

- 必須設定BGP對等群組、且要建立LIF的SVM之BGP工作階段必須處於作用中狀態。
- 必須為 SVM 的任何傳出 VIP 流量建立通往 BGP 路由器或 BGP LIF 子網路中任何其他路由器的靜態路由。
- 您應該開啟多重路徑路由，以便傳出的 VIP 流量可以使用所有可用的路由。

  如果未啟用多重路徑路由、則所有傳出的VIP流量都會從單一介面發出。

步驟

1. 建立VIP資料LIF：

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   如果您未使用指定主連接埠、則會自動選取 VIP 連接埠 `network interface create` 命令。

   根據預設、VIP資料LIF屬於系統建立的每個IPspace名為「VIP」的廣播網域。您無法修改VIP廣播網域。

   VIP資料LIF可同時在裝載BGP LIF IP空間的所有連接埠上存取。如果本機節點上的VIP SVM沒有作用中的BGP工作階段、則VIP資料LIF會容錯移轉至節點上已針對該SVM建立BGP工作階段的下一個VIP連接埠。

2. 驗證BGP工作階段是否處於VIP資料LIF SVM的UP狀態：

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

如果 BGP 狀態為 `down` 對於節點上的 SVM 、 VIP 資料 LIF 會容錯移轉至另一個節點、而該節點的 BGP 狀態是 SVM 的正常狀態。如果 BGP 狀態為 `down` 在所有節點上、 VIP 資料 LIF 無法在任何位置託管、且 LIF 狀態為「關閉」。

管理**BGP**的命令

從 ONTAP 9.5 開始、您可以使用 `network bgp` 用於管理 ONTAP 中 BGP 工作階段的命令。

管理**BGP**組態

如果您想要…	使用此命令…
建立BGP組態	`network bgp config create`
修改BGP組態	`network bgp config modify`
刪除BGP組態	`network bgp config delete`
顯示BGP組態	`network bgp config show`
顯示VIP LIF SVM的BGP狀態	`network bgp vserver-status show`

管理**BGP**預設值

如果您想要…	使用此命令…
修改BGP預設值	`network bgp defaults modify`
顯示BGP預設值	`network bgp defaults show`

管理**BGP**對等群組

如果您想要…	使用此命令…
建立BGP對等群組	`network bgp peer-group create`
修改BGP對等群組	`network bgp peer-group modify`
刪除BGP對等群組	`network bgp peer-group delete`
顯示BGP對等群組資訊	`network bgp peer-group show`
重新命名BGP對等群組	`network bgp peer-group rename`

使用 **MD5** 管理 **BGP** 對等群組

從 ONTAP 9 。 16.1 開始，您可以在現有的 BGP 對等群組上啟用或停用 MD5 驗證。

> ⓘ 如果您在現有的 BGP 對等群組上啟用或停用 MD5 ，則 BGP 連線會終止並重新建立，以套用 MD5 組態變更。

如果您想要…	使用此命令…

在現有的 BGP 對等群組上啟用 MD5	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
在現有的 BGP 對等群組上停用 MD5	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

相關資訊

- "指令參考資料ONTAP"
- "網路 BGP"
- "網路介面"
- "安全性IPsec組態修改"

平衡網路負載

使用 **DNS** 負載平衡最佳化 **ONTAP** 網路流量

您可以將叢集設定為從適當載入的lifs處理用戶端要求。如此一來、生命與連接埠的使用率就會更加平衡、進而提升叢集的效能。

DNS負載平衡有助於選擇適當負載的資料LIF、並平衡所有可用連接埠（實體、介面群組和VLAN）之間的使用者網路流量。

透過DNS負載平衡、LIF會與SVM的負載平衡區域建立關聯。站台範圍的DNS伺服器已設定為轉送所有DNS要求、並根據網路流量和連接埠資源的可用度（CPU使用率、處理量、開放式連線等）、傳回負載最低的LIF。DNS負載平衡具有下列優點：

- 新的用戶端連線在可用資源之間取得平衡。
- 無需手動介入、即可決定在掛載特定SVM時要使用哪些LIF。
- DNS 負載平衡支援 NFSv3 、 NFSv4 、 NFSv4.1 、 SMB 2.0 、 SMB 2.1 、 SMB 3.0 和 S3 。

瞭解 **ONTAP** 網路的 **DNS** 負載平衡

用戶端可藉由指定IP位址（與LIF關聯）或主機名稱（與多個IP位址關聯）來掛載SVM。依預設、整個站台的DNS伺服器會以循環配置資源的方式選取生命體、以平衡所有生命體的工作負載。

循環資源負載平衡可能會導致部分生命量過載、因此您可以選擇使用DNS負載平衡區域來處理SVM中的主機名稱解析。使用DNS負載平衡區域、可確保新用戶端連線在可用資源之間取得更好的平衡、進而提升叢集的效能。

DNS負載平衡區域是叢集內的DNS伺服器、可動態評估所有LIF上的負載、並傳回適當載入的LIF。在負載平衡區域中、DNS會根據負載、為每個LIF指派權重（度量）。

每個LIF都會根據其主節點的連接埠負載和CPU使用率來指派一個權重。負載較少的連接埠上的LIF在DNS查詢中傳回的機率較高。您也可以手動指派權重。

為 ONTAP 網路建立 DNS 負載平衡區域

您可以建立DNS負載平衡區域、以便根據負載（即LIF上掛載的用戶端數目）、動態選擇LIF。您可以在建立資料LIF時建立負載平衡區域。

開始之前

站台範圍DNS伺服器上的DNS轉寄站必須設定為將負載平衡區域的所有要求轉送到設定的LIF。

這"NetApp知識庫：如何在叢集模式下設定 DNS 負載平衡"包含有關使用條件轉送配置 DNS 負載平衡的詳細資訊。

關於這項工作

- 任何資料LIF都能回應DNS查詢、以取得DNS負載平衡區域名稱。
- DNS負載平衡區域在叢集中必須有唯一的名稱、而且區域名稱必須符合下列需求：
  - 不得超過256個字元。
  - 其中應至少包含一段期間。
  - 第一個和最後一個字元不應為句點或任何其他特殊字元。
  - 字元之間不得包含任何空格。
  - DNS名稱中的每個標籤不得超過63個字元。

    標籤是指在期間之前或之後出現的文字。例如、名稱為storage.company.com的DNS區域有三個標籤。

步驟

使用 `network interface create`命令搭配 `dns-zone`選項來建立 DNS 負載平衡區域。如"指令參考資料ONTAP"需詳細 `network interface create`資訊，請參閱。

如果負載平衡區域已存在、則會將LIF新增至該區域。

下列範例示範如何在建立 LIF 時建立名為 storage.company.com 的 DNS 負載平衡區域 `lif1`：

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

從負載平衡區域新增或移除 ONTAP LIF

您可以從虛擬機器（SVM）的DNS負載平衡區域新增或移除LIF。您也可以從負載平衡區域同時移除所有的LIF。

開始之前

- 負載平衡區域中的所有LIF都應該屬於同一個SVM。

- LIF只能是一個DNS負載平衡區域的一部分。
- 如果生命體屬於不同的子網路、則必須設定每個子網路的容錯移轉群組。

關於這項工作

處於管理中斷狀態的LIF會從DNS負載平衡區域中暫時移除。當LIF返回管理UP狀態時、LIF會自動新增至DNS負載平衡區域。

步驟

在負載平衡區域中新增LIF或移除LIF：

如果您想要...	輸入...

新增LIF	`network interface modify -vserver vserver_name -lif lif_name -dns-zone zone_name`
	範例：
	`network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

移除單一LIF	`network interface modify -vserver vserver_name -lif lif_name -dns-zone none`
	範例：
	`network interface modify -vserver vs1 -lif data1 -dns -zone none`

移除所有生命	`network interface modify -vserver vserver_name -lif * -dns-zone none`
	範例：
	`network interface modify -vserver vs0 -lif * -dns-zone none`
	您可以從負載平衡區域移除 SVM 中的所有生命負載、以移除 SVM 中的 SVM 。

相關資訊

- "修改網路介面"

設定 ONTAP 網路的 DNS 服務

在建立NFS或SMB伺服器之前、您必須先為SVM設定DNS服務。一般而言、DNS名稱伺服器是NFS或SMB伺服器要加入之網域的Active Directory整合式DNS伺服器。

關於這項工作

Active Directory整合式DNS伺服器包含網域LDAP和網域控制器伺服器的服務位置記錄（SRV),如果SVM找不到Active Directory LDAP伺服器和網域控制器、NFS或SMB伺服器設定就會失敗。

SVM使用主機名稱服務ns-交換器資料庫來判斷要使用哪些名稱服務、以及在查詢主機資訊時的順序。主機資料庫支援的兩種名稱服務為檔案和DNS。

在建立SMB伺服器之前、您必須確定DNS是其中一個來源。

若要檢視mgwd程序和SecD程序的DNS名稱服務統計資料、請使用統計資料UI。

步驟

1. 判斷主機名稱服務資料庫目前的組態為何。在此範例中、主機名稱服務資料庫會使用預設設定。

   `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 如有必要、請執行下列動作。

   a. 依所需順序將DNS名稱服務新增至主機名稱服務資料庫、或重新排序來源。

      在此範例中、主機資料庫會設定為依該順序使用DNS和本機檔案。

      `vserver services name-service *ns-switch* modify -vserver *vs1* -database *hosts* -sources *dns,files*`

   b. 驗證名稱服務組態是否正確。

      `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. 設定DNS服務。

   `vserver services name-service dns create -vserver *vs1* -domains *example.com,example2.com* -name-servers *10.0.0.50,10.0.0.51*`

   vserver services name-service DNS create命令會執行自動組態驗證、並在ONTAP 無法聯絡名稱伺服器時回報錯誤訊息。

4. 確認DNS組態正確、且服務已啟用。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. 驗證名稱伺服器的狀態。

```
vserver services name-service dns check -vserver vs1
```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

在SVM上設定動態DNS

如果您想要Active Directory整合式DNS伺服器在DNS中動態登錄NFS或SMB伺服器的DNS記錄、則必須在SVM上設定動態DNS（DDNS）。

開始之前

必須在SVM上設定DNS名稱服務。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器、而且必須為SVM建立NFS或SMB伺服器或Active Directory帳戶。

關於這項工作

指定的完整網域名稱（FQDN）必須是唯一的：

指定的完整網域名稱（FQDN）必須是唯一的：

- 若為 NFS 、則為中指定的值 `-vserver-fqdn` 作為的一部分 `vserver services name-service dns dynamic-update` 命令會成為已註冊的 FQDN 。
- 對於SMB、指定為CIFS伺服器的NetBios名稱和CIFS伺服器完整網域名稱的值、會成為該LIF的註冊FQDN。這在ONTAP 不進行設定的情況下無法進行。在下列案例中、LIF FQDN為「CIFS_VS1.EXAMPLE.COM":」

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

若要避免SVM FQDN組態失敗、但不符合DDNS更新的RFC規則、請使用符合RFC規範的FQDN名稱。如需詳細資訊、請參閱 "RFC 1123"。

步驟

1. 在SVM上設定DDNS：

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   星號無法作為自訂FQDN的一部分使用。例如、 `*.netapp.com` 無效。

2. 確認DDNS組態正確：

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

設定 **ONTAP** 網路的動態 **DNS** 服務

如果您想要Active Directory整合式DNS伺服器在DNS中動態登錄NFS或SMB伺服器的DNS記錄、則必須在SVM上設定動態DNS（DDNS）。

開始之前

必須在SVM上設定DNS名稱服務。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器、而且必須為SVM建立NFS或SMB伺服器或Active Directory帳戶。

關於這項工作

指定的FQDN必須是唯一的。

> 若要避免SVM FQDN組態失敗、但不符合DDNS更新的RFC規則、請使用符合RFC規範的FQDN名稱。

步驟

1. 在SVM上設定DDNS：

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   星號無法作為自訂FQDN的一部分使用。例如、 `*.netapp.com` 無效。

2. 確認DDNS組態正確：

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

主機名稱解析

瞭解 ONTAP 網路的主機名稱解析

必須能夠將主機名稱轉譯為數字IP位址、才能存取用戶端及存取服務。ONTAP您必須設定儲存虛擬機器（SVM）、才能使用本機或外部名稱服務來解析主機資訊。支援設定外部DNS伺服器、或設定本機主機檔案以進行主機名稱解析。ONTAP

使用外部DNS伺服器時、您可以設定動態DNS（DDNS）、它會自動將新的或變更的DNS資訊從儲存系統傳送到DNS伺服器。如果沒有動態DNS更新、您必須在新系統上線或現有DNS資訊變更時、手動將DNS資訊（DNS名稱和IP位址）新增至識別的DNS伺服器。此程序緩慢且容易出錯。在災難恢復期間、手動設定可能會導致長時間停機。

設定 DNS 以進行 ONTAP 網路的主機名稱解析

您可以使用DNS存取本機或遠端來源以取得主機資訊。您必須設定DNS、才能存取其中一個或兩個來源。

必須能夠查詢主機資訊、才能正確存取用戶端。ONTAP您必須設定名稱服務、才能啟用ONTAP 支援功能、以存取本機或外部DNS服務來取得主機資訊。

ONTAP 會將名稱服務組態資訊儲存在相當於的表格中 `/etc/nsswitch.conf` UNIX 系統上的檔案。

使用外部**DNS**伺服器設定**SVM**和資料**LIF**以進行主機名稱解析

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。。 `vserver services name-service dns create` 如果只輸入一個 DNS 伺服器名稱、命令會發出警告。

關於這項工作

請參閱 設定動態DNS服務 如需在SVM上設定動態DNS的詳細資訊、

步驟

1. 在SVM上啟用DNS：

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

下列命令可啟用SVM VS1上的外部DNS伺服器：

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

ⓘ ° `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

如需與 DNS 相關的服務原則資訊、請參閱 "更新版本中的生命與服務政策ONTAP"。

設定名稱服務交換器表以進行主機名稱解析

您必須正確設定名稱服務交換器表、才能啟用ONTAP 支援功能、以參考本機或外部名稱服務來擷取主機資訊。

開始之前

您必須決定要在環境中使用哪種名稱服務來進行主機對應。

步驟

1. 將必要的項目新增至名稱服務交換器表：

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. 驗證名稱服務交換器表格是否包含所需順序的預期項目：

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

範例

以下範例修改名稱服務交換器表格中的項目、讓 SVM VS1 先使用本機主機檔案、然後使用外部 DNS 伺服器來解析主機名稱：

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

用於管理 **ONTAP Hosts** 表的 **ONTAP** 命令

叢集管理員可以新增、修改、刪除及檢視管理儲存虛擬機器（SVM）主機表中的主機名稱項目。SVM管理員只能為指派的SVM設定主機名稱項目。

用於管理本機主機名稱項目的命令

您可以使用 `vserver services name-service dns hosts` 建立、修改或刪除 DNS 主機表格項目的命令。

當您建立或修改DNS主機名稱項目時、可以指定多個以逗號分隔的別名位址。

如果您想要...	使用此命令...
建立DNS主機名稱項目	`vserver services name-service dns hosts create`
修改DNS主機名稱項目	`vserver services name-service dns hosts modify`
刪除DNS主機名稱項目	`vserver services name-service dns hosts delete`

如需命令的詳細資訊 `vserver services name-service dns hosts` ，請參閱 "指令參考資料ONTAP"。

保護您的網路安全

使用 **FIPS** 為所有 **SSL** 連線設定 **ONTAP** 網路安全性

ONTAP 的所有 SSL 連線均符合聯邦資訊處理標準 (FIPS) 140-2。您可以開啟和關閉 SSL FIPS 模式，全域設定 SSL 協議，並關閉ONTAP中的任何弱密碼。

根據預設， ONTAP 上的 SSL 設為停用 FIPS 相容性，並啟用下列 TLS 通訊協定：

- TLSv1.3 （從 ONTAP 9.11.1 開始）
- TLSv1.2

先前的 ONTAP 版本預設啟用下列 TLS 通訊協定：

- TLSv1.1 （從 ONTAP 9.12.1 開始預設為停用）
- TLSv1 （從 ONTAP 9.8 開始預設為停用）

啟用SSL FIPS模式時、ONTAP 從靜止到外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

如果您想要系統管理員帳戶使用SSH公開金鑰來存取SVM、則必須先確認主機金鑰演算法受到支援、才能啟用SSL FIPS模式。

附註： ONTAP 主機金鑰演算法支援已在更新版本的版本中變更。

發行版ONTAP	支援的金鑰類型	不支援的金鑰類型
9.11.1 及更新版本	ECDSA-SHA2-nistp256	RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	SSH-DSS SSH-RSA

沒有支援金鑰演算法的現有SSH公開金鑰帳戶、必須先以支援的金鑰類型重新設定、才能啟用FIPS、否則系統管理員驗證將會失敗。

如需詳細資訊、請參閱 "啟用SSH公開金鑰帳戶"。

ONTAP 9.18.1 引入了對 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法的支持，用於 SSL，從而為抵禦未來潛在的量子電腦攻擊提供了額外的安全保障。這些演算法僅在以下情況下可用FIPS 已停用。當 FIPS 被停用且對等方支援時，將協商後量子加密演算法。

啟用 **FIPS**

建議所有安全的使用者在系統安裝或升級之後、立即調整其安全組態。啟用SSL FIPS模式時、ONTAP 從靜止到外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

啟用FIPS時、您無法安裝或建立RSA金鑰長度為4096的憑證。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 啟用 FIPS ：

   ```
   security config modify * -is-fips-enabled true
   ```

3. 當系統提示您繼續時、請輸入 `y`

4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。

範例

如果您執行ONTAP 的是更新版本的版本、則不會看到警告訊息。

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

如"指令參考資料ONTAP"需有關及 SSL FIPS 模式組態的詳細 `security config modify`資訊，請參閱。

停用**FIPS**

從ONTAP 9.18.1 開始， ONTAP中的 SSL 支援 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法。只有在禁用 FIPS 且對等方支援這些演算法時，這些演算法才可用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令來停用FIPS：

   ```
   security config modify -is-fips-enabled false
   ```

3. 當系統提示您繼續時、請輸入 `y`。
4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動重新啟動叢集中的每個節點。

如果您需要使用 SSLv3 協議，則必須依照上述步驟停用 FIPS。只有在停用 FIPS 的情況下才能啟用 SSLv3。

您可以使用以下命令啟用 SSLv3。如果您執行的是ONTAP 9.9.1 或更高版本，則不會看到此警告訊息。

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

檢視**FIPS**法規遵循狀態

您可以查看整個叢集是否正在執行目前的安全性組態設定。

步驟

1. 如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。
2. 檢視目前的法規遵循狀態：

   `security config show`

   ```
   cluster1::> security config show
   Cluster    Supported
   FIPS Mode  Protocols Supported Cipher Suites
   ---------- ---------
   ------------------------------------------------------------
   false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
   TLS_RSA_WITH_AES_128_CCM_8,
              TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                        TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_RSA_WITH_AES_128_CBC_SHA256,
   TLS_RSA_WITH_AES_256_CCM,
                        TLS_RSA_WITH_AES_256_CCM_8,
                        ...
   ```

   如"指令參考資料ONTAP"需詳細 `security config show`資訊，請參閱。

相關資訊

- "FIPS 203：基於模組格的金鑰封裝機制標準（ML-KEM）"
- "FIPS 204：基於模組格的數位簽章標準（ML-DSA）"

- "FIPS 205：無狀態雜湊數位簽章標準 (SLH-DSA)"

設定 IPsec 在線上加密

準備在 ONTAP 網路上使用 IP 安全性

從 ONTAP 9 8 開始，您可以選擇使用 IP 安全性（ IPsec ）來保護網路流量。IPsec 是 ONTAP 提供的數種資料傳輸或傳輸中加密選項之一。在正式作業環境中使用 IPsec 之前，您應該做好設定的準備。

ONTAP 中的 IP 安全實作

IPsec 是由 IETF 維護的網際網路標準。它提供資料加密與完整性，以及 IP 層級網路端點之間流量傳輸的驗證。

使用 ONTAP 時， IPsec 可保護 ONTAP 和各種用戶端之間的所有 IP 流量，包括 NFS ， SMB 和 iSCSI 傳輸協定。除了隱私權和資料完整性之外，網路流量還能防範多種攻擊，例如重播和攔截式攻擊。ONTAP 使用 IPsec 傳輸模式實作。它利用網際網路金鑰交換（ IKE） 傳輸協定第 2 版，在 ONTAP 和使用 IPv4 或 IPv6 的用戶端之間協商金鑰資料。

當叢集上啟用 IPsec 功能時，網路需要 ONTAP 安全性原則資料庫（ SPD ）中的一或多個項目，才能符合各種流量特性。這些項目會對應至處理及傳送資料所需的特定保護詳細資料（例如密碼套件和驗證方法）。每個用戶端也需要對應的 SPD 項目。

對於某些類型的流量，最好使用另一個資料傳輸加密選項。例如，對於 NetApp SnapMirror 和叢集對等流量的加密，一般建議使用傳輸層安全性（ TLS ）傳輸協定，而非 IPsec 。這是因為 TLS 在大多數情況下都能提供更好的效能。

相關資訊

- "網際網路工程工作團隊"
- "RFC 4301-Security Architecture for the Internet Protocol （網際網路傳輸協定的安全架構）"

ONTAP IPsec 實作的演進

IPsec 最初是在ONTAP 9.8 中引入的。該實現在後續ONTAP版本中不斷發展，如下所述。

ONTAP 9.18.1

IPsec硬體卸載支援已擴展到IPv6流量。

ONTAP 9.17.1

IPsec 硬體卸載支援擴充至"鏈路聚合組" 。"後量子預共享密鑰（PPK）"支援 IPsec 預共用金鑰 (PSK) 驗證。

ONTAP 9.16.1.

加密和完整性檢查等多項密碼編譯作業可卸載至支援的 NIC 卡。如需詳細資訊、請參閱 IPsec 硬體卸載功能 。

ONTAP 9.12.1

MetroCluster IP 和 MetroCluster 網路附加組態提供 IPsec 前端主機傳輸協定支援。MetroCluster 叢集所提供的 IPsec 支援僅限於前端主機流量， MetroCluster 叢集間的生命體不受支援。

零點9.10.1 ONTAP

除了 PSK 之外，憑證還可用於 IPsec 驗證。在ONTAP 9.10.1 之前的版本中，僅支援使用 PSK 進行身份驗證。

部分**9.9.1 ONTAP**

IPsec 使用的加密演算法已通過 FIPS 140-2 驗證。這些演算法由 ONTAP 中的 NetApp 密碼編譯模組處理，該模組執行 FIPS 140-2 驗證。

部分**9.8 ONTAP**

根據傳輸模式實作， IPsec 的支援一開始就可用。

IPsec 硬體卸載功能

如果您使用的是 ONTAP 9 。 16.1 或更新版本，您可以選擇將某些運算密集的作業（例如加密和完整性檢查）卸載到儲存節點上安裝的網路介面控制器（ NIC ）卡。卸載到 NIC 卡的作業處理量約為 5% 或更低。這可大幅改善受 IPsec 保護的網路流量的效能和處理量。

要求與建議

在使用 IPsec 硬體卸載功能之前，您應該考量幾項需求。

支援的乙太網路卡

您只需安裝並使用受支援的乙太網路卡。從ONTAP 9.16.1 開始，支援以下乙太網路卡：

- X50131A （ 2p ， 40G/100g/200g/400G 乙太網路控制器）
- X60132A （ 4p ， 10G/25G 乙太網路控制器）

ONTAP 9.17.1 增加了對以下乙太網路卡的支援：

- X50135A（2p，40G/100G乙太網路控制器）
- X60135A（2p，40G/100G乙太網路控制器）

以下平台支援 X50131A 和 X50135A 卡：

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

以下平台支援 X60132A 和 X60135A 卡：

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

查看"NetApp Hardware Universe"有關支援的平台和卡片的更多資訊。

叢集範圍

IPsec 硬體卸載功能是針對叢集進行全域設定。例如，此命令會 `security ipsec config`套用至叢集中的所有節點。

一致的組態

支援的 NIC 卡應安裝在叢集中的所有節點上。如果支援的 NIC 卡只能在某些節點上使用，則當容錯移轉後，如果部分生命負載未裝載於具有卸載功能的 NIC 上，您就會發現效能大幅降低。

停用反重播

您必須停用 ONTAP （預設組態）和 IPsec 用戶端上的 IPsec 反重新執行保護。如果未停用，將不支援分割和多重路徑（備援路由）。

如果 ONTAP IPsec 組態已從預設變更為啟用反重新執行保護，請使用此命令將其停用：

```
security ipsec config modify -replay-window 0
```

您必須確定用戶端上的 IPsec 反重新執行保護已停用。請參閱用戶端的 IPsec 文件，以停用反重播保護。

限制

在使用 IPsec 硬體卸載功能之前，您應該考慮幾項限制。

IPv6

從ONTAP 9.18.1 開始，IPsec 硬體卸載功能支援 IPv6。在ONTAP 9.18.1 之前的版本中，IPsec 硬體卸載不支援 IPv6。

延伸序號

硬體卸載功能不支援 IPsec 延伸序列號。僅使用正常的 32 位元序列號。

連結集合體

從ONTAP 9.17.1 開始，您可以將 IPsec 硬體卸載功能與"鏈路聚合組" 。

在 9.17.1 之前的版本中，IPsec 硬體卸載功能不支援連結聚合。它不能與通過 `network port ifgrp` ONTAP CLI 中的指令。

ONTAP CLI 中的組態支援

ONTAP 9 。 16.1 中更新了三個現有的 CLI 命令，以支援以下所述的 IPsec 硬體卸載功能。如需詳細資訊，請參閱"在 ONTAP 中設定 IP 安全性"。

指令**ONTAP**	更新
`security ipsec config show`	布林參數 `Offload Enabled`顯示目前的 NIC 卸載狀態。
`security ipsec config modify`	此參數 `is-offload-enabled`可用於啟用或停用 NIC 卸載功能。
`security ipsec config show-ipsecsa`	新增了四個新的計數器，以位元組和封包顯示傳入和傳出流量。

ONTAP REST API 中的組態支援

ONTAP 9 中更新了兩個現有的 REST API 端點。 16.1 可支援 IPsec 硬體卸載功能，如下所述。

REST端點	更新
`/api/security/ipsec`	此參數 `offload_enabled`已新增，可透過修補方法使用。
`/api/security/ipsec/security_association`	新增兩個計數器值，以追蹤卸載功能處理的總位元組和封包數。

從 ONTAP 自動化文件中深入瞭解 ONTAP REST API ，包括 "ONTAP REST API 的新功能"。您也應該檢閱 ONTAP 自動化文件，以取得有關的詳細資訊 "IPsec 端點"。

相關資訊

- "安全 IPSEC"

設定 ONTAP 網路的 IP 安全性

在 ONTAP 叢集上設定及啟動 IPsec 進行中加密需要執行數項工作。

設定 IPsec 之前，請務必先檢閱"準備使用 IP 安全性"。例如，您可能需要決定是否使用以 ONTAP 9 開頭的可用 IPsec 硬體卸載功能。 16.1

在叢集上啟用IPsec

您可以在叢集上啟用 IPsec ，以確保資料在傳輸過程中持續加密且安全。

步驟

1. 探索是否已啟用IPsec：

   ```
   security ipsec config show
   ```

   如果結果包括 `IPsec Enabled: false`，繼續下一步。

2. 啟用IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

   您可以使用布爾參數來啟用 IPsec 硬體卸載功能 `is-offload-enabled`。

3. 再次執行探索命令：

   ```
   security ipsec config show
   ```

   現在的結果包括 `IPsec Enabled: true`。

準備使用憑證驗證建立 IPsec 原則

如果您只使用預先共用金鑰（ PSK ）進行驗證、而且不會使用憑證驗證、則可以略過此步驟。

在建立使用憑證進行驗證的 IPsec 原則之前、您必須確認符合下列先決條件：

- ONTAP 和用戶端都必須安裝另一方的 CA 憑證、以便雙方可驗證終端實體（ ONTAP 或用戶端）憑證
- 系統會為ONTAP 參與該原則的Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the

> 可共享證書的產品。ONTAP不需要在憑證與lifs之間建立一對一對應關係。

步驟

1. 除非已安裝 ONTAP 憑證管理（例如 ONTAP 自我簽署的根 CA ）、否則請將在相互驗證期間使用的所有 CA 憑證（包括 ONTAP 端和用戶端 CA ）安裝到憑證管理。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. 若要確保在驗證期間安裝的 CA 位於 IPsec CA 搜尋路徑內、請使用將 ONTAP 憑證管理 CA 新增至 IPsec 模組 `security ipsec ca-certificate add` 命令。
   - 命令範例 *
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. 建立並安裝認證以供ONTAP 《Sfor the Suse LIF（供《Sfor the Suse：此憑證的發卡行CA必須已安裝ONTAP 至ESA並新增至IPsec。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

如需ONTAP 更多有關資訊、請參閱ONTAP 《》介紹文件中的安全認證命令。

定義安全性原則資料庫（**SPD**）

在允許流量在網路上傳輸之前、IPsec需要SPD項目。無論您使用的是用於驗證的PSK或憑證、都是如此。

步驟

1. 使用 `security ipsec policy create` 命令至：
   a. 選取ONTAP 要參與IPsec傳輸的IP位址或子網路。
   b. 選取要連線ONTAP 至「靜態IP位址」的用戶端IP位址。

      > 用戶端必須使用預先共用金鑰（PSK）來支援網際網路金鑰交換版本2（IKEv2）。

   c. 可選擇細粒度的流量參數，例如上層協定（UDP、TCP、ICMP 等）、本機連接埠號碼和遠端連接埠號，以保護流量。對應的參數如下 `protocols` ， `local-ports`和 `remote-ports`分別。

      跳過此步驟以保護ONTAP 所有介於整個過程中的資訊流量、例如：靜態IP位址和用戶端IP位址。保護所有流量是預設設定。

   d. 輸入的 PSK 或公開金鑰基礎架構（ PKI ） `auth-method` 所需驗證方法的參數。
      i. 如果您輸入一個 PSK 、請包含參數、然後按 <enter> 鍵提示您輸入並驗證預先共用金鑰。

`local-identity`如果主機和用戶端都使用強化天鵝，而且沒有為主機或用戶端選取萬用字元原則，則和 `remote-identity`參數是選用的。

ii. 如果您輸入 PKI 、也需要輸入 `cert-name`、 `local-identity`、 `remote-identity` 參數。如果遠端端憑證身分不明、或是需要多個用戶端身分識別、請輸入特殊身分識別 `ANYTHING`。

e. 從ONTAP 9.17.1 開始，可以選擇輸入後量子預共享金鑰 (PPK) 身份 `ppk-identity`參數。 PPK提供了額外的安全保障，以抵禦未來潛在的量子電腦攻擊。輸入 PPK 身分時，系統會提示您輸入 PPK 金鑰。PPK僅支援 PSK 身份驗證。

詳細了解 `security ipsec policy create`在"指令參考資料ONTAP" 。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

除非 ONTAP 和用戶端都設定了相符的 IPsec 原則、而且雙方都有驗證認證（可以是 PSK 或憑證）、否則 IP 流量無法在用戶端和伺服器之間傳輸。

使用**IPsec**身分識別

對於預先共用金鑰驗證方法、如果主機和用戶端都使用強化天鵝、而且沒有為主機或用戶端選取萬用字元原則、則本機和遠端身分識別是選用的。

對於公開密碼匙基礎建設/憑證驗證方法、本機和遠端身分識別都是必要的。身分識別會指定在每一方憑證中認證的身分識別、並用於驗證程序。如果遠端身分識別不明、或是可能有許多不同的身分識別、請使用特殊身分識別 `ANYTHING`。

關於這項工作

在不受限的情況下、可透過修改SPD項目或在SPD原則建立期間來指定身分識別。ONTAPSPD可以是IP位址或字串格式身分識別名稱。

步驟

1. 使用下列命令修改現有的 SPD 身分識別設定：

```
security ipsec policy modify
```

命令範例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsec多個用戶端組態

當少數用戶端需要使用IPsec時、每個用戶端只需使用一個SPD項目就足夠了。但是、當數百甚至數千個用戶端需要使用IPsec時、NetApp建議使用IPsec多重用戶端組態。

關於這項工作

支援將多個網路上的多個用戶端連線至單一SVM IP位址、並啟用IPsec。ONTAP您可以使用下列其中一種方法來達成此目的：

- 子網路組態

  若要允許特定子網路上的所有用戶端（例如 192.168.134.0/24 ）使用單一 SPD 原則項目連線到單一 SVM IP 位址、您必須指定 `remote-ip-subnets` 子網路形式。此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。

  > 在子網路組態中使用單一原則項目時、該子網路中的IPsec用戶端會共用IPsec身分識別和預先共用金鑰（PSK）。不過、憑證驗證並不符合此要求。使用憑證時、每個用戶端都可以使用自己的唯一憑證或共用憑證進行驗證。IPsec會根據安裝在本機信任存放區上的CA來檢查憑證的有效性。ONTAP支援憑證撤銷清單（CRL）檢查。ONTAP

- 允許所有用戶端組態

  若要允許任何用戶端連線至 SVM IPsec 啟用的 IP 位址、無論其來源 IP 位址為何、請使用 `0.0.0.0/0` 指定時使用萬用字元 `remote-ip-subnets` 欄位。

  此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。對於憑證驗證、您可以輸入 `ANYTHING`。

  此外、當 `0.0.0.0/0` 使用萬用字元時、您必須設定要使用的特定本機或遠端連接埠號碼。例如、 `NFS port 2049`。

  步驟

  a. 使用下列其中一個命令來設定多個用戶端的 IPsec 。

     i. 如果您使用 * 子網路組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     命令範例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. 如果您使用 * 允許所有用戶端組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

命令範例

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

顯示 IPsec 統計資料

透過協商、ONTAP 可在「穩定SVM IP位址」和「用戶端IP位址」之間建立稱為「IKE安全性關聯」（SA）的安全通道。兩個端點都安裝了IPsec SAS、以執行實際的資料加密與解密工作。您可以使用統計資料命令來檢查IPsec SAS和IKE SAS的狀態。

如果您使用 IPsec 硬體卸載功能，則會使用命令顯示數個新的計數器 `security ipsec config show-ipsecsa`。

命令範例

IKE SA命令範例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

相關資訊

- "安全性憑證安裝"
- "安全 IPSEC"

配置ONTAP後端集群網路加密

從ONTAP 9.18.1 開始，您可以為後端叢集網路上的傳輸中資料配置傳輸層安全性 (TLS) 加密。此加密技術可在後端叢集網路上的ONTAP節點之間傳輸客戶資料時，保護儲存在ONTAP中的客戶資料。

關於這項工作

- 後端集群網路加密預設為停用狀態。
- 啟用後端叢集網路加密後，儲存在ONTAP中的所有客戶資料在後端叢集網路上的ONTAP節點之間傳輸時都會被加密。集群網路的部分流量（例如控制路徑資料）未加密。
- 預設情況下，後端叢集網路加密將使用叢集中每個節點自動產生的憑證。你可以[管理集群網路加密證書]每個節點都使用自訂安裝的憑證。

開始之前

- 您必須是ONTAP管理員。 `admin`執行下列任務所需的權限等級。
- 叢集中的所有節點必須執行ONTAP 9.18.1 或更高版本才能啟用後端叢集網路加密。

啟用或停用叢集網路通訊加密

步驟

1. 查看目前集群網路加密狀態：

```
security cluster-network show
```

此命令顯示集群網路加密的目前狀態：

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. 啟用或停用TLS後端叢集網路加密：

```
security cluster-network modify -enabled <true|false>
```

此命令啟用或停用後端叢集網路上客戶傳輸資料的加密通訊。

管理集群網路加密證書

1. 查看目前集群網路加密證書資訊：

```
security cluster-network certificate show
```

此命令顯示目前集群網路加密證書資訊：

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

叢集中每個節點的憑證和憑證授權單位 (CA) 名稱均已顯示。

2. 修改節點的叢集網路加密證書：

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

此指令修改特定節點的叢集網路加密證書。在執行此命令之前，必須先安裝憑證並由已安裝的 CA 進行簽署。有關證書管理的更多信息，請參閱"使用系統管理員管理 ONTAP 憑證"。如果 `-name`如果未指定，則使用自動產生的預設憑證。

在 ONTAP 網路中設定生命安全的防火牆原則

設定防火牆可增強叢集的安全性、並有助於防止未獲授權的存取儲存系統。根據預設、內建防火牆會設定為允許遠端存取特定的IP服務集、以供資料、管理及叢集間生命體使用。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。

- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

防火牆原則可用來控制對管理服務傳輸協定的存取、例如SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH、DNS或SNMP。無法為NFS或SMB等資料傳輸協定設定防火牆原則。

您可以使用下列方式來管理防火牆服務和原則：

- 啟用或停用防火牆服務
- 顯示目前的防火牆服務組態
- 使用指定的原則名稱和網路服務建立新的防火牆原則
- 將防火牆原則套用至邏輯介面
- 建立新的防火牆原則、該原則是現有原則的確切複本

  您可以使用這項功能、在同一個SVM中建立具有類似特性的原則、或將原則複製到不同的SVM。

- 顯示防火牆原則的相關資訊
- 修改防火牆原則所使用的IP位址和網路遮罩
- 刪除LIF未使用的防火牆原則

防火牆原則與生命

LIF防火牆原則是用來限制透過每個LIF存取叢集。您需要瞭解預設防火牆原則如何影響每種LIF類型的系統存取、以及如何自訂防火牆原則以提高或降低LIF的安全性。

使用 OR `network interface modify` 命令設定 LIF 時 `network interface create`，為參數指定的值會決定允許存取 LIF 的 `-firewall-policy`服務傳輸協定和 IP 位址。如"指令參考資料ONTAP"需詳細 `network interface`資訊，請參閱。

在許多情況下、您可以接受預設的防火牆原則值。在其他情況下、您可能需要限制特定IP位址和特定管理服務傳輸協定的存取。可用的管理服務傳輸協定包括SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH, DNS及SNMP。

所有叢集生命的防火牆原則預設為 `""` 且無法修改。

下表說明在ONTAP 建立LIF時指派給每個LIF的預設防火牆原則、具體取決於其角色（版本號為9.5或更早）或服務原則ONTAP （版本為9.6及更新版本）：

防火牆原則	預設服務傳輸協定	預設存取	LIF套用至
管理	DNS、http、https、NDMP、ndmps、 NTP、SNMP、ssh	任何位址（0.00.0.0/0）	叢集管理、SVM管理及節點管理生命里

MGMT-NFS	DNS、http、https、NDMP、ndmps、 NTP、portmap、SNMP、ssh	任何位址（0.00.0.0/0）	也支援SVM管理存取的資料生命量
叢集間	HTTPS、NDMP、ndmps	任何位址（0.00.0.0/0）	所有叢集間LIF
資料	DNS、NDMP、ndms、portmap	任何位址（0.00.0.0/0）	所有資料生命量

portmap服務組態

portmap服務會將RPC服務對應至其接聽的連接埠。

Portmap服務可在ONTAP 不間斷的情況下於更新版本中使用、ONTAP 從版本9.4到ONTAP 版本9.6均可設定、並從ONTAP 版本9.7開始自動管理。

- 在更新版本的版本中、連接埠對應服務（rpcbind）一律可在連接埠111上存取、因為網路組態必須仰賴內建的不只是第三方防火牆的功能。ONTAP ONTAP
- 從S得9.4到S得9.6、您可以修改防火牆原則、以控制portmap服務是否可在特定的生命期中存取。ONTAP ONTAP
- 從功能更新至功能更新至功能更新至功能更新至功能更新至功能更新。ONTAP而是會自動為所有支援NFS服務的LIF開啟portmap連接埠。
- Portmap服務可在ONTAP 防火牆內設定、範圍從版本9.4到ONTAP 版本9.6。*

本主題的其餘部分將討論如何設定ONTAP 從版本ONTAP 號至版本號之間的適用效能提升介面防火牆服務。

視組態而定、您可能無法在特定類型的生命期（通常是管理生命期和叢集間生命期）上存取服務。在某些情況下、您甚至可能無法存取資料生命期。

您可以期望的行為

從版本9.4到版本9.6的功能設計、可在升級時提供無縫轉換。ONTAP ONTAP如果已透過特定類型的lifs存取portmap服務、則可透過這些類型的lifs繼續存取。如同在 ONTAP 9.3 及更早版本中、您可以在 LIF 類型的防火牆原則中指定可在防火牆內存取的服務。

叢集中的所有節點都必須執行ONTAP 從功能上到ONTAP 功能上的從功能上的資訊、才能使行為生效。只有傳入流量會受到影響。

新規則如下：

- 升級至9.4到9.6版時ONTAP 、根據預設或自訂、將portmap服務新增至所有現有的防火牆原則。
- 建立新叢集或新的IPspace時ONTAP 、不將portmap服務新增至預設資料原則、而只新增至預設管理或叢集間原則。
- 您可以視需要將portmap服務新增至預設或自訂原則、並視需要移除服務。

如何新增或移除**portmap**服務

若要將portmap服務新增至SVM或叢集防火牆原則（可在防火牆內存取）、請輸入：

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

若要從SVM或叢集防火牆原則中移除portmap服務（使其在防火牆內無法存取）、請輸入：

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

您可以使用網路介面modify命令、將防火牆原則套用至現有的LIF。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立防火牆原則並將其指派給 LIF

當您建立LIF時、預設的防火牆原則會指派給每個LIF。在許多情況下、預設的防火牆設定運作良好、您不需要變更這些設定。如果您想要變更可存取LIF的網路服務或IP位址、可以建立自訂防火牆原則並將其指派給LIF。

關於這項工作

- 您無法使用建立防火牆原則 `policy` 名稱 `data`、 `intercluster`、 `cluster`或 `mgmt`。

  這些值保留給系統定義的防火牆原則。

- 您無法設定或修改叢集I生命 的防火牆原則。

  所有服務類型的叢集LIF防火牆原則都設為0.00.0.0/0。

- 如果您需要從原則中移除服務、則必須刪除現有的防火牆原則並建立新原則。
- 如果叢集上已啟用IPv6、您可以使用IPv6位址建立防火牆原則。

  啟用 IPv6 之後、 `data`、 `intercluster`和 `mgmt` 防火牆原則包括： /0 （ IPv6 萬用字元）在其接受的位址清單中。

- 使用System Manager設定跨叢集的資料保護功能時、您必須確保叢集間LIF IP位址包含在允許的清單中、而且叢集間LIF和公司擁有的防火牆都允許HTTPS服務。

  依預設 `intercluster` 防火牆原則允許從所有 IP 位址（ 0.0.0/0 或： /0 （ IPv6 ））存取、並啟用 HTTPS 、 NDMP 和 NDMPS 服務。如果您修改此預設原則、或是為叢集間LIF建立自己的防火牆原則、則必須將每個叢集間LIF IP位址新增至允許的清單、並啟用HTTPS服務。

- 從支援SJS9.6開始ONTAP 、不支援HTTPS和SSH防火牆服務。

  在 ONTAP 9.6 中 `management-https` 和 `management-ssh` LIF 服務可用於 HTTPS 和 SSH 管理存取。

步驟

1. 建立防火牆原則、讓特定SVM上的LIF可以使用：

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   您可以多次使用此命令、為防火牆原則中的每個服務新增多個網路服務和允許的IP位址清單。

2. 使用確認原則已正確新增 `system services firewall policy show` 命令。

3. 將防火牆原則套用至LIF：

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. 使用確認原則已正確新增至 LIF `network interface show -fields firewall-policy` 命令。

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

建立防火牆原則並將其指派給 **LIF** 的範例

下列命令會建立名為data_http的防火牆原則、以啟用從10.10子網路IP位址存取HTTP和HTTPS傳輸協定、將該原則套用至SVM VS1上名為data1的LIF、然後顯示叢集上的所有防火牆原則：

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

管理防火牆服務和原則的 ONTAP 命令

您可以使用 `system services firewall` 管理防火牆服務的命令 `system services firewall policy` 管理防火牆原則的命令、以及 `network interface modify` 管理生命的防火牆設定的命令。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。
- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

如果您想要...	使用此命令...
啟用或停用防火牆服務	`system services firewall modify`
顯示目前的防火牆服務組態	`system services firewall show`
建立防火牆原則或新增服務至現有的防火牆原則	`system services firewall policy create`
將防火牆原則套用至LIF	`network interface modify -lif lifname -firewall-policy`
修改與防火牆原則相關的IP位址和網路遮罩	`system services firewall policy modify`
顯示防火牆原則的相關資訊	`system services firewall policy show`
建立一個新的防火牆原則、該原則是現有原則的確切複本	`system services firewall policy clone`
刪除LIF未使用的防火牆原則	`system services firewall policy delete`

相關資訊

- "系統服務防火牆"
- "修改網路介面"

QoS 標記（僅限叢集管理員）

瞭解 ONTAP 網路服務品質（ QoS ）

網路服務品質（ QoS ）標記可協助您根據網路狀況，排列不同流量類型的優先順序，以有效使用網路資源。您可以針對每個IPspace所支援的流量類型、設定傳出IP封包的差異化服務程式碼點（Dscp）值。

針對**UC**法規遵循的**DSCP**標示

您可以使用預設或使用者提供的Dscp程式碼、在特定傳輸協定的傳出（出口）IP封包流量上啟用差異化服務程式碼點（Dscp）標記。DSCP標示是一種分類及管理網路流量的機制、也是統一化功能（UC）法規遵循的一項元件。

提供IPspace、傳輸協定及dscp值、即可啟用dscp標記（也稱為_qos標記_或_服務品質標記_）。可套用DSCP標示的傳輸協定為NFS、SMB、iSCSI、SnapMirror、NDMP、 FTP、HTTP/HTTPS、SSH、遠端登入和SNMP。

如果您在啟用指定傳輸協定的dscp標記時未提供dscp值、則會使用預設值：

- 資料傳輸協定/流量的預設值為0X0A（10）。
- 控制傳輸協定/流量的預設值為0x30（48）。

修改 ONTAP 網路 QoS 標記值

您可以針對每個IPspace修改不同傳輸協定的服務品質（QoS）標記值。

開始之前

叢集中的所有節點都必須執行相同版本ONTAP 的Sof the Sof。

步驟

使用修改 QoS 標記值 `network qos-marking modify` 命令。

- 。 `-ipspace` 參數指定要修改 QoS 標記項目的 IPspace 。
- 此 `–protocol`參數指定要修改 QoS 標記項目的通訊協定。
- 。 `-dscp` 參數指定差異化服務代碼點 (DSCP) 值。可能的值範圍從0到63。
- 。 `-is-enabled` 參數用於在提供的 IPspace 中啟用或停用指定傳輸協定的 QoS 標記 `-ipspace` 參數。

下列命令會在預設IPspace中啟用NFS傳輸協定的QoS標記：

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

下列命令會將預設IPspace中NFS傳輸協定的Dscp值設為20：

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

如"指令參考資料ONTAP"需更多關於 `network qos-marking modify`通訊協定的資訊和可能的值，請參閱。

檢視 ONTAP 網路 QoS 標記值

您可以針對每個IPspace顯示不同傳輸協定的QoS標記值。

步驟

使用顯示 QoS 標記值 `network qos-marking show` 命令。

下列命令會顯示預設IPspace中所有傳輸協定的QoS標記：

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `network qos-marking show`資訊，請參閱。

管理 SNMP （僅限叢集管理員）

瞭解 ONTAP 網路上的 SNMP

您可以設定SNMP來監控叢集中的SVM、以避免發生問題、並在問題確實發生時予以回應。管理SNMP包括設定SNMP使用者、以及為所有SNMP事件設定SNMP traphost目的地（管理工作站）。依預設、SNMP會在資料生命量上停用。

您可以在資料SVM中建立及管理唯讀SNMP使用者。資料生命期必須設定為在SVM上接收SNMP要求。

SNMP網路管理工作站（或管理程式）可以查詢SVM SNMP代理程式以取得資訊。SNMP代理程式會收集資訊並將其轉送給SNMP管理程式。SNMP代理程式也會在發生特定事件時產生設陷通知。SVM上的SNMP代理程式具有唯讀權限、無法用於任何設定作業或採取修正行動來回應陷阱。提供與SNMP v1、v2c和v3版本相容的SNMP代理程式。ONTAP使用密碼和加密技術、可提供進階的安全性。

如需ONTAP 更多有關支援SNMP的資訊、請參閱 "TR-4220：Data ONTAP 支援SNMP"。

MIB 總覽

mib（管理資訊庫）是描述SNMP物件和設陷的文字檔。

MIBs說明儲存系統管理資料的結構、並使用包含物件識別碼（OID）的階層式命名空間。每個oid都會識別可透過SNMP讀取的變數。

由於MIBs不是組態檔、ONTAP 而且無法讀取這些檔案、因此SNMP功能不受MIBs影響。提供下列的mib檔案：ONTAP

- NetApp 自訂 MIB (`netapp.mib`)

支援IPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）和ICMP（RFC 2466）MIBs（同時顯示IPv6和IPv6資料）ONTAP 。

ONTAP 也會在中的物件識別碼（ OID ）和物件簡短名稱之間提供簡短的交互參照 `traps.dat` 檔案：

> NetApp 支援網站上提供最新版本的 ONTAP MIB 和「traps.dat」檔案。不過、支援網站上的這些檔案版本不一定對應ONTAP 於您的版本的SNMP功能。這些檔案可協助您評估最新ONTAP 版的SNMP功能。

SNMP設陷

SNMP設陷會擷取系統監控資訊、這些資訊會以非同步通知的形式從SNMP代理程式傳送至SNMP管理程式。

SNMP設陷有三種類型：標準、內建及使用者定義。不支援ONTAP 使用者定義的陷阱。

陷阱可用於定期檢查在MIB中定義的操作臨界值或故障。如果達到臨界值或偵測到故障、SNMP代理程式會傳送訊息（設陷）給警示事件的traphosts。

> ONTAP 支援 SNMPv1 和 SNMPv3 設陷。不支援SNMP v2c擷取和通知。ONTAP

標準SNMP設陷

這些陷阱定義於RFC 1215。支援的五種標準SNMP設陷ONTAP ：冷啟動、暖啟動、連結、LinkUp和驗證失敗。

> 驗證失敗設陷預設為停用。您必須使用 `system snmp authtrap` 命令來啟用陷阱。如"指令參考資料ONTAP"需詳細 `system snmp authtrap`資訊，請參閱。

內建SNMP設陷

內建的設陷會預先定義在ONTAP 支援中、並在發生事件時自動傳送至traphost清單上的網路管理站台。這些陷阱（例如diskFailedShutdown, cpuTooBusy和volumeNearlyFull）是在自訂的mib中定義的。

每個內建陷阱都會以獨特的陷阱代碼來識別。

為 ONTAP 網路建立 SNMP 社群

使用SNMP v1和SNMP v2c時、您可以建立SNMP社群、做為管理站與儲存虛擬機器

（SVM）之間的驗證機制。

透過在資料 SVM 中建立 SNMP 社群、您可以執行命令、例如 `snmpwalk` 和 `snmpget` 資料生命。

關於這項工作

- 在全新安裝ONTAP 的功能中、預設會停用SNMPv1和SNMPv2c。

  在建立SNMP社群之後、會啟用SNMP v1和SNMP v2c。

- 支援唯讀社群。ONTAP
- 依預設、指派給資料生命期的「資料」防火牆原則會將 SNMP 服務設為 `deny`。

  您必須建立新的防火牆原則、並將 SNMP 服務設為 `allow` 為資料 SVM 建立 SNMP 使用者時。

  從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- 您可以為管理SVM和資料SVM的SNMP v1和SNMP v2c使用者建立SNMP社群。
- 由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 根 OID （ 1.3.6.1.4.1.789 ）、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

步驟

1. 使用建立 SNMP 社群 `system snmp community add` 命令。下列命令顯示如何在管理SVM叢集1中建立SNMP社群：

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   下列命令顯示如何在資料SVM VS1中建立SNMP社群：

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. 使用系統SNMP community show命令來驗證是否已建立社群。

   下列命令顯示為SNMP v1和SNMP v2c所建立的兩個社群：

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. 使用檢查是否允許 SNMP 作為「資料」防火牆原則中的服務 `system services firewall policy show` 命令。

下列命令顯示預設的「資料」防火牆原則不允許SNMP服務（僅「管理」防火牆原則允許SNMP服務）：

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. 建立允許使用存取的新防火牆原則 `snmp` 使用進行服務 `system services firewall policy create` 命令。

   下列命令會建立一個新的資料防火牆原則「 data1 」、允許使用 `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. 使用命令搭配 -firewall-policy 參數，將防火牆原則套用至資料 LIF `network interface modify`。

   下列命令會將新的「data1」防火牆原則指派給LIF「dataif1」：

   ```
   network interface modify -vserver vs1 -lif datalif1 -firewall-policy
   data1
   ```

   如"指令參考資料ONTAP"需詳細 `network interface modify`資訊，請參閱。

在 **ONTAP** 叢集中設定 **SNMPv3** 使用者

相較於SNMPv1和SNMPv2c、v3是一種安全的傳輸協定。若要使用v3、您必須設定一個v3使用者、以便從SNMP管理程式執行SNMP公用程式。

步驟

使用 `security login create`指令建立 SNMPv3 使用者。

系統會提示您提供下列資訊：

- 引擎ID：預設值和建議值為本機引擎ID
- 驗證傳輸協定
- 驗證密碼
- 隱私權傳輸協定
- 隱私權傳輸協定密碼

結果

v3使用者可以使用使用者名稱和密碼、從SNMP管理程式登入、然後執行SNMP公用程式命令。

v3安全參數

v3包含驗證功能、選取時會要求使用者在叫用命令時輸入名稱、驗證傳輸協定、驗證金鑰及其所需的安全層級。

下表列出了v3安全參數：

參數	命令列選項	說明
工程師ID	-e引擎ID	SNMP代理程式的引擎ID。預設值為本機引擎ID（建議使用）。
安全性名稱	-u名稱	使用者名稱不得超過32個字元。
驗證傳輸協定	-A｛NONE	md5

SHA	SHA-256}	驗證類型可以是「無」、「MD5」、「SHa」或「SHA-256」。
驗證金鑰	-A通關密碼	至少八個字元的通關密碼。
安全性層級	I {authNoPrimv	authPrimv
noauthNoPrimiv}	安全層級可以是驗證、無隱私權、驗證、隱私權或無驗證、 無隱私。	私有傳輸協定
-x {nONE	DE	AES128}
隱私權傳輸協定可以是無、DE或AES128	私有密碼	-X密碼

不同安全層級的範例

此範例顯示以不同安全性層級建立的 SNMPv3 使用者如何使用 SNMP 用戶端端指令、例如 `snmpwalk`，查詢叢集物件。

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

您必須使用 `snmpwalk` 5.3.1 或更新版本、當驗證傳輸協定為 SHA 時。

安全性層級：**authPrim**

下列輸出顯示使用驗證權限安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS模式

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全性層級：**authNoPrim**

下列輸出顯示使用驗證NoPrimiv安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS模式

FIPS 不允許您為隱私權傳輸協定選擇 * 無 * 。因此、無法在 FIPS 模式中設定驗證 NoPrimv SNMPv3 使用者。

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全性層級：**noAuthNoPrimiv**

下列輸出顯示使用noAuthNoPrimiv安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS模式

FIPS 不允許您為隱私權傳輸協定選擇 * 無 * 。

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

在 **ONTAP** 網路上設定用於 **SNMP** 的 **traphosts**

您可以將traphost（SNMP管理程式）設定為在叢集中產生SNMP設陷時接收通知（SNMP設陷PDU）。您可以指定SNMP traphost的主機名稱或IP位址（IPv4或IPv6）。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。

SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。
- 叢集上必須啟用IPv6、才能使用IPv6位址來設定SNMP traphosts。
- 建立 traphosts 時，您必須指定預先定義的使用者型安全模式（ USM ）驗證和隱私權認證。

步驟

新增SNMP traphost：

```
system snmp traphost add
```

只有當至少有一個SNMP管理站台指定為traphost時、才能傳送陷阱。

下列命令會以已知的USM使用者新增名為yyy.example.com的v3 traphost：

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

下列命令會使用主機的IPv6位址來新增traphost：

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

驗證 ONTAP 叢集中的 SNMP 輪詢

設定SNMP之後、您應該確認可以輪詢叢集。

關於這項工作

若要輪詢叢集、您需要使用第三方命令、例如 `snmpwalk`。

步驟

1. 傳送SNMP命令、從不同的叢集輪詢叢集。

   對於執行 SNMPv1 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

   在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

對於執行 SNMPv2c 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

對於執行 SNMPv3 的系統、請使用 CLI 命令 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

用於管理 **SNMP** ，設陷和 **traphosts** 的 **ONTAP** 命令

您可以使用 `system snmp` 用於管理 SNMP 、設陷和 traphosts 的命令。您可以使用 `security` 用於管理每個 SVM 的 SNMP 使用者的命令。您可以使用 `event` 管理與 SNMP 設陷相關事件的命令。

設定SNMP的命令

如果您想要...	使用此命令...
在叢集上啟用SNMP	`options -option-name snmp.enable -option-value on` SNMP服務必須符合管理（管理）防火牆原則。您可以使用系統服務防火牆原則show命令來驗證是否允許SNMP。
停用叢集上的SNMP	`options -option-name snmp.enable -option-value off`

用於管理SNMP v1、v2c和v3使用者的命令

如果您想要...	使用此命令...
設定SNMP使用者	`security login create`
顯示SNMP使用者	`security snmpusers`和 `security login show -application snmp`
刪除SNMP使用者	`security login delete`

修改SNMP使用者登入方法的存取控制角色名稱	`security login modify`

提供聯絡人和位置資訊的命令

如果您想要…	使用此命令…
顯示或修改叢集的聯絡詳細資料	`system snmp contact`
顯示或修改叢集的位置詳細資料	`system snmp location`

管理**SNMP**社群的命令

如果您想要…	使用此命令…
為SVM或叢集中的所有SVM新增唯讀（RO）社群	`system snmp community add`
刪除社群或所有社群	`system snmp community delete`
顯示所有社群的清單	`system snmp community show`

由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 根 OID （ 1.3.6.1.4.1.789 ）、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

用於顯示**SNMP**選項值的命令

如果您想要…	使用此命令…
顯示所有SNMP選項的目前值、包括叢集聯絡人、聯絡人位置、叢集是否設定為傳送陷阱、traphosts清單、以及社群和存取控制類型清單	`system snmp show`

用於管理**SNMP**陷阱和**traphosts**的命令

如果您想要…	使用此命令…
啟用從叢集傳送的SNMP設陷	`system snmp init -init 1`
停用從叢集傳送的SNMP設陷	`system snmp init -init 0`
新增接收叢集中特定事件SNMP通知的traphost	`system snmp traphost add`
刪除traphost	`system snmp traphost delete`
顯示traphosts清單	`system snmp traphost show`

用於管理與**SNMP**陷阱相關的事件的命令

如果您想要...	使用此命令...
顯示產生SNMP陷阱（內建）的事件	`event route show` 使用 `-snmp-support true` 僅檢視 SNMP 相關事件的參數。 使用 `instance -messagename <message>` 此參數可檢視事件發生原因的詳細說明、以及任何修正動作。 不支援將個別SNMP設陷事件路由傳送至特定的traphost目的地。所有SNMP設陷事件都會傳送至所有的traphost目的地。
顯示SNMP設陷記錄清單、這是已傳送至SNMP設陷的事件通知	`event snmphistory show`
刪除SNMP設陷歷程記錄	`event snmphistory delete`

相關資訊

- "系統 SNMP"
- "安全性"
- "安全性"
- "活動"
- "安全登入"

管理**SVM**中的路由

瞭解 **ONTAP** 網路上的 **SVM** 路由

SVM的路由表會決定SVM用來與目的地通訊的網路路徑。瞭解路由表的運作方式非常重要、如此一來、您就能在網路問題發生之前先行防範。

路由規則如下：

- 透過最具體的可用路由傳送流量。ONTAP
- 當無法使用更多特定路由時、透過預設閘道路由（網路遮罩為0位元）路由流量。ONTAP

如果路由具有相同目的地、網路遮罩和度量、則無法保證系統在重新開機或升級後會使用相同的路由。如果您已設定多個預設路由、這尤其會造成問題。

最佳做法是僅為 SVM 配置一個預設路由。為了避免中斷，您應該確保預設路由能夠到達任何無法透過更特定的路由到達的網路位址。有關詳細信息，請參閱"NetApp知識庫：SU134 - 叢集ONTAP中的路由配置不正確可能會導致網路存取中斷"

為 ONTAP 網路建立靜態路由

您可以在儲存虛擬機器（SVM）內建立靜態路由、以控制LIF如何將網路用於傳出流量。

當您建立與SVM相關聯的路由項目時、該路由會被指定SVM擁有且與閘道位於同一子網路的所有LIF使用。

步驟

使用 `network route create` 建立路由的命令。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

如"指令參考資料ONTAP"需詳細 `network route create`資訊，請參閱。

啟用 ONTAP 網路的多重路徑路由

如果多個路由的目的地度量相同、則只會針對傳出流量選取其中一個路由。這會導致其他路由未使用來傳送傳出流量。您可以啟用多重路徑路由、使所有可用路由的負載平衡、以符合其度量、而非 ECMP 路由、後者會在相同度量的可用路由之間平衡負載。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 啟用多重路徑路由：

   ```
   network options multipath-routing modify -is-enabled true
   ```

   叢集中的所有節點均已啟用多重路徑路由。

   ```
   network options multipath-routing modify -is-enabled true
   ```

   如"指令參考資料ONTAP"需詳細 `network options multipath-routing modify`資訊，請參閱。

從 ONTAP 網路刪除靜態路由

您可以從儲存虛擬機器（SVM）刪除不需要的靜態路由。

步驟

使用 `network route delete` 刪除靜態路由的命令。

下列範例會刪除與SVM vs0關聯的靜態路由、閘道為10.63.0.1、目的地IP位址為0.00.0/0：

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

如"指令參考資料ONTAP"需詳細 `network route delete`資訊，請參閱。

檢視 ONTAP 路由資訊

您可以顯示叢集上每個SVM的路由組態資訊。這有助於診斷與用戶端應用程式或服務之間的連線問題有關的路由問題、以及叢集中某個節點上的LIF。

步驟

1. 使用 `network route show` 顯示一或多個 SVM 內路由的命令。下列範例顯示在vs0 SVM中設定的路由：

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. 使用 `network route show-lifs` 顯示一或多個 SVM 內路由和生命的關聯的命令。

   以下範例顯示vs0 SVM擁有路由的lifs：

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   深入瞭解 `network route show`及 `network route show-lifs` "指令參考資料ONTAP"。

3. 使用 `network route active-entry show` 命令可在一個或多個節點、 SVM 、子網路或具有指定目的地的路由上顯示已安裝的路由。

   下列範例顯示特定SVM上所有已安裝的路由：

```
network route active-entry show -vserver Data0
```

```
Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `network route active-entry show`資訊，請參閱。

從 ONTAP 網路的路由表中移除動態路由

收到針對IPv6和IPv6的ICMP重新導向時、動態路由會新增至路由表。根據預設、動態路由會在300秒後移除。如果您想要在不同時間內維持動態路由、可以變更逾時值。

關於這項工作

您可以將逾時值從0設定為65,535秒。如果您將值設為0、則路由永遠不會過期。移除動態路由可避免因無效路由持續存在而導致連線中斷。

步驟

1. 顯示目前的逾時值。
   - 對於IPV4：

     ```
     network tuning icmp show
     ```

   - 對於IPv6：

     ```
     network tuning icmp6 show
     ```

2. 修改逾時值。
   - 對於IPV4：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - 對於IPv6：

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. 確認逾時值已正確修改。
   - 對於IPV4：

     ```
     network tuning icmp show
     ```

   - 對於IPv6：

```
network tuning icmp6 show
```

如"指令參考資料ONTAP"需詳細 `network tuning icmp`資訊，請參閱。

ONTAP 網路資訊

檢視 ONTAP 網路資訊

使用 CLI 、您可以檢視與連接埠、生命、路由、容錯移轉規則、容錯移轉群組、 防火牆規則、 DNS 、 NIS 和連線。從 ONTAP 9.8 開始、您也可以下載 System Manager 中顯示的網路相關資料。

此資訊在重新設定網路設定或疑難排解叢集等情況下非常實用。

如果您是叢集管理員、可以檢視所有可用的網路資訊。如果您是SVM管理員、則只能檢視與您指派的SVM相關的資訊。

在 System Manager 中、當您在 *List View* 中顯示資訊時、您可以按一下 * 下載 * 、並下載顯示的物件清單。

- 此清單會以「以逗號分隔的值（CSV）」格式下載。
- 只會下載可見欄中的資料。
- CSV檔案名稱的格式為物件名稱和時間戳記。

檢視 ONTAP 網路連接埠資訊

您可以顯示有關特定連接埠或叢集中所有節點上所有連接埠的資訊。

關於這項工作

將顯示下列資訊：

- 節點名稱
- 連接埠名稱
- IPSpace名稱
- 廣播網域名稱
- 連結狀態（向上或向下）
- MTU設定
- 連接埠速度設定與作業狀態（每秒1 Gb或10 Gb）
- 自動交涉設定（true或假）
- 雙工模式和作業狀態（半雙工或全雙工）
- 連接埠的介面群組（若適用）
- 連接埠的VLAN標記資訊（若適用）

- 連接埠的健全狀況（健全狀況或降級）
- 連接埠標記為降級的原因

如果欄位的資料無法使用（例如、非作用中連接埠的作業雙工和速度將無法使用）、欄位值會列為 -。

步驟

使用顯示網路連接埠資訊 `network port show` 命令。

您可以透過指定來顯示每個連接埠的詳細資訊 `-instance` 或使用指定欄位名稱來取得特定資訊 `-fields` 參數。

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

檢視 ONTAP VLAN 資訊

您可以顯示有關特定VLAN或叢集中所有VLAN的資訊。

關於這項工作

您可以透過指定來顯示每個 VLAN 的詳細資訊 `-instance` 參數。您可以使用指定欄位名稱來顯示特定資訊

`-fields` 參數。

步驟

使用顯示有關 VLAN 的資訊 `network port vlan show` 命令。下列命令會顯示叢集中所有VLAN的相關資訊：

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

如"指令參考資料ONTAP"需詳細 `network port vlan show`資訊，請參閱。

檢視 ONTAP 介面群組資訊

您可以顯示介面群組的相關資訊、以判斷其組態。

關於這項工作

將顯示下列資訊：

- 介面群組所在的節點
- 介面群組中包含的網路連接埠清單
- 介面群組名稱
- 發佈功能（MAC、IP、連接埠或連續）
- 介面群組的媒體存取控制（MAC）位址
- 連接埠活動狀態；也就是所有彙總連接埠都處於作用中狀態（完全參與）、某些連接埠為作用中狀態（部分參與）、或無作用中狀態

步驟

使用顯示介面群組的相關資訊 `network port ifgrp show` 命令。

您可以透過指定來顯示每個節點的詳細資訊 `-instance` 參數。您可以使用指定欄位名稱來顯示特定資訊 `-fields` 參數。

下列命令會顯示叢集中所有介面群組的相關資訊：

```
network port ifgrp show
          Port     Distribution                    Active
Node      IfGrp    Function     MAC Address        Ports   Ports
--------- -------- ------------ -----------------  ------- --------
cluster-1-01
          a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
          a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
          a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
          a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

下列命令會顯示單一節點的詳細介面群組資訊：

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

如"指令參考資料ONTAP"需詳細 `network port ifgrp show`資訊，請參閱。

檢視 ONTAP LIF 資訊

您可以檢視LIF的詳細資訊、以判斷其組態。

您也可能想要檢視此資訊來診斷基本的LIF問題、例如檢查是否有重複的IP位址、或驗證網路連接埠是否屬於正確的子網路。儲存虛擬機器（SVM）管理員只能檢視與SVM相關聯的LIF資訊。

關於這項工作

將顯示下列資訊：

- 與LIF相關的IP位址
- LIF的管理狀態
- LIF的作業狀態

資料生命體的作業狀態取決於資料生命體相關聯的SVM狀態。當SVM停止時、LIF的作業狀態會變更為「關閉」。當SVM再次啟動時、作業狀態會變更為up

- 節點和LIF所在的連接埠

如果欄位的資料無法使用（例如、如果沒有擴充狀態資訊）、欄位值會列為 –。

步驟

使用命令顯示 LIF 資訊 `network interface show`。

您可以指定-instance參數來檢視每個LIF的詳細資訊、或使用-fields參數指定欄位名稱來取得特定資訊。

下列命令會顯示叢集中所有LIF的一般資訊：

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

下列命令顯示單一LIF的詳細資訊：

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                  Data Protocol: nfs,cifs
                      Home Node: node-01
                      Home Port: e0c
                   Current Node: node-03
                   Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                  IPv4 Link Local: -
                      Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

檢視 ONTAP 網路的路由資訊

您可以顯示SVM內的路由資訊。

步驟

視您要檢視的路由資訊類型而定、輸入適當的命令：

若要檢視有關...的資訊	輸入...
靜態路由（每SVM）	`network route show`

每個路由上的LIF（每個SVM）	`network route show-lifs`

您可以透過指定來顯示每個航線的詳細資訊 `-instance` 參數。下列命令會顯示叢集1中SVM內的靜態路由：

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

下列命令會顯示叢集1中所有SVM的靜態路由和邏輯介面（lifs）關聯：

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------

0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

深入瞭解 `network route show`及 `network route show-lifs` "指令參考資料ONTAP"。

檢視 **ONTAP DNS** 主機表格項目

DNS主機表項目會將主機名稱對應至IP位址。您可以針對叢集中的所有SVM顯示主機名稱和別名、以及它們對應的IP位址。

步驟

使用vserver services name-service DNS hosts show命令顯示所有SVM的主機名稱項目。

下列範例顯示主機表格項目：

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

檢視 **ONTAP DNS** 網域組態資訊

您可以在叢集中顯示一或多個儲存虛擬機器（SVM）的DNS網域組態、以驗證其設定是否正確。

步驟

使用檢視 DNS 網域組態 `vserver services name-service dns show` 命令。

下列命令會顯示叢集中所有SVM的DNS組態：

```
vserver services name-service dns show
                                                    Name
Vserver         State     Domains                   Servers
--------------- --------- ------------------------- -------------
cluster-1        enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs1             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs2             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs3             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
```

下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

檢視 ONTAP 容錯移轉群組資訊

您可以檢視容錯移轉群組的相關資訊、包括每個容錯移轉群組中的節點和連接埠清單、是否啟用或停用容錯移轉、以及要套用至每個LIF的容錯移轉原則類型。

步驟

1. 使用顯示每個容錯移轉群組的目標連接埠 `network interface failover-groups show` 命令。

   下列命令會顯示雙節點叢集上所有容錯移轉群組的相關資訊：

```
network interface failover-groups show
                                 Failover
Vserver          Group           Targets
---------------  --------------  --------------------------------
Cluster
                 Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
vs1
                 Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
```

   如"指令參考資料ONTAP"需詳細 `network interface failover-groups show`資訊，請參閱。

2. 使用顯示特定容錯移轉群組的目標連接埠和廣播網域 `network interface failover-groups show` 命令。

   下列命令會顯示SVM VS4容錯移轉群組data12的詳細資訊：

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. 使用顯示所有生命所使用的容錯移轉設定 `network interface show` 命令。

   下列命令會顯示每個LIF所使用的容錯移轉原則和容錯移轉群組：

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -------------------  ---------------------  --------------
Cluster   cluster1-01_clus_1   local-only             Cluster
Cluster   cluster1-01_clus_2   local-only             Cluster
Cluster   cluster1-02_clus_1   local-only             Cluster
Cluster   cluster1-02_clus_2   local-only             Cluster
cluster1  cluster_mgmt         broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1    local-only             Default
cluster1  cluster1-02_mgmt1    local-only             Default
vs1       data1                disabled               Default
vs3       data2                system-defined         group2
```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

檢視 ONTAP LIF 容錯移轉目標

您可能必須檢查LIF的容錯移轉原則和容錯移轉群組是否設定正確。為了避免容錯移轉規則組態錯誤、您可以顯示單一LIF或所有LIF的容錯移轉目標。

關於這項工作

顯示LIF容錯移轉目標可讓您檢查下列項目：

- 是否使用正確的容錯移轉群組和容錯移轉原則來設定生命體
- 所產生的容錯移轉目標連接埠清單是否適用於每個LIF
- 資料LIF的容錯移轉目標是否不是管理連接埠（e0M）

步驟

使用顯示 LIF 的容錯移轉目標 `failover` 的選項 `network interface show` 命令。

下列命令會顯示雙節點叢集中所有LIF的容錯移轉目標相關資訊。。 `Failover Targets` 列顯示指定 LIF 的節點連接埠組合（優先順序）清單。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

檢視負載平衡區域中的 ONTAP 生命負載

您可以顯示屬於負載平衡區域的所有生命期、以驗證負載平衡區域是否設定正確。您也可

以檢視特定LIF的負載平衡區域、或檢視所有LIF的負載平衡區域。

步驟

使用下列其中一項命令、顯示所需的生命量與負載平衡詳細資料

若要顯示...	輸入...
特定負載平衡區域中的LIF	`network interface show -dns-zone zone_name` `zone_name` 指定負載平衡區域的名稱。
特定LIF的負載平衡區域	`network interface show -lif lif_name -fields dns-zone`
所有生命區的負載平衡區域	`network interface show -fields dns-zone`

顯示**lifs**負載平衡區域的範例

下列命令會顯示SVM vs0之負載平衡區域storage.company.com中所有LIF的詳細資料：

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

下列命令會顯示LIF資料3的DNS區域詳細資料：

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

下列命令會顯示叢集中所有LIF及其對應DNS區域的清單：

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

檢視 ONTAP 叢集連線

您可以依用戶端、邏輯介面、傳輸協定或服務、顯示叢集中的所有作用中連線、或節點上的作用中連線數。您也可以顯示叢集中的所有聆聽連線。

依用戶端顯示作用中連線（僅限叢集管理員）

您可以檢視用戶端的作用中連線、以驗證特定用戶端所使用的節點、並檢視每個節點的用戶端計數之間可能存在的不平衡。

關於這項工作

用戶端的作用中連線數在下列案例中很有用：

- 尋找忙碌或過載的節點。
- 判斷特定用戶端存取磁碟區的速度緩慢的原因。

  您可以檢視用戶端正在存取之節點的詳細資料、然後將其與磁碟區所在的節點進行比較。如果存取磁碟區需要周遊叢集網路、用戶端可能會因為遠端存取超額訂閱的遠端節點上的磁碟區而遇到效能降低的問題。

- 驗證是否所有節點都能用於資料存取。
- 尋找連線數量異常高的用戶端。
- 驗證特定用戶端是否有連線至節點。

步驟

使用顯示節點上用戶端的作用中連線計數 `network connections active show-clients` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-clients`資訊，請參閱。

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

依傳輸協定顯示作用中連線（僅限叢集管理員）

您可以依節點上的傳輸協定（TCP或udp）顯示作用中連線的計數、以比較叢集內的傳輸協定使用量。

關於這項工作

依傳輸協定的作用中連線數在下列案例中很有用：

- 尋找正在失去連線的udp用戶端。

  如果某個節點接近其連線限制、則會先捨棄UDP用戶端。

- 驗證是否未使用其他通訊協定。

步驟

使用在節點上依通訊協定顯示作用中連線的計數 `network connections active show-protocols` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-protocols`資訊，請參閱。

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

依服務顯示作用中連線（僅限叢集管理員）

您可以針對叢集中的每個節點、依服務類型（例如NFS、SMB、掛載等）顯示作用中連線的計數。這對於比較叢集內的服務使用量很有用、因為這有助於判斷節點的主要工作負載。

關於這項工作

依服務列出的作用中連線數在下列案例中非常實用：

- 驗證所有節點是否用於適當的服務、以及該服務的負載平衡是否正常運作。
- 驗證是否未使用其他服務。使用顯示節點上依服務顯示作用中連線的計數 `network connections active show-services` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-services`資訊，請參閱。

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

在節點和**SVM**上顯示**LIF**的作用中連線

您可以依節點和儲存虛擬機器（SVM）顯示每個LIF的作用中連線數、以檢視叢集內LIF之間的連線不平衡。

關於這項工作

LIF的作用中連線數在下列案例中很有用：

- 比較每個LIF上的連線數目、找出過載的LIF。
- 驗證DNS負載平衡是否適用於所有資料LIF。
- 比較不同SVM的連線數目、找出使用最多的SVM。

步驟

使用顯示 SVM 和節點每個 LIF 的作用中連線計數 `network connections active show-lifs` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-lifs`資訊，請參閱。

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

顯示叢集中的作用中連線

您可以顯示叢集中作用中連線的相關資訊、以檢視個別連線所使用的LIF、連接埠、遠端主機、服務、儲存虛擬機器（SVM）和傳輸協定。

關於這項工作

在下列情況下、檢視叢集中的作用中連線十分有用：

- 驗證個別用戶端是否在正確的節點上使用正確的傳輸協定和服務。
- 如果用戶端無法使用特定的節點、傳輸協定和服務組合來存取資料、您可以使用此命令來尋找類似的用戶端來進行組態或封包追蹤比較。

步驟

使用顯示叢集中的作用中連線 `network connections active show` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show`資訊，請參閱。

下列命令顯示節點節點節點1上的作用中連線：

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

下列命令顯示SVM VS1上的作用中連線：

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

顯示叢集中的接聽連線

您可以顯示叢集中偵聽連線的相關資訊、以檢視接受特定傳輸協定和服務連線的生命與連接埠。

關於這項工作

檢視叢集中的聆聽連線在下列情況下非常有用：

- 如果與LIF的用戶端連線持續失敗、請確認所需的傳輸協定或服務正在聆聽LIF。
- 如果透過另一個節點上的LIF遠端資料存取某個節點上的磁碟區失敗、請驗證是否在每個叢集LIF上開啟UP/rclipcp接聽程式。
- 如果SnapMirror在同一叢集中的兩個節點之間傳輸失敗、請驗證是否在每個叢集LIF上開啟UP/rclipcp接聽程式。
- 如果SnapMirror在不同叢集的兩個節點之間傳輸失敗、請驗證是否在每個叢集間的LIF上開啟了TCP/IP接聽程式。

步驟

使用顯示每個節點的聆聽連線 `network connections listening show` 命令。

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

如"指令參考資料ONTAP"需詳細 `network connections listening show`資訊，請參閱。

用於診斷網路問題的 **ONTAP** 命令

您可以使用命令來診斷網路上的問題、例如 `ping`, `traceroute`, `ndp`, 和 `tcpdump`。您也可以使用命令、例如 `ping6` 和 `traceroute6` 診斷 IPv6 問題。

如果您想要...	輸入此命令...
測試節點是否能連線到網路上的其他主機	`network ping`
測試節點是否能連線至IPv6網路上的其他主機	`network ping6`
追蹤將IPv4封包帶到網路節點的路由	`network traceroute`
追蹤IPv6封包通往網路節點的路由	`network traceroute6`
管理鄰近探索傳輸協定（NDP）	`network ndp`
顯示在指定網路介面或所有網路介面上接收和傳送的封包統計資料	`run -node` *`node_name`* `ifstat` * 附註 * ：此命令可從 nodesdesh 取得。
顯示從叢集中每個節點和連接埠探索到的鄰近裝置相關資訊、包括遠端裝置類型和裝置平台	`network device-discovery show`
檢視節點的CDP鄰近節點（ONTAP 僅支援CDPv1廣告）	`run -node` *`node_name`* `cdpd show-neighbors` * 附註 * ：此命令可從 nodesdesh 取得。

追蹤在網路中傳送和接收的封包	`network tcpdump start -node node-name -port port_name` * 附註 * ：此命令可從 nodesdesh 取得。
測量叢集間或叢集內節點之間的延遲和處理量	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` 如需詳細資訊、請參閱 "效能管理"。

相關資訊

- "指令參考資料ONTAP"
- "網路ping"
- "網路追蹤"
- "網路裝置探索秀"
- "網路 NDP"

檢視與鄰近探索通訊協定的網路連線

檢視 **ONTAP** 與鄰近探索通訊協定的網路連線能力

在資料中心中、您可以使用鄰近探索通訊協定來檢視實體或虛擬系統與其網路介面配對之間的網路連線。支援兩種鄰近探索傳輸協定：Cisco探索傳輸協定（CDP）和連結層探索傳輸協定（LLDP）ONTAP 。

鄰近探索傳輸協定可讓您自動探索及檢視網路中已直接連線之傳輸協定裝置的相關資訊。每個裝置都會通告識別、功能和連線資訊。此資訊會以乙太網路框架傳輸至多點傳送MAC位址、並由所有鄰近的啟用傳輸協定的裝置接收。

若要讓兩個裝置成為鄰近裝置、每個裝置都必須啟用並正確設定傳輸協定。探索傳輸協定功能僅限於直接連線的網路。鄰近設備可包括採用傳輸協定的裝置、例如交換器、路由器、橋接器等。支援兩種鄰近探索通訊協定、可個別或一起使用。ONTAP

- Cisco探索傳輸協定（CDP）*

CDP是Cisco Systems開發的專屬連結層傳輸協定。叢ONTAP 集連接埠的預設功能為啟用、但必須明確啟用資料連接埠。

連結層探索傳輸協定（**LLDP**）

LLDP是標準文件IEEE 802.1AB中指定的廠商中立傳輸協定。所有連接埠都必須明確啟用此功能。

使用CDP偵測網路連線能力、包括審查部署考量、在資料連接埠上啟用、檢視鄰近裝置、以及視需要調整CDP組態值。預設會在叢集連接埠上啟用CDP。

也必須在任何交換器和路由器上啟用CDP、才能顯示鄰近裝置的相關資訊。

發行版ONTAP	說明
9.10.1及更早版本	叢集交換器健全狀況監視器也會使用CDP來自動探索叢集和管理網路交換器。
9.11.1 及更新版本	叢集交換器健全狀況監視器也會使用CDP來自動探索叢集、儲存設備和管理網路交換器。

相關資訊

"系統管理"

使用**CDP**的考量事項

根據預設、符合CDP的裝置會傳送CDPv2通告。CDP相容的裝置僅在收到CDPv1廣告時才會傳送CDPv1廣告。僅支援CDPv1。ONTAP因此ONTAP 、當某個節點傳送CDPv1廣告時、符合CDP的鄰近裝置會傳回CDPv1廣告。

在節點上啟用CDP之前、您應該先考慮下列資訊：

- 所有連接埠均支援CDP。
- CDP通告由處於up狀態的連接埠傳送和接收。
- 必須在傳輸和接收裝置上啟用CDP、才能傳送和接收CDP通告。
- CDP通告會定期傳送、您可以設定時間間隔。
- 當LIF的IP位址變更時、節點會在下一個CDP通告中傳送更新的資訊。
- 更新版本：ONTAP
  - 叢集連接埠上一律會啟用CDP。
  - 預設會在所有非叢集連接埠上停用CDP。
- 更新版本：ONTAP
  - 叢集和儲存連接埠上一律會啟用CDP。
  - 預設會在所有非叢集和非儲存連接埠上停用CDP。

> 有時當節點上的生命區發生變更時、接收裝置端（例如交換器）的CDP資訊不會更新。如果遇到這樣的問題、您應該將節點的網路介面設定為停機狀態、然後再設定為UP狀態。

- CDP通告中只會通告IPv4位址。
- 對於具有VLAN的實體網路連接埠、會通告在該連接埠上VLAN上設定的所有生命體。
- 對於屬於介面群組一部分的實體連接埠、該介面群組上設定的所有IP位址都會在每個實體連接埠上通告。

- 對於裝載VLAN的介面群組、介面群組和VLAN上設定的所有生命體都會在每個網路連接埠上通告。
- 由於端口上的 CDP 封包限制為不超過 1500 位元組
  配置大量的生命流量時、相鄰交換器上只會報告這些 IP 位址的子集。

啟用或停用**CDP**

若要探索及傳送通告至符合CDP的鄰近裝置、必須在叢集的每個節點上啟用CDP。

根據預設ONTAP 、在支援的版本中、CDP會在節點的所有叢集連接埠上啟用、並在節點的所有非叢集連接埠上停用。

根據預設ONTAP 、在更新版本的版本中、CDP會在節點的所有叢集和儲存連接埠上啟用、並在節點的所有非叢集和非儲存連接埠上停用。

關於這項工作

。 `cdpd.enable` 選項可控制是否在節點的連接埠上啟用或停用 CDP ：

- 若為ONTAP 版本不含更新版本的版本、On可在非叢集連接埠上啟用CDP。
- 若為ONTAP 版本的版本、則on會在非叢集和非儲存連接埠上啟用CDP。
- 對於版本不含更新版本的版本、Off會停用非叢集連接埠上的CDP；您無法在叢集連接埠上停用CDP。ONTAP
- 針對版本的版本、Off會停用非叢集和非儲存連接埠上的CDP；您無法在叢集連接埠上停用CDP。ONTAP

如果在連接至CDP相容裝置的連接埠上停用CDP、則可能無法最佳化網路流量。

步驟

1. 顯示節點或叢集中所有節點的目前CDP設定：

若要檢視CDP設定…	輸入…
節點	`run - node <node_name> options cdpd.enable`
叢集中的所有節點	`options cdpd.enable`

2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上啟用或停用CDP：

若要啟用或停用CDP：	輸入…
節點	`run -node node_name options cdpd.enable {on or off}`
叢集中的所有節點	`options cdpd.enable {on or off}`

檢視**CDP**鄰近資訊

只要連接埠連接至符合CDP的裝置、即可檢視連接至叢集節點每個連接埠的鄰近裝置相關資訊。您可以使用 `network device-discovery show -protocol cdp`命令來檢視鄰近的資訊。如"指令參考資料ONTAP"需詳細 `network device-discovery show`資訊，請參閱。

關於這項工作

在版本更新的版本中、由於叢集連接埠一律啟用CDP、因此這些連接埠的CDP鄰近資訊一律會顯示。ONTAP必須在非叢集連接埠上啟用CDP、這些連接埠才會顯示鄰近資訊。

在版本更新的版本中、由於叢集和儲存連接埠一律啟用CDP、因此這些連接埠的CDP鄰近資訊一律會顯示。ONTAP必須在非叢集和非儲存連接埠上啟用CDP、這些連接埠才會顯示鄰近資訊。

步驟

顯示所有連接至叢集中節點上連接埠的CDP相容裝置相關資訊：

```
network device-discovery show -node node -protocol cdp
```

下列命令顯示連接至節點ST2650/212上連接埠的鄰近裝置：

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

輸出會列出連線至指定節點每個連接埠的Cisco裝置。

設定**CDP**訊息的保留時間

保留時間是指CDP通告儲存在鄰近CDP相容裝置快取中的期間。保留時間會在每個CDPv1封包中通告、並在節點收到CDPv1封包時更新。

- 的值 `cdpd.holdtime` 在 HA 配對的兩個節點上、選項應設為相同的值。
- 預設的保留時間值為180秒、但您可以輸入介於10秒到255秒之間的值。
- 如果在保留時間到期之前移除IP位址、則CDP資訊會快取、直到保留時間過期為止。

步驟

1. 顯示節點或叢集中所有節點的目前CDP保留時間：

若要檢視保留時間...	輸入...
節點	`run -node node_name options cdpd.holdtime`
叢集中的所有節點	`options cdpd.holdtime`

2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上設定CDP保留時間：

若要設定保留時間...	輸入...
節點	`run -node node_name options cdpd.holdtime holdtime`
叢集中的所有節點	`options cdpd.holdtime holdtime`

設定傳送**CDP**通告的時間間隔

CDP通告會定期傳送給CDP鄰近裝置。視網路流量和網路拓撲的變更而定、您可以增加或減少傳送CDP通告的時間間隔。

- 的值 `cdpd.interval` 在 HA 配對的兩個節點上、選項應設為相同的值。
- 預設時間間隔為60秒、但您可以輸入5秒到900秒之間的值。

步驟

1. 顯示節點或叢集中所有節點的目前CDP通告時間間隔：

若要檢視時間間隔...	輸入...
節點	`run -node node_name options cdpd.interval`
叢集中的所有節點	`options cdpd.interval`

2. 針對節點的所有連接埠或叢集中所有節點的所有連接埠、設定傳送CDP通告的時間間隔：

若要設定時間間隔...	輸入...
節點	`run -node node_name options cdpd.interval interval`

叢集中的所有節點	`options cdpd.interval interval`

檢視或清除**CDP**統計資料

您可以檢視每個節點上叢集和非叢集連接埠的CDP統計資料、以偵測潛在的網路連線問題。CDP統計資料會從上次清除的時間開始累計。

關於這項工作

在《支援連結埠的CDP》（《支援端口的CDP）中、由於這些連接埠上的流量一律會顯示CDP統計資料。ONTAP必須在連接埠上啟用CDP、才能顯示這些連接埠的統計資料。

在《支援叢集與儲存連接埠的CDP（CDP）9.11.1及更新版本中、由於這些連接埠上的流量一律會顯示CDP統計資料。ONTAP必須在非叢集或非儲存連接埠上啟用CDP、才能顯示這些連接埠的統計資料。

步驟

顯示或清除節點上所有連接埠的目前CDP統計資料：

如果您想要...	輸入...
檢視CDP統計資料	`run -node node_name cdpd show-stats`
清除CDP統計資料	`run -node node_name cdpd zero-stats`

顯示及清除統計資料的範例

下列命令會在清除CDP統計資料之前顯示這些統計資料。輸出會顯示自上次清除統計資料以來、已傳送和接收的封包總數。

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

下列命令會清除CDP統計資料：

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:              0   | Csum Errors:         0   | Unsupported Vers:      0
 Invalid length:       0   | Malformed:           0   | Mem alloc fails:       0
 Missing TLVs:         0   | Cache overflow:      0   | Other errors:          0

TRANSMIT
 Packets:              0   | Xmit fails:          0   | No hostname:           0
 Packet truncated:     0   | Mem alloc fails:     0   | Other errors:          0

OTHER
 Init failures:        0
```

統計資料清除後、會在傳送或接收下一個CDP廣告之後開始累積。

連線至不支援 **CDP** 的乙太網路交換器

一些供應商的交換器不支援 CDP。查看"NetApp知識庫： ONTAP設備發現顯示節點而不是交換機"了解更多詳情。

有兩種方法可以解決此問題：

- 停用 CDP 並啟用 LLDP （如果支援）。請參閱 "使用 LLDP 來偵測網路連線" 以取得更多詳細資料。
- 在交換器上設定 MAC 位址封包篩選器、以捨棄 CDP 通告。

使用 **LLDP** 來偵測 **ONTAP** 網路連線

使用LLDP偵測網路連線能力包括審查部署考量、在所有連接埠上啟用、檢視鄰近裝置、以及視需要調整LLDP組態值。

在顯示鄰近裝置的相關資訊之前、也必須在任何交換器和路由器上啟用LLDP。

目前可報告下列類型長度值結構（TLV）ONTAP ：

- 機箱ID
- 連接埠ID
- 存留時間（TTL）
- 系統名稱

  系統名稱TLV不會傳送至CNA裝置。

某些整合式網路介面卡（CNA）、例如X1143介面卡和UTA2內建連接埠、包含LLDP的卸載支援：

- LLDP卸載用於資料中心橋接（DCB）。
- 叢集與交換器之間顯示的資訊可能有所不同。

  交換器所顯示的機箱ID和連接埠ID資料、可能與CNA和非CNA連接埠不同。

例如：

- 對於非CNA連接埠：
  - 機箱ID是節點上其中一個連接埠的固定MAC位址
  - 連接埠ID是節點上個別連接埠的連接埠名稱
- 對於CNA連接埠：
  - 機箱ID和連接埠ID是節點上個別連接埠的MAC位址。

不過、叢集所顯示的資料對於這些連接埠類型而言是一致的。

LLDP規格定義透過SNMP mib存取所收集的資訊。不過ONTAP 、目前不支援LLDP MIB.

啟用或停用 **LLDP**

若要探索及傳送通告給符合LLDP的鄰近裝置、必須在叢集的每個節點上啟用LLDP。從ONTAP 推出支援支援支援的支援方案開始、在節點的所有連接埠上預設都會啟用LLDP。

關於這項工作

對於 ONTAP 9.10.1 及更早版本、 `lldp.enable` 選項可控制是否在節點的連接埠上啟用或停用 LLDP ：

- `on` 在所有連接埠上啟用 LLDP 。
- `off` 停用所有連接埠上的 LLDP 。

對於 ONTAP 9.11.1 及更新版本、 `lldp.enable` 選項可控制在節點的非叢集和非儲存連接埠上啟用或停用 LLDP ：

- `on` 在所有非叢集和非儲存連接埠上啟用 LLDP 。
- `off` 在所有非叢集和非儲存連接埠上停用 LLDP 。

步驟

1. 顯示節點或叢集中所有節點的目前 LLDP 設定：
   - 單一節點： `run -node node_name options lldp.enable`
   - 所有節點：選項 `lldp.enable`
2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上啟用或停用 LLDP ：

若要在 … 上啟用或停用 LLDP	輸入…
節點	`run -node node_name options lldp.enable {on

off}`	叢集中的所有節點
`options lldp.enable {on	off}`

- 單一節點：

```
run -node node_name options lldp.enable {on|off}
```

- 所有節點：

```
options lldp.enable {on|off}
```

檢視 LLDP 鄰近區域資訊

只要連接埠連接至符合LLDP標準的裝置、即可檢視連接至叢集節點每個連接埠的鄰近裝置相關資訊。您可以使用network device-dinDiscovery show命令來檢視鄰近資訊。

步驟

1. 顯示所有與LLDP相容裝置連線至叢集中節點上之連接埠的相關資訊：

```
network device-discovery show -node node -protocol lldp
```

下列命令顯示連接至節點叢集-1_01上連接埠的鄰近節點。輸出會列出連線至指定節點每個連接埠的啟用LLDP的裝置。如果是 `-protocol` 省略選項、輸出也會列出啟用 CDP 的裝置。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

調整傳輸LLDP廣告的時間間隔

LLDP廣告會定期傳送給LLDP鄰近裝置。您可以根據網路流量和網路拓撲的變更、增加或減少傳送 LLDP 通告的時間間隔。

關於這項工作

IEEE建議的預設時間間隔為30秒、但您可以輸入5秒到300秒之間的值。

步驟

1. 顯示節點或叢集中所有節點目前的LLDP通告時間間隔：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - 所有節點：

     ```
     options lldp.xmit.interval
     ```

2. 調整為節點的所有連接埠或叢集中所有節點的所有連接埠傳送LLDP通告的時間間隔：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - 所有節點：

     ```
     options lldp.xmit.interval <interval>
     ```

調整**LLDP**廣告的即時時間值

存留時間（TTL）是LLDP廣告儲存在鄰近的LLDP相容裝置快取中的一段時間。TTL會在每個LLDP封包中通告、並在節點收到LLDP封包時進行更新。TTL可在傳出的LLDP框架中修改。

關於這項工作

- TTL 是計算值、即傳輸間隔的乘積 (`lldp.xmit.interval`）和保留倍數 (`lldp.xmit.hold`）再加上一項。
- 預設的保留倍數值為4、但您可以輸入1到100之間的值。
- 因此、根據IEEE的建議、預設TTL為121秒、但調整傳輸時間間隔並保留倍頻值、即可指定傳出訊框的值、從6秒到30001秒。
- 如果在TTL過期之前移除IP位址、則會快取LLDP資訊、直到TTL過期為止。

步驟

1. 顯示節點或叢集中所有節點的目前保留倍數值：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

◦ 所有節點：

```
options lldp.xmit.hold
```

2. 調整節點的所有連接埠或叢集中所有節點的所有連接埠上的保留倍頻值：
   ◦ 單一節點：

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

   ◦ 所有節點：

```
options lldp.xmit.hold <hold_value>
```

檢視或清除 **LLDP** 統計資料

您可以檢視每個節點上叢集和非叢集連接埠的 LLDP 統計資料、以偵測潛在的網路連線問題。LLDP 統計資料是從上次清除時開始累積的。

關於這項工作

對於版本9.10.1及更早版本、由於LLDP一律啟用叢集連接埠、因此會針對這些連接埠上的流量顯示LLDP統計資料。ONTAP必須在非叢集連接埠上啟用 LLDP 、這些連接埠的統計資料才會顯示出來。

對於版本僅9.11.1及更新版本、因為LLDP一律啟用叢集與儲存連接埠、因此會針對這些連接埠上的流量顯示LLDP統計資料。ONTAP必須在非叢集和非儲存連接埠上啟用LLDP、才能顯示這些連接埠的統計資料。

步驟

顯示或清除節點上所有連接埠的目前 LLDP 統計資料：

如果您想要...	輸入...
檢視 LLDP 統計資料	`run -node node_name lldp stats`
清除 LLDP 統計資料	`run -node node_name lldp stats -z`

顯示及清除統計資料範例

下列命令會在 LLDP 統計資料被清除之前顯示這些統計資料。輸出會顯示自上次清除統計資料以來、已傳送和接收的封包總數。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

下列命令會清除LLDP統計資料。

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

清除統計資料後、會在傳送或接收下一個LLDP廣告之後開始累積。