管理網路和安全
AFX

NetApp
February 11, 2026

目錄

管理網路和安全

管理 AFX 儲存系統叢集網絡

您需要配置 AFX 儲存系統的網路。網路環境支援多種場景，包括客戶端存取 SVM 上的資料和叢集間通訊。

建立網路資源是重要的第一步。您還需要根據需要執行其他管理操作，例如編輯或刪除網路定義。

建立廣播域

廣播域透過將屬於同一第二層網路的連接埠進行分組來簡化叢集網路的管理。然後可以為儲存虛擬機 (SVM) 分配群組中的端口，用於資料或管理流量。

集群設定期間會建立多個廣播域，包括：

預設

此廣播域包含「預設」IP空間中的連接埠。這些連接埠主要用於提供資料。還包括叢集管理和節點管理連接埠。

簇

此廣播域包含「集群」IP空間中的連接埠。這些連接埠用於集群通信，包括集群中所有節點的所有集群連接埠。

您可以在叢集初始化後建立其他廣播域。建立廣播網域時，將自動建立包含相同連接埠的故障轉移群組。

關於此任務

為廣播域定義的連接埠的最大傳輸單元 (MTU) 值將更新為廣播域中設定的 MTU 值。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*概覽*。
2. 在「廣播域」下，選擇 + Add 。
3. 提供廣播域的名稱或接受預設值。

   所有廣播網域在 IP 空間內必須是唯一的。

4. 提供最大傳輸單元（MTU）。

   MTU是廣播域內可接受的最大資料包。

5. 選擇所需的連接埠並選擇*儲存*。

建立 IP 空間

IP空間是IP位址和相關網路配置的管理域。這些空間可用於透過隔離管理和路由來支援您的 SVM。例如，當用戶端具有來自相同 IP 位址和子網路範圍的重疊 IP 位址時，它們很有用。

您必須先擁有一個 IP 空間，然後才能建立子網路。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*概覽*。
2. 在「IP 空間」下，選擇 + Add 。
3. 提供 IP 空間的名稱或接受預設值。

   所有 IP 空間名稱在叢集內必須是唯一的。

4. 選擇*儲存*。

下一步

您可以使用 IP 空間來建立子網路。

建立子網路

子網路或子網路強制對網路中的 IP 位址空間進行邏輯劃分。它使您能夠指派專用的 IP 位址區塊來建立網路介面 (LIF)。子網路允許您使用子網路名稱而不是特定的 IP 位址和網路遮罩組合，從而簡化了 LIF 的建立。

開始之前

您必須有一個廣播域和將定義子網路的 IP 空間。另請注意：

- 所有子網路名稱在特定 IP 空間內必須是唯一的。
- 子網路使用的 IP 位址範圍不能與其他子網路的 IP 位址重疊。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*概覽*。
2. 在「子網路」標籤下，選擇 + Add 。
3. 提供設定詳細信息，包括子網路名稱、IP 位址詳細資訊和廣播網域。
4. 選擇*儲存*。

下一步

新的子網路將簡化網路介面的建立。

建立網路介面

邏輯網路介面 (LIF) 由 IP 位址和相關網路設定參數組成。它可以與實體或邏輯連接埠相關聯，通常由客戶端用來存取 SVM 提供的資料。 LIF 在發生故障時提供彈性，並且可以在節點連接埠之間遷移，因此通訊不會中斷。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*概覽*。
2. 在「網路介面」標籤下，選擇 + Add 。
3. 提供配置詳細信息，包括介面名稱、介面類型、允許的協定和 IP 位址詳細資訊。
4. 選擇*儲存*。

相關資訊

- "管理 AFX 乙太網路端口"
- "了解ONTAP廣播域"
- "了解ONTAP IP 空間配置"
- "了解ONTAP網路的子網"
- "網路架構概述"

管理 AFX 儲存系統乙太網路連接埠

AFX 系統使用的連接埠為網路連接和通訊提供了基礎。有多種選項可用於客製化網路的第二層配置。

創建 VLAN

VLAN 由分組到廣播域的交換器連接埠組成。 VLAN 可讓您提高安全性、隔離潛在問題並限制 IP 網路基礎架構內的可用路徑。

開始之前

網路中部署的交換器必須符合 IEEE 802.1Q 標準或具有特定於供應商的 VLAN 實作。

關於此任務

請注意以下事項：

- 您無法在沒有任何成員連接埠的介面群組連接埠上建立 VLAN。
- 當您第一次在連接埠上設定 VLAN 時，連接埠可能會關閉，導致網路暫時中斷。後續向相同連接埠新增 VLAN 不會影響連接埠狀態。
- 您不應在網路介面上建立與交換器的本機 VLAN 具有相同識別碼的 VLAN。例如，如果網路介面 e0b 位於本機 VLAN 10 上，則不應在該介面上建立 VLAN e0b-10。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*乙太網路連接埠*。
2. 選擇 + VLAN。
3. 提供配置詳細信息，包括所需節點的 ID、廣播域和連接埠。

   VLAN 無法連接到託管叢集 LIF 的連接埠或指派給叢集 IP 空間的連接埠。

4. 選擇*儲存*。

結果

您已建立 VLAN 來提高安全性、隔離問題並限制 IP 網路基礎架構內的可用路徑。

創建 LAG

鏈路聚合組 (LAG) 是一種將多個實體網路連接組合成單一邏輯連接的技術。您可以使用它來增加頻寬並在節點

之間提供冗餘。

步驟

1. 在系統管理員中，選擇*網路*，然後選擇*乙太網路連接埠*。
2. 選擇*連結聚合組*。
3. 提供配置詳細信息，包括節點、廣播域、連接埠、模式和負載分佈。
4. 選擇*儲存*。

相關資訊

- "管理 AFX 群集網絡"
- "了解ONTAP網路連接埠配置"
- "組合實體連接埠以建立ONTAP介面組"

準備 AFX 儲存系統驗證服務

您需要準備AFX系統對使用者帳戶和角色定義的身份驗證和授權服務。

配置 LDAP

您可以設定輕量級目錄存取協定 (LDAP) 伺服器以在中心位置維護驗證資訊。

開始之前

您必須產生憑證簽署請求並新增 CA 簽署的伺服器數位憑證。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 選擇⚙在 **LDAP** 旁邊。
3. 選擇+ Add 並提供 LDAP 伺服器的名稱或 IP 位址。
4. 提供必要的配置信息，包括架構、基本 DN、端口和綁定。
5. 選擇*儲存*。

設定 SAML 身份驗證

安全性斷言標記語言 (SAML) 驗證使用戶能夠透過安全性身分提供者 (IdP) 而不是使用其他協定（如 LDAP）的提供者進行身份驗證。

開始之前

- 必須配置您計劃用於遠端身份驗證的身份提供者。有關配置詳細信息，請參閱提供者文件。
- 您必須擁有身分提供者的 URI。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。

2. 選擇⚙在 安全 下，**SAML** 驗證 旁。
3. 選擇*啟用 SAML 身份驗證*。
4. 提供 **IdP URL** 和 主機系統 IP 位址並選擇 儲存。

   確認視窗顯示元資料訊息，該資訊已自動複製到您的剪貼簿。

5. 導覽至您指定的 IdP 系統並從剪貼簿複製元資料以更新系統元資料。
6. 返回系統管理員中的確認視窗並選擇*我已使用主機 URI 或元資料配置了 IdP*。
7. 選擇*登出*以啟用基於 SAML 的身份驗證。

   IdP 系統將顯示身份驗證畫面。

相關資訊

- "管理 AFX 叢集使用者和角色"
- "為遠端ONTAP用戶設定 SAML 身份驗證"
- "身份驗證和存取控制"

管理 AFX 儲存系統叢集使用者和角色

您可以根據 AFX 提供的身份驗證和授權服務定義使用者帳戶和角色。

ⓘ 每個ONTAP用戶都需要分配一個角色。角色包括權限並決定使用者能夠執行的操作。

建立帳戶角色

當您的 AFX 叢集設定並初始化時，會自動建立叢集管理員和儲存 VM 管理員的角色。您可以建立其他使用者帳戶角色來定義指派了這些角色的使用者可以在您的叢集上執行的特定功能。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 在「安全」部分中，在「使用者和角色」旁邊，選擇→。
3. 在「角色」下，選擇 + Add 。
4. 提供角色的名稱和屬性。
5. 選擇*儲存*。

建立集群帳戶

您可以建立一個叢集級帳戶，以便在執行叢集或 SVM 管理時使用。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 在“安全”部分中，選擇→在*使用者和角色*旁邊。

3. 選擇 + Add . 在 用戶 下。
4. 輸入使用者名，然後選擇使用者的角色。

   該角色應該適合使用者。例如，**admin** 角色能夠在您的叢集上執行所有設定任務。

5. 選擇使用者登入方法和身份驗證方法；通常是*密碼*。
6. 輸入用戶的密碼。
7. 選擇*儲存*。

結果

已建立新帳戶並可供您的 AFX 叢集使用。

相關資訊

- "準備身份驗證服務"
- "額外的 AFX SVM 管理"

管理 AFX 儲存系統上的證書

根據您的環境，您需要在管理 AFX 的過程中建立和管理數位憑證。您可以執行幾個相關任務。

產生憑證簽署請求

要開始使用數位證書，您需要產生證書簽名請求 (CSR)。 CSR 用於從憑證授權單位 (CA) 要求簽署的憑證。作為此過程的一部分， ONTAP會建立公鑰/私鑰對並將公鑰包含在 CSR 中。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 在「安全」下，在「憑證」旁邊，選擇 →
3. 選擇 + Generate CSR 。
4. 提供主題的通用名稱和國家/地區；可選地提供組織和組織單位。
5. 若要變更定義憑證的預設值，請選擇 ↙↗ More options 並進行所需的更新。
6. 選擇*生成*。

結果

您已產生可用於請求公鑰憑證的 CSR。

新增受信任的憑證授權單位

ONTAP提供了一組預設的可信任根證書，可用於傳輸層安全性 (TLS) 和其他協定。您可以根據需要新增其他受信任的憑證授權單位。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 在「安全」下，在「憑證」旁邊，選擇 → 。
3. 選擇選項卡 受信任的憑證授權單位，然後選擇 + Add 。
4. 提供配置信息，包括名稱、範圍、通用名稱、類型和證書詳細信息；您可以透過選擇*導入*來導入證書。
5. 選擇“新增”。

結果

您已將受信任的憑證授權單位新增至您的 AFX 系統。

續訂或刪除受信任的憑證授權單位

受信任的憑證授權單位必須每年更新。如果您不想更新過期的證書，您應該將其刪除。

步驟

1. 選擇“集群”，然後選擇“設定”。
2. 在「安全」下，在「憑證」旁邊，選擇 → 。
3. 選擇選項卡「受信任的憑證授權單位」。
4. 選擇您想要續約或刪除的信任憑證授權單位。
5. 更新或刪除憑證授權單位。

若要更新憑證授權機構，請執行下列操作：	若要刪除憑證授權機構，請執行下列操作：
a. 選擇 ⋮ 然後選擇*續訂*。 b. 輸入或匯入憑證資訊並選擇*更新*。	a. 選擇 ⋮ 然後選擇*刪除*。 b. 確認您要刪除並選擇*刪除*。

結果

您已更新或刪除 AFX 系統上現有的受信任憑證授權單位。

新增客戶端/伺服器憑證或本機憑證授權單位

您可以新增用戶端/伺服器憑證或本機憑證授權單位作為啟用安全 Web 服務的一部分。

步驟

1. 在系統管理員中，選擇*集群*，然後選擇*設定*。
2. 在「安全」下，在「憑證」旁邊，選擇 → 。
3. 根據需要選擇*用戶端/伺服器憑證*或*本機憑證授權單位*。
4. 新增證書資訊並選擇*儲存*。

結果

您已為 AFX 系統新增了新的用戶端/伺服器憑證或本機權限。

續訂或刪除客戶端/伺服器憑證或本機憑證授權單位

客戶端/伺服器憑證和本地憑證授權單位必須每年更新。如果您不想更新過期的憑證或本機憑證授權機構，您應該刪除它們。

步驟

1. 選擇“集群”，然後選擇“設定”。
2. 在「安全」下，在「憑證」旁邊，選擇 →。
3. 根據需要選擇*用戶端/伺服器憑證*或*本機憑證授權單位*。
4. 選擇您要續約或刪除的憑證。
5. 更新或刪除憑證授權單位。

若要更新憑證授權機構，請執行下列操作：	若要刪除憑證授權機構，請執行下列操作：
a. 選擇⋮然後選擇*續訂*。 b. 輸入或匯入憑證資訊並選擇*更新*。	選擇⋮然後選擇*刪除*。

結果

您已更新或刪除 AFX 系統上現有的用戶端/伺服器憑證或本機憑證授權單位。

相關資訊

- "在ONTAP中產生並安裝由 CA 簽署的伺服器證書"
- "使用 System Manager 管理ONTAP證書"

版權資訊

商標資訊