事件、效能和健全狀況監控
ONTAP 9

NetApp
April 24, 2024

目錄

事件、效能和健全狀況監控

使用System Manager監控叢集效能

使用System Manager監控叢集效能

本節主題將說明如何在ONTAP 更新版本的更新版本中使用System Manager來管理叢集健全狀況和效能。

您可以在System Manager儀表板上檢視系統的相關資訊、以監控叢集效能。儀表板會顯示重要警示和通知、儲存層和磁碟區的效率和容量、叢集中可用的節點、HA配對中節點的狀態、最活躍的應用程式和物件、 以及叢集或節點的效能指標。

儀表板可讓您判斷下列資訊：

- 健全狀況：叢集的健全度如何？
- 容量：叢集上有哪些可用容量？
- 效能：根據延遲、IOPS和處理量、叢集的效能如何？
- 網路：網路如何設定主機和儲存物件、例如連接埠、介面和儲存VM？

在「健全狀況與容量」總覽中、您可以按一下 → 以檢視其他資訊並執行工作。

在「效能」總覽中、您可以根據小時、日、週、月或年來檢視指標。

在「網路總覽」中、會顯示網路中每個物件的數量（例如「8個NVMe / FC連接埠」）。 您可以按一下號碼來檢視每個網路物件的詳細資料。

檢視叢集儀表板的效能

使用儀表板、針對您可能想要新增或移動的工作負載做出明智決策。您也可以查看尖峰使用時間、以規劃可能的變更。

效能值每3秒重新整理一次、效能圖表每15秒重新整理一次。

步驟

1. 按一下*儀表板*。
2. 在「效能」下、選取時間間隔。

識別熱磁碟區和其他物件

識別經常存取的磁碟區（熱磁碟區）和資料（熱物件）、加速叢集效能。

> 從 ONTAP 9.10.1 開始、您可以使用檔案系統分析中的「活動追蹤」功能來監控磁碟區中的 Hot 物件。

步驟

1. 按一下「儲存設備>磁碟區」。
2. 篩選IOPS、延遲和處理量欄、以檢視經常存取的磁碟區和資料。

修改QoS

從 ONTAP 9.8 開始、當您配置儲存設備時、 服務品質（QoS） 預設為啟用。您可以在資源配置程序期間停用QoS或選擇自訂QoS原則。您也可以在配置儲存設備之後修改QoS。

步驟

1. 在 System Manager 中，選擇 * Storage* ，然後選擇 * Volumes * 。
2. 在您要修改 QoS 的磁碟區旁、選取 ⋮ 然後 * 編輯 * 。

監控風險

自 ONTAP 9.10.0 起，您可以使用 System Manager 來監控 Active IQ Digital Advisor 所回報的風險事項。 從版本《21》開始ONTAP 、您可以使用System Manager來確認風險。

NetApp Active IQ Digital Advisor 會報告能夠降低風險、改善儲存環境效能與效率的機會。 有了System Manager、您就能瞭解Active IQ 到由VMware回報的風險、並獲得可據以行動的情報、協助您管理儲存設備、達到更高的可用度、更高的安全性、以及更好的儲存效能。

連結**Active IQ** 至您的帳戶

若要接收Active IQ 有關來自NetApp的風險資訊、您應先Active IQ 從System Manager連結至您的帳戶。

步驟

1. 在System Manager中、按一下*叢集>設定*。
2. 在「* Active IQ 《》註冊》下、按一下「註冊」。
3. 輸入您的認證Active IQ 資料以供填寫。
4. 驗證您的認證資料後、按一下*「確認」以連結Active IQ 至System Manager*。

檢視風險數量

從ONTAP 版本號的0：9.10.0開始、您可以從System Manager的儀表板檢視Active IQ 由NetApp回報的風險數量。

開始之前

您必須從System Manager建立連線至Active IQ 您的無法使用的帳戶。 請參閱 連結Active IQ 至您的帳戶。

步驟

1. 在System Manager中、按一下*儀表板*。
2. 在「健全狀況」區段中、檢視報告的風險數量。

> ⓘ 您可以按一下顯示風險數量的訊息、檢視每個風險的詳細資訊。 請參閱 檢視風險詳細資料。

檢視風險詳細資料

從ONTAP 功能區9.10.0開始、您可以從System Manager檢視Active IQ 由功能區所報告的風險如何根據影響區進行分類。 您也可以檢視每個已報告風險的詳細資訊、其對系統的潛在影響、以及您可以採取的修正行動。

開始之前

您必須從System Manager建立連線至Active IQ 您的無法使用的帳戶。 請參閱 連結Active IQ 至您的帳戶。

步驟

1. 按一下*事件>所有事件*。
2. 在「總覽」區段的* Active IQ 《參考建議》下、檢視每個「影響領域」類別中的風險數量。 風險類別包括：
    - 效能與效率
    - 可用度與保護
    - 容量
    - 組態
    - 安全性
3. 按一下* Active IQ 《建議*》索引標籤、即可檢視每項風險的相關資訊、包括：
    - 對系統的影響程度
    - 風險類別
    - 受影響的節點
    - 所需的緩解類型
    - 您可以採取的修正行動

瞭解風險

從《21》（《21》）開始、您可以使用System Manager來確認任何開放式風險。ONTAP

步驟

1. 在System Manager中、執行中的程序來顯示風險清單 檢視風險詳細資料。
2. 按一下您要確認的開放風險風險名稱。
3. 在下列欄位中輸入資訊：
    - 提醒（日期）
    - 理由
    - 註解
4. 按一下*「Acknowledge」

> 在您承認某項風險之後、需要幾分鐘的時間才能將變更反映在Active IQ 提出的各項建議清單中。

不承認風險

從版本號《21：10.1》開始ONTAP 、您可以使用System Manager來取消確認先前已確認的任何風險。

步驟

1. 在System Manager中、執行中的程序來顯示風險清單 檢視風險詳細資料。
2. 按一下您要取消認可的已確認風險的風險名稱。
3. 在下列欄位中輸入資訊：
   - 理由
   - 註解
4. 按一下*取消認可*。

> 在您取消認可某項風險之後、需要幾分鐘的時間才能將變更反映在Active IQ 「推薦」清單中。

System Manager 洞見

從 ONTAP 9.11.1 開始、系統管理員會顯示 _Insights 、協助您最佳化系統的效能與安全性。

> 若要檢視、自訂及回應深入分析、請參閱 "獲得深入見解、協助您最佳化系統"

容量洞見

System Manager 可根據系統的容量狀況顯示下列洞見：

洞見	嚴重性	條件	修正
本機層缺乏空間	補救風險	一或多個本機層的整體容量超過 95% 、而且成長迅速。現有的工作負載可能無法擴充、或是在極端情況下、現有的工作負載可能會用盡空間而故障。	• 建議的修正 * ：執行下列其中一個選項。 • 清除 Volume 恢復佇列。 • 在完整佈建的磁碟區上啟用精簡配置、以釋放受困的儲存空間。 • 將磁碟區移到另一個本機層。 • 刪除不需要的 Snapshot 複本。 • 刪除磁碟區中不需要的目錄或檔案。 • 啟用 Fabric Pool 將資料分層至雲端。

應用程式缺乏空間	需要注意	一或多個磁碟區已滿 95% 以上、但未啟用自動擴充功能。	• 建議 * ：啟用自動擴充、最高可達目前容量的 150% 。 • 其他選項 * ： • 刪除 Snapshot 複本以回收空間。 • 調整磁碟區大小。 • 刪除目錄或檔案。
FlexGroup 磁碟區的容量不平衡	最佳化儲存	一或多個 FlexGroup 磁碟區的組成磁碟區大小隨著時間而成長不平均、導致容量使用率不平衡。 如果組成磁碟區已滿、可能會發生寫入失敗。	• 建議 * ：重新平衡 FlexGroup 磁碟區。
儲存 VM 容量不足	最佳化儲存	一或多個儲存 VM 的容量接近最大容量。如果儲存 VM 達到最大容量、您將無法為新的或現有的磁碟區配置更多空間。	• 建議 * ：如果可能、請增加儲存 VM 的最大容量限制。

安全見解

System Manager 可針對可能危及資料或系統安全的情況、顯示下列深入見解。

洞見	嚴重性	條件	修正
磁碟區仍處於反勒索軟體學習模式	需要注意	一或多個磁碟區已處於反勒索軟體學習模式 90 天。	• 建議 * ：為這些磁碟區啟用反勒索軟體作用中模式。
磁碟區上已啟用自動刪除 Snapshot 複本	需要注意	在一個或多個磁碟區上啟用快照自動刪除。	• 建議 * ：停用自動刪除 Snapshot 複本。否則、萬一發生勒索軟體攻擊、可能無法針對這些磁碟區進行資料恢復。
Volume 沒有 Snapshot 原則	需要注意	一個或多個磁碟區沒有適當的 Snapshot 原則附加在它們上。	• 建議 * ：將 Snapshot 原則附加至沒有 Snapshot 原則的磁碟區。否則、萬一發生勒索軟體攻擊、可能無法針對這些磁碟區進行資料恢復。
未設定原生 FPolicy	最佳實務做法	未在一或多個 NAS 儲存 VM 上設定原生 FPolicy 。	• 推薦 * ： * 重要 * ：封鎖副檔名可能會導致非預期的結果。從 9.11.1 開始、您可以為儲存 VM 啟用原生 FPolicy 、以封鎖已知用於勒索軟體攻擊的超過 3000 個副檔名。 "設定原生 FPolicy" 在 NAS 儲存 VM 中、控制允許或不允許寫入環境磁碟區的副檔名。

已啟用 Telnet	最佳實務做法	安全 Shell （ SSH ）應用於安全的遠端存取。	• 建議 * ：停用 Telnet 並使用 SSH 進行安全的遠端存取。
設定的 NTP 伺服器太少	最佳實務做法	針對 NTP 設定的伺服器數量少於 3 部。	• 建議 * ：將至少三個 NTP 伺服器與叢集建立關聯。 否則、叢集時間的同步可能會發生問題。
已啟用遠端 Shell （ RSH ）	最佳實務做法	安全 Shell （ SSH ）應用於安全的遠端存取。	• 建議 * ：停用 RSH 並使用 SSH 進行安全遠端存取。
未設定登入橫幅	最佳實務做法	未針對叢集、儲存 VM 或兩者設定登入訊息。	• 建議 * ：設定叢集和儲存 VM 的登入橫幅、並啟用其使用。
AutoSupport 使用的是不安全的傳輸協定	最佳實務做法	AutoSupport 未設定為透過 HTTPS 通訊。	• 建議 * ：強烈建議使用 HTTPS 做為預設傳輸通訊協定、將 AutoSupport 訊息傳送給技術支援部門。
預設管理使用者未鎖定	最佳實務做法	沒有人使用預設的系統管理帳戶（ admin 或 diag ）登入、而且這些帳戶不會被鎖定。	• 建議 * ：不使用預設管理帳戶時、請鎖定這些帳戶。
Secure Shell （ SSH ）使用非安全的密碼	最佳實務做法	目前的組態使用不安全的 CBC 密碼。	• 建議 * ：您應該僅允許網路伺服器上的安全密碼、以保護與訪客的安全通訊。移除名稱包含「 CBC 」的密碼、例如「 ais128/CBC 」、「 aes192-CBC 」、「 AES256-CBC 」和「 3DES-CBC 」。
停用全域 FIPS 140-2 規範	最佳實務做法	叢集上的全域 FIPS 140-2 規範已停用。	• 建議 * ：基於安全考量、您應啟用符合全球 FIPS 140-2 標準的加密技術、以確保 ONTAP 能安全地與外部用戶端或伺服器用戶端通訊。
磁碟區並未受到勒索軟體攻擊的監控	需要注意	在一或多個磁碟區上停用反勒索軟體。	• 建議 * ：在磁碟區上啟用反勒索軟體。否則、您可能不會注意到磁碟區受到威脅或攻擊。
儲存 VM 並未設定用於反勒索軟體	最佳實務做法	一或多個儲存 VM 未設定為提供反勒索軟體保護。	• 建議 * ：在儲存 VM 上啟用反勒索軟體。否則、您可能不會注意到儲存 VM 受到威脅或攻擊。

組態洞見

System Manager 可以顯示下列深入資訊、以回應您對系統組態的疑慮。

洞見	嚴重性	條件	修正

叢集未設定用於通知	最佳實務做法	電子郵件、Webhooks 或 SNMP traphost 未設定為可讓您接收有關叢集問題的通知。	• 建議 * ：設定叢集通知。
叢集未設定為自動更新。	最佳實務做法	叢集尚未設定為在最新的磁碟鑑定套件、磁碟韌體、機櫃韌體和 SP/BMC 韌體檔案可用時、接收自動更新。	• 建議 * ：啟用此功能。
叢集韌體不是最新的	最佳實務做法	您的系統沒有最新的韌體更新、可能會有改善、安全性修補程式或新功能、有助於保護叢集的安全、以獲得更好的效能。	• 建議 * ：更新 ONTAP 韌體。

獲得深入見解、協助您最佳化系統

有了System Manager、您可以檢視有助於最佳化系統的洞見。

關於這項工作

從版本支援的版本起、您可以在System Manager中檢視洞見、協助您最佳化系統的容量和安全法規遵循。ONTAP

從功能完善的版本9.11.1開始ONTAP 、您可以檢視更多深入見解、協助您最佳化系統的容量、安全法規遵循及組態。

> • 封鎖延伸可能會導致非預期的結果。 * 從 ONTAP 9.11.1 開始、您可以使用系統管理員為儲存 VM 啟用原生 FPolicy 。您可能會收到 System Manager Insight 的訊息、建議您這樣做 "設定原生 FPolicy" 適用於儲存 VM 。
>
> 使用 FPolicy 原生模式、您可以允許或不允許特定的副檔名。System Manager 建議使用超過 3000 個不允許的檔案副檔名、這些副檔名曾在過去的勒索軟體攻擊中使用過。 您環境中的合法檔案可能會使用其中一些副檔名、而封鎖這些副檔名可能會導致非預期的問題。
>
> 因此、強烈建議您修改擴充功能清單、以符合您環境的需求。請參閱 "如何從系統管理員使用系統管理員建立的原生 FPolicy 組態中移除副檔名、以重新建立原則"。
>
> 若要深入瞭解原生 FPolicy 、請參閱 "FPolicy組態類型"。

根據最佳實務做法、這些洞見會顯示在單一頁面上、您可以立即採取行動來最佳化系統。如需每個深入分析的詳細資訊、請參閱 "System Manager 洞見"。

檢視最佳化洞見

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。

   「* Insights *」頁面會顯示一組見解。 每組洞見都可能包含一或多個洞見。 將顯示下列群組：

   - 需要您的注意
   - 補救風險
   - 最佳化您的儲存設備

2. （選用）按一下頁面右上角的這些按鈕、篩選所顯示的洞見：

   - 顯示安全性相關洞見。
   - 顯示容量相關洞見。
   - 顯示組態相關洞見。
   - All 顯示所有見解。

回應洞見以最佳化您的系統

在System Manager中、您可以藉由取消洞見、探索不同的方法來修正問題、或是開始修正問題的程序來回應洞見。

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 將游標停留在深入資訊上、即可顯示可執行下列動作的按鈕：

   - 解除：從檢視中移除深入見解。 若要「解僱」洞察、請參閱 [customize-settings-insights]。
   - 瀏覽：瞭解各種方法、以修正深入見解中提及的問題。 只有在有多種補救方法時、才會顯示此按鈕。
   - 修正：啟動補救Insight中提及問題的程序。系統會要求您確認是否要採取套用修正程式所需的行動。

> 有些動作可從System Manager的其他頁面啟動、但* Insights *頁面可讓您從這個頁面啟動這些動作、協助您簡化日常工作。

自訂深入分析的設定

您可以在 System Manager 中自訂要通知的深入資訊。

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 在頁面右上角、按一下 ⋮，然後選擇*設定*。
3. 在*設定*頁面上、請確認您要收到通知的深入資訊旁的核取方塊有勾選。 如果您先前曾拒絕某個見解、您可以在其核取方塊中勾選、以「取消關閉」該見解。

4. 按一下「 * 儲存 * 」。

將洞見匯出成**PDF**檔案

您可以將所有適用的洞見匯出成PDF檔案。

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 在頁面右上角、按一下 ⋮，然後選擇*匯出*。

設定原生 **FPolicy**

從 ONTAP 9.11.1 開始、當您收到建議實作原生 FPolicy 的 System Manager Insight 時、您可以在儲存 VM 和 Volume 上進行設定。

開始之前

當您存取 System Manager Insights 時、在 * 套用最佳實務做法 * 下、您可能會收到訊息、表示未設定原生 FPolicy 。

若要深入瞭解 FPolicy 組態類型、請參閱 "FPolicy組態類型"。

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 在 * 套用最佳實務 * 下、找出 * 未設定原生 FPolicy * 。
3. 在採取行動之前、請先閱讀下列訊息：

> ◦ 封鎖延伸可能會導致非預期的結果。 * 從 ONTAP 9.11.1 開始、您可以使用系統管理員為儲存 VM 啟用原生 FPolicy 。
> 使用 FPolicy 原生模式、您可以允許或不允許特定的副檔名。System Manager 建議使用超過 3000 個不允許的檔案副檔名、這些副檔名曾在過去的勒索軟體攻擊中使用過。 您環境中的合法檔案可能會使用其中一些副檔名、而封鎖這些副檔名可能會導致非預期的問題。
>
> 因此、強烈建議您修改擴充功能清單、以符合您環境的需求。請參閱 "如何從系統管理員使用系統管理員建立的原生 FPolicy 組態中移除副檔名、以重新建立原則"。

4. 按一下 **Fix** 。
5. 選取您要套用原生 FPolicy 的儲存 VM 。
6. 針對每個儲存 VM 、選取要接收原生 FPolicy 的磁碟區。
7. 按一下「設定」。

使用**CLI**監控及管理叢集效能

效能監控與管理總覽

您可以設定基本的效能監控與管理工作、並找出並解決常見的效能問題。

如果您的情況符合下列假設、您可以使用這些程序來監控及管理叢集效能：

- 您想要使用最佳實務做法、而非探索每個可用選項。
- 您想要顯示系統狀態和警示、監控叢集效能、以及使用Active IQ Unified Manager 除了OnCommand 使用VMware命令列介面以外的其他功能、使用VMware（前身為VMware Unified Manager）執行根本原因分析ONTAP 。
- 您使用ONTAP 的是效能不穩定的命令列介面來設定儲存服務品質（QoS）。

  QoS也可在System Manager、NSLA、WFA、VSC（VMware外掛程式）和API中使用。

- 您想要使用虛擬應用裝置來安裝Unified Manager、而非Linux或Windows安裝。
- 您願意使用靜態組態、而非DHCP來安裝軟體。
- 您可以在ONTAP 進階權限層級存取指令檔。
- 您是具有「admin」角色的叢集管理員。

相關資訊

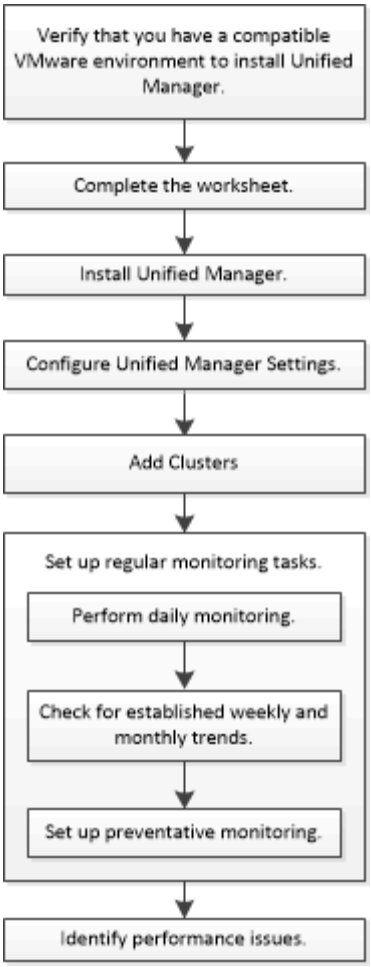
如果這些假設不符合您的情況、您應該看到下列資源：

- "安裝過程Active IQ Unified Manager"
- "系統管理"

監控效能

效能監控與維護工作流程總覽

監控和維護叢集效能包括安裝 Active IQ Unified Manager 軟體、設定基本監控工作、識別效能問題、以及視需要進行調整。



確認您的**VMware**環境受到支援

若要成功安裝Active IQ Unified Manager VMware、您必須確認您的VMware環境符合必要的要求。

步驟

1. 確認您的VMware基礎架構符合安裝Unified Manager的規模需求。
2. 前往 "互通性對照表" 若要驗證您是否擁有下列元件的支援組合：
   - 版本ONTAP
   - ESXi作業系統版本
   - VMware vCenter Server版本
   - VMware Tools版本
   - 瀏覽器類型與版本

     - "互通性對照表" 列出Unified Manager支援的組態。
3. 按一下所選組態的組態名稱。

   該組態的詳細資料會顯示在「組態詳細資料」視窗中。

4. 檢閱下列索引標籤中的資訊：
    - 附註

      列出組態專屬的重要警示和資訊。
    - 原則與準則

      提供所有組態的一般準則。

工作表**Active IQ Unified Manager**

安裝、設定及連接Active IQ Unified Manager 等功能之前、您應該先準備好環境的特定資訊。您可以將資訊記錄在工作表中。

Unified Manager安裝資訊

部署軟體的虛擬機器	您的價值
ESXi伺服器IP位址	
主機完整網域名稱	
主機IP位址	
網路遮罩	
閘道 IP 位址	
主要DNS位址	
次要DNS位址	
搜尋網域	
維護使用者名稱	
維護使用者密碼	

Unified Manager組態資訊

設定	您的價值
維護使用者電子郵件地址	
NTP 伺服器	

SMTP伺服器主機名稱或IP位址	
SMTP 使用者名稱	
SMTP 密碼	
SMTP預設連接埠	25（預設值）
傳送警示通知的電子郵件	
LDAP連結辨別名稱	
LDAP綁定密碼	
Active Directory管理員名稱	
Active Directory密碼	
驗證伺服器基礎辨別名稱	
驗證伺服器主機名稱或IP位址	

叢集資訊

針對Unified Manager上的每個叢集擷取下列資訊。

第1叢集、共N個	您的價值
主機名稱或叢集管理IP位址	
系統管理員使用者名稱ONTAP 系統管理員必須已被指派「admin」角色。	
管理員密碼ONTAP	
傳輸協定（HTTP或HTTPS）	

相關資訊

"系統管理員驗證與RBAC"

安裝Active IQ Unified Manager

下載及部署Active IQ Unified Manager 功能

若要安裝軟體、您必須下載虛擬應用裝置（VA）安裝檔案、然後使用VMware vSphere Client將檔案部署至VMware ESXi伺服器。VA可在OVA檔案中使用。

步驟

1. 前往 *NetApp 支援網站軟體下載*頁面，找到 Active IQ Unified Manager。

   https://mysupport.netapp.com/products/index.html

2. 在* Select Platform*下拉式功能表中選取* VMware vSpher*、然後按一下* Go！*
3. 將「OVA」檔案儲存至VMware vSphere Client可存取的本機或網路位置。
4. 在VMware vSphere Client中、按一下*檔案*>*部署OVF範本*。
5. 找到「OVA」檔案、然後使用精靈在ESXi伺服器上部署虛擬應用裝置。

   您可以使用精靈中的*內容*索引標籤來輸入靜態組態資訊。

6. 開啟VM電源。
7. 按一下「主控台」索引標籤以檢視初始開機程序。
8. 依照提示在VM上安裝VMware Tools。
9. 設定時區。
10. 輸入維護使用者名稱和密碼。
11. 移至VM主控台顯示的URL。

設定初始Active IQ Unified Manager 的靜態設定

當您第一次存取Web UI時、會出現「還原初始設定」對話方塊、Active IQ Unified Manager 讓您設定一些初始設定並新增叢集。

步驟

1. 接受AutoSupport 預設啟用的設定。
2. 輸入NTP伺服器詳細資料、維護使用者電子郵件地址、SMTP伺服器主機名稱及其他的SMTP選項、然後按一下*「Save*（儲存*）」。

完成後

初始設定完成後、會顯示「叢集資料來源」頁面、您可以在其中新增叢集詳細資料。

指定要監控的叢集

您必須將叢集新增至Active IQ Unified Manager VMware伺服器、才能監控叢集、檢視叢集探索狀態、以及監控其效能。

您需要的產品

- 您必須具備下列資訊：
  - 主機名稱或叢集管理IP位址

    主機名稱是Unified Manager用來連線至叢集的完整網域名稱（FQDN）或簡稱。此主機名稱必須解析為叢集管理IP位址。

  叢集管理IP位址必須是管理儲存虛擬機器（SVM）的叢集管理LIF。如果使用節點管理LIF、則作業會失敗。

  - 系統管理員使用者名稱和密碼ONTAP
  - 可在叢集上設定的傳輸協定類型（HTTP或HTTPS）、以及叢集的連接埠編號
- 您必須具有應用程式管理員或儲存管理員角色。
- 這個系統管理員必須具備ONTAPI和SSH管理員角色。ONTAP
- Unified Manager FQDN必須能夠ping ONTAP 指令功能。

  您可以使用 ONTAP 命令來驗證這一點 `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*。

關於這項工作

若要進行支援、您必須同時新增本機和遠端叢集、而且叢集必須正確設定。MetroCluster

步驟

1. 按一下「組態>*叢集資料來源*」。
2. 在「叢集」頁面中、按一下「新增」。
3. 在「新增叢集」對話方塊中、指定所需的值、例如叢集的主機名稱或IP位址（IPv4或IPv6）、使用者名稱、密碼、通訊協定及連接埠號碼。

   預設會選取HTTPS傳輸協定。

   您可以將叢集管理IP位址從IPv6變更為IPv4、或從IPv6變更為IPv6。新的IP位址會在下一個監控週期結束後、反映在叢集網格和叢集組態頁面中。

4. 按一下「 * 新增 * 」。
5. 如果選取HTTPS、請執行下列步驟：
   a. 在「授權主機」對話方塊中、按一下「檢視憑證」以檢視叢集的憑證資訊。
   b. 按一下「是」。

      Unified Manager只會在一開始新增叢集時檢查憑證、但不會檢查每個API呼叫ONTAP 到Etricity。

   如果憑證已過期、您就無法新增叢集。您必須更新SSL憑證、然後新增叢集。

6. 選用：檢視叢集探索狀態：
   a. 從「叢集設定」頁面檢閱叢集探索狀態。

   叢集會在預設監控時間間隔約15分鐘後新增至Unified Manager資料庫。

設定基本監控工作

執行每日監控

您可以執行每日監控、確保不會發生任何需要注意的立即效能問題。

步驟

1. 從這個功能表、前往*事件目錄*頁面、檢視所有目前和過時的事件。Active IQ Unified Manager
2. 從 * 檢視 * 選項中、選取 `Active Performance Events` 並決定需要採取什麼行動。

利用每週和每月的效能趨勢來找出效能問題

識別效能趨勢可協助您分析磁碟區延遲、以識別叢集是否過度使用或使用不足。您可以使用類似的步驟來識別CPU、網路或其他系統瓶頸。

步驟

1. 找出您懷疑使用量過低或過度使用的磁碟區。
2. 在* Volume Details（磁碟區詳細資料）索引標籤上、按一下 30 d*以顯示歷史資料。
3. 在「解密資料依據」下拉式功能表中、選取「延遲」、然後按一下「提交」。
4. 在叢集元件比較表中取消選取* Aggregate *、然後將叢集延遲與磁碟區延遲圖表進行比較。
5. 選取* Aggregate *並取消選取叢集元件比較表中的所有其他元件、然後將Aggregate延遲與Volume延遲圖表進行比較。
6. 將讀取/寫入延遲圖表與Volume延遲圖表進行比較。
7. 判斷用戶端應用程式負載是否造成工作負載爭用、並視需要重新平衡工作負載。
8. 判斷該集合體是否過度使用、並視需要造成爭用和重新平衡工作負載。

使用效能臨界值來產生事件通知

事件是Active IQ Unified Manager 指在發生預先定義的情況或效能計數器值超過臨界值時、由現象中心自動產生的通知。事件可協助您識別所監控叢集的效能問題。您可以設定警示、在發生特定嚴重性類型的事件時自動傳送電子郵件通知。

設定效能臨界值

您可以設定效能臨界值來監控關鍵效能問題。使用者定義的臨界值會在系統接近或超過定義的臨界值時觸發警告或重大事件通知。

步驟

1. 建立「警告」和「重大」事件臨界值：
   a. 選擇*組態*>*效能臨界值*。
   b. 按一下「 * 建立 * 」。
   c. 選取物件類型、然後指定原則的名稱和說明。
   d. 選取物件計數器條件、並指定定義「警告」和「重大」事件的限制值。

e. 選取要傳送事件時必須違反限制值的持續時間、然後按一下「儲存」。

2. 將臨界值原則指派給儲存物件。

   a. 移至「Inventory」頁面以取得先前選取的相同叢集物件類型、然後從「View」（檢視）選項中選擇「* Performance 」（效能）。

   b. 選取您要指派臨界值原則的物件、然後按一下*指派臨界值原則*。

   c. 選取您先前建立的原則、然後按一下*指派原則*。

範例

您可以設定使用者定義的臨界值、以瞭解關鍵效能問題。例如、如果您有Microsoft Exchange Server、而且知道當磁碟區延遲超過20毫秒時會當機、您可以將警告臨界值設為12毫秒、臨界臨界臨界值設為15毫秒。有了此臨界值設定、您就能在磁碟區延遲超過限制時收到通知。

新增警示

您可以設定警示、以便在產生特定事件時通知您。您可以為單一資源、一組資源或特定嚴重性類型的事件設定警示。您可以指定通知的頻率、並將指令碼與警示建立關聯。

您需要的產品

- 您必須設定通知設定、例如使用者電子郵件地址、SMTP伺服器和SNMP設陷主機、才能讓Active IQ Unified Manager 此伺服器在產生事件時使用這些設定來傳送通知給使用者。
- 您必須知道要觸發警示的資源和事件、以及您要通知的使用者使用者名稱或電子郵件地址。
- 如果您想要根據事件執行指令碼、必須使用「指令碼」頁面將指令碼新增至Unified Manager。
- 您必須具有應用程式管理員或儲存管理員角色。

關於這項工作

除了從「警示設定」頁面建立警示之外、您也可以在收到事件後直接從「事件詳細資料」頁面建立警示、如以下所述。

步驟

1. 在左導覽窗格中、按一下*儲存管理*>*警示設定*。
2. 在「警示設定」頁面中、按一下「新增」。
3. 在「新增警示」對話方塊中、按一下「名稱」、然後輸入警示的名稱和說明。
4. 按一下*資源*、然後選取要納入警示或排除在警示範圍之外的資源。

   您可以在「名稱包含」欄位中指定文字字串、以選取一組資源、藉此設定篩選條件。根據您指定的文字字串、可用資源清單僅會顯示符合篩選規則的資源。您指定的文字字串區分大小寫。

   如果資源同時符合您所指定的「包含」和「排除」規則、則排除規則優先於「包含」規則、而且不會針對與排除資源相關的事件產生警示。

5. 按一下*事件*、然後根據您要觸發警示的事件名稱或事件嚴重性類型來選取事件。

若要選取多個事件、請在選取時按Ctrl鍵。

6. 按一下「動作」、然後選取您要通知的使用者、選擇通知頻率、選擇是否要將SNMP設陷傳送到設陷接收器、並指派指令碼在產生警示時執行。

   如果您修改為使用者指定的電子郵件地址、然後重新開啟警示以進行編輯、則「名稱」欄位會顯示空白、因為修改後的電子郵件地址不再對應至先前選取的使用者。此外、如果您從「使用者」頁面修改所選使用者的電子郵件地址、則所選使用者的修改電子郵件地址不會更新。

   您也可以選擇透過SNMP設陷通知使用者。

7. 按一下「 * 儲存 * 」。

新增警示的範例

本範例說明如何建立符合下列需求的警示：

- 警示名稱：HealthTest
- 資源：包括名稱包含「abc」的所有磁碟區、並排除名稱包含「xyz」的所有磁碟區
- 事件：包括所有重要的健全狀況事件
- 行動：包括「sample@domain.com」、「Test」指令碼、使用者必須每15分鐘通知一次

在「新增警示」對話方塊中執行下列步驟：

1. 按一下*名稱*、然後輸入 `HealthTest` 在*警示名稱*欄位中。
2. 按一下「資源」、然後在「包含」索引標籤中、從下拉式清單中選取「磁碟區」。
   a. 輸入 `abc` 在 * 名稱 Contains* 欄位中、顯示名稱包含「 abc 」的磁碟區。
   b. 選取*<<All Volumes whose name contains 'abc'>>「可用資源」區域中的「*」、然後將其移至「選取的資源」區域。
   c. 按一下*排除*、然後輸入 `xyz` 在「名稱包含」欄位中、然後按一下「新增」。
3. 按一下「事件」、然後從「事件嚴重性」欄位中選取「嚴重」。
4. 從「Matching Event（符合事件）」區域中選取* All Critical事件*、然後將其移至「Selected Event（選取的事件）」區域。
5. 按一下「動作」、然後輸入 `sample@domain.com` 在警示這些使用者欄位中。
6. 選擇*每15分鐘提醒一次*、每15分鐘通知使用者一次。

   您可以設定警示、在指定時間內重複傳送通知給收件者。您應該決定警示的事件通知啟動時間。

7. 在Select Script to執行（選擇要執行的指令碼）功能表中、選取* Test*指令碼。
8. 按一下「 * 儲存 * 」。

設定警示設定

您可以指定Active IQ Unified Manager 哪些事件來自於「觸發警示」、哪些電子郵件收件

者用於這些警示、以及警示的頻率。

您需要的產品

您必須具有應用程式管理員角色。

關於這項工作

您可以針對下列類型的效能事件、設定獨特的警示設定：

- 因違反使用者定義的臨界值而觸發的重大事件
- 因違反使用者定義的臨界值、系統定義的臨界值或動態臨界值而觸發的警告事件

根據預設、所有新事件的電子郵件警示都會傳送給Unified Manager管理使用者。您可以新增其他使用者的電子郵件地址、將電子郵件警示傳送給其他使用者。

> 若要停用特定類型事件的警示傳送、您必須清除事件類別中的所有核取方塊。此動作不會停止在使用者介面中顯示事件。

步驟

1. 在左側導覽窗格中、選取* Storage Management **>** Alert Setup *。

   隨即顯示警示設定頁面。

2. 按一下「新增」、為每種事件類型設定適當的設定。

   若要將電子郵件警示傳送給多位使用者、請在每個電子郵件地址之間輸入一個逗號。

3. 按一下「 * 儲存 * 」。

找出**Active IQ Unified Manager** 效能問題

如果發生效能事件、您可以在Active IQ Unified Manager VMware內部找出問題的根源、並使用其他工具加以修正。您可能會在每日監控期間收到事件的電子郵件通知或通知事件。

步驟

1. 按一下電子郵件通知中的連結、即可直接前往發生效能事件的儲存物件。

如果您…	然後…
收到活動的電子郵件通知	按一下連結即可直接前往活動詳細資料頁面。
在分析「事件詳細目錄」頁面時、請注意事件	選取要直接前往事件詳細資料頁面的事件。

2. 如果事件已超過系統定義的臨界值、請遵循UI中的建議動作來疑難排解問題。
3. 如果事件已超過使用者定義的臨界值、請分析事件以判斷您是否需要採取行動。
4. 如果問題仍然存在、請檢查下列設定：
   - 儲存系統上的傳輸協定設定

- 任何乙太網路或光纖交換器上的網路設定
- 儲存系統上的網路設定
- 儲存系統上的磁碟配置和Aggregate度量

5. 如果問題持續發生、請聯絡技術支援部門以尋求協助。

使用 **Active IQ Digital Advisor** 檢視系統效能

對於ONTAP 任何傳送AutoSupport 遙測資料給NetApp的支援系統、您都可以檢視廣泛的效能和容量資料。顯示系統效能的時間比您在System Manager中看到的更長。Active IQ

您可以檢視CPU使用率、延遲、IOPS、依傳輸協定的IOPS、以及網路處理量的圖表。您也可以下載此資料的CSV格式、以便在其他工具中進行分析。

除了這些效能資料之外Active IQ 、還可讓您根據工作負載來顯示儲存效率、並將該效率與該類型工作負載的預期效率進行比較。您可以檢視容量趨勢、並預估在特定時間範圍內可能需要增加多少儲存容量。

- 儲存效率可在主儀表板左側的客戶、叢集和節點層級上使用。
- 效能可在主儀表板左側的叢集和節點層級取得。

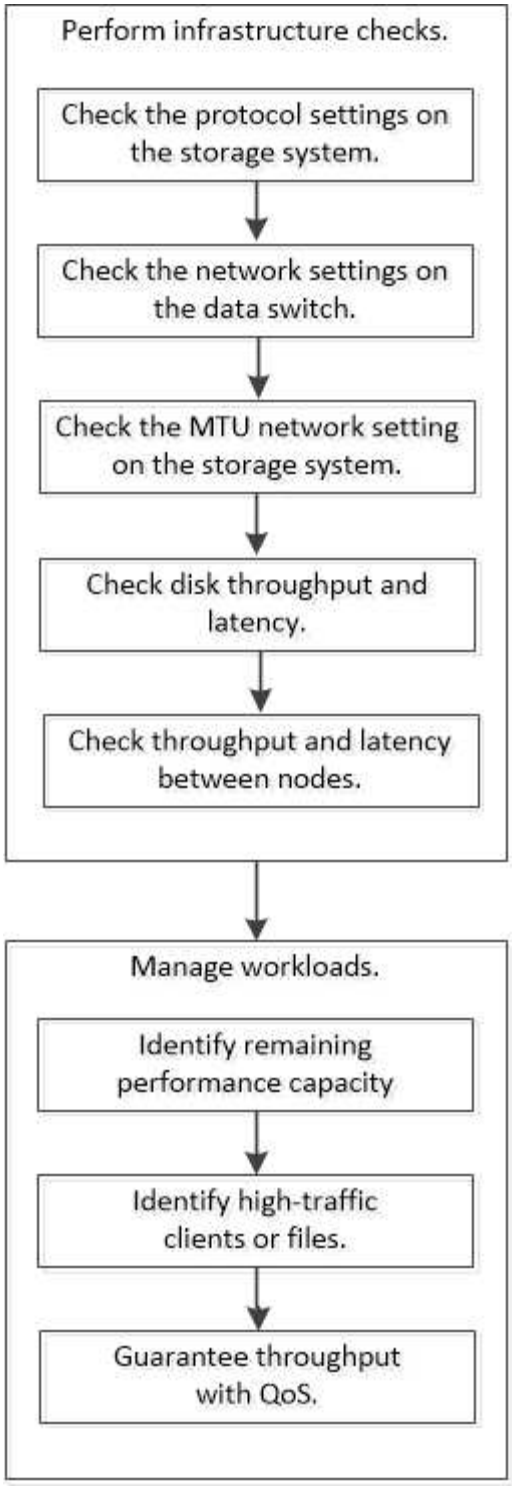
相關資訊

- "Active IQ Digital Advisor 數位顧問文件"
- "Active IQ Digital Advisor 影片播放清單"
- "網頁入口網站Active IQ"

管理效能問題

效能管理工作流程

找出效能問題之後、您可以對基礎架構進行一些基本診斷檢查、以排除明顯的組態錯誤。如果問題並未明確指出、您可以開始研究工作負載管理問題。



執行基礎架構檢查

檢查儲存系統上的傳輸協定設定

檢查**NFS TCP**的最大傳輸大小

對於NFS、您可以檢查讀取和寫入的TCP最大傳輸大小是否會造成效能問題。如果您認為規模正在減緩效能、您可以增加效能。

您需要的產品

- 您必須擁有叢集管理員權限才能執行此工作。
- 您必須使用進階權限層級命令來執行此工作。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查TCP最大傳輸大小：

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. 如果TCP最大傳輸大小太小、請增加大小：

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

下列範例變更的 TCP 傳輸大小上限 `SVM1` 至 1048576 ：

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

檢查**iSCSI TCP**讀寫大小

對於iSCSI、您可以檢查TCP讀寫大小、以判斷大小設定是否造成效能問題。如果大小是問題的根源、您可以加以修正。

您需要的產品

此工作需要進階權限層級命令。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查TCP視窗大小設定：

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. 修改TCP視窗大小設定：

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. 返回管理權限：

```
set -privilege admin
```

範例

下列範例變更的 TCP 視窗大小 `SVM1` 至 131,400 位元組：

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

檢查**CIFS**多工設定

如果CIFS網路效能緩慢導致效能問題、您可以修改多工設定來改善及修正。

步驟

1. 檢查CIFS多工設定：

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. 修改CIFS多工設定：

   ```
   vserver cifs options modify -vserver -vserver_name -max-mpx integer
   ```

範例

下列範例會變更最大多工處理次數 `SVM1` 至 255 ：

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

檢查**FC**介面卡連接埠速度

介面卡目標連接埠速度應符合其所連接裝置的速度、以最佳化效能。如果連接埠設為自動協商、則在接管與恢復或其他中斷之後、重新連線可能需要較長的時間。

您需要的產品

使用此介面卡做為其主連接埠的所有LIF都必須離線。

步驟

1. 使介面卡離線：

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. 檢查連接埠介面卡的最大速度：

   ```
   fcp adapter show -instance
   ```

3. 如有必要、請變更連接埠速度：

   ```
   network fcp adapter modify -node nodename -adapter adapter -speed
   ```

```
{1|2|4|8|10|16|auto}
```

4. 將介面卡上線：

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. 將介面卡上的所有生命都上線：

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

範例

以下範例變更介面卡的連接埠速度 `0d` 開啟 `node1` 至 2 Gbps ：

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

檢查資料交換器上的網路設定

雖然您必須在用戶端、伺服器和儲存系統（即網路端點）上維持相同的MTU設定、但NIC和交換器等中繼網路裝置應設定為最大MTU值、以確保效能不會受到影響。

為獲得最佳效能、網路中的所有元件都必須能夠轉送巨型框架（9000位元組IP、9022位元組（包括乙太網路）。資料交換器應設為至少9022位元組、但大多數交換器的典型值為9216。

程序

對於資料交換器、請檢查MTU大小是否設為9022或更高。

如需詳細資訊、請參閱交換器廠商文件。

檢查儲存系統上的**MTU**網路設定

如果儲存系統上的網路設定與用戶端或其他網路端點不同、您可以變更這些設定。雖然管理網路MTU設定設為1500、但資料網路MTU大小應為9000。

關於這項工作

廣播網域內的所有連接埠都有相同的MTU大小、但e0M連接埠處理管理流量除外。如果連接埠是廣播網域的一部分、請使用 `broadcast-domain modify` 用於變更修改的廣播網域內所有連接埠的 MTU 命令。

請注意、NIC和資料交換器等中繼網路裝置的MTU大小可以設定為比網路端點更高的MTU大小。如需詳細資訊、請參閱 "檢查資料交換器上的網路設定"。

步驟

1. 檢查儲存系統上的MTU連接埠設定：

```
network port show -instance
```

2. 變更連接埠所使用之廣播網域上的MTU：

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain
broadcast_domain -mtu new _mtu
```

範例

下列範例將MTU連接埠設定變更為9000：

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

檢查磁碟處理量和延遲

您可以檢查叢集節點的磁碟處理量和延遲度量、以協助您進行疑難排解。

關於這項工作

此工作需要進階權限層級命令。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查磁碟處理量與延遲度量：

   ```
   statistics disk show -sort-key latency
   ```

範例

下列範例顯示每個使用者讀取或寫入作業的總計 `node2` 開啟 `cluster1`：

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                     Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

檢查節點之間的處理量和延遲

您可以使用 `network test-path` 用於識別網路瓶頸或預先限定節點之間的網路路徑的

命令。您可以在叢集間節點或叢集內節點之間執行命令。

您需要的產品

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限層級命令。
- 對於叢集間路徑、必須對來源與目的地叢集進行對等處理。

關於這項工作

有時候、節點之間的網路效能可能無法滿足您對路徑組態的期望。例如、SnapMirror複寫作業所見的大型資料傳輸傳輸傳輸速率為1 Gbps、與來源叢集和目的地叢集之間的10 GbE連結不一致。

您可以使用 `network test-path` 用於測量節點之間的處理量和延遲的命令。您可以在叢集間節點或叢集內節點之間執行命令。

> 測試會將網路路徑與資料一起飽和、因此當系統不忙碌、節點之間的網路流量不多時、您應該執行命令。測試會在十秒後逾時。此命令只能在ONTAP flex9節點之間執行。

。 `session-type` 選項可識別您在網路路徑上執行的作業類型、例如、 SnapMirror 複寫至遠端目的地的「SnapMirror 遠端」。類型會指定測試中使用的資料量。下表定義工作階段類型：

工作階段類型	說明
同步鏡射位置	SnapMirror在同一叢集中的節點之間使用的設定
同步鏡射遠端	SnapMirror在不同叢集的節點之間使用的設定（預設類型）
RemoteDataTransfer	由用來在同一個叢集中的節點之間遠端存取資料的ONTAP 設定（例如、針對儲存在不同節點上磁碟區中的檔案、向節點提出NFS要求）

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 測量節點之間的處理量和延遲：

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   來源節點必須位於本機叢集內。目的地節點可以位於本機叢集或是連接叢集。的值為 "local" `-source-node` 指定執行命令的節點。

   下列命令可測量之間 SnapMirror 類型複寫作業的處理量和延遲 `node1` 在本機叢集和上 `node3` 開啟 `cluster2`：

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
Min latency in ms:  61.14
Max latency in ms:  3056.86
```

3. 返回管理權限：

   ```
   set -privilege admin
   ```

完成後

如果效能不符合對路徑組態的期望、您應該檢查節點效能統計資料、使用可用的工具來隔離網路中的問題、檢查交換器設定等。

管理工作負載

找出剩餘的效能容量

效能容量（或稱「_E餘 量」）會測量在資源上的工作負載效能開始受到延遲影響之前、您可以在節點或集合體上放置多少工作。瞭解叢集上可用的效能容量、有助於您配置及平衡工作負載。

您需要的產品

此工作需要進階權限層級命令。

關於這項工作

您可以將下列值用於 `-object` 用於收集和顯示保留空間統計資料的選項：

- 對於 CPU 、 `resource_headroom_cpu`。
- 對於集合體、 `resource_headroom_aggr`。

您也可以使用System Manager和Active IQ Unified Manager 整套功能來完成這項工作。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 開始即時保留空間統計資料收集：

   ```
   statistics start –object resource_headroom_cpu|aggr
   ```

如需完整的命令語法、請參閱手冊頁。

3. 顯示即時保留空間統計資訊：

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   如需完整的命令語法、請參閱手冊頁。

4. 返回管理權限：

   ```
   set -privilege admin
   ```

範例

下列範例顯示叢集節點的平均每小時保留空間統計資料。

您可以透過減去來計算節點的可用效能容量 `current_utilization` 來自的計數器 `optimal_point_utilization` 計數器。在此範例中、是的使用率容量 `CPU_sti2520-213` 為 -14% （ 72% 至 86% ）、表示過去一小時的 CPU 平均利用率過高。

您可以指定 `ewma_daily`、 `ewma_weekly`` 或 ``ewma_monthly` 以獲得較長時間內的相同資訊平均值。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                current_utilization                               86
                  optimal_point_ops                             2573
              optimal_point_latency                             3589
           optimal_point_utilization                              72
     optimal_point_confidence_factor                               1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                current_utilization                                 0
                  optimal_point_ops                                 0
              optimal_point_latency                                 0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                               1
2 entries were displayed.
```

識別高流量用戶端或檔案

您可以使用ONTAP 「支援物件」技術來識別造成大量叢集流量的用戶端或檔案。識別出這些「頂尖」用戶端或檔案之後、您可以重新平衡叢集工作負載、或採取其他步驟來解決問題。

您需要的產品

您必須是叢集管理員才能執行此工作。

步驟

1. 檢視存取叢集的主要用戶端：

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   如需完整的命令語法、請參閱手冊頁。

   下列命令會顯示存取的主要用戶端 `cluster1`：

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                                 *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. 檢視叢集上存取的主要檔案：

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   如需完整的命令語法、請參閱手冊頁。

   下列命令會顯示在上存取的最上層檔案 `cluster1`：

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

保證**QoS**的處理量

透過 **QoS** 總覽來保證處理量

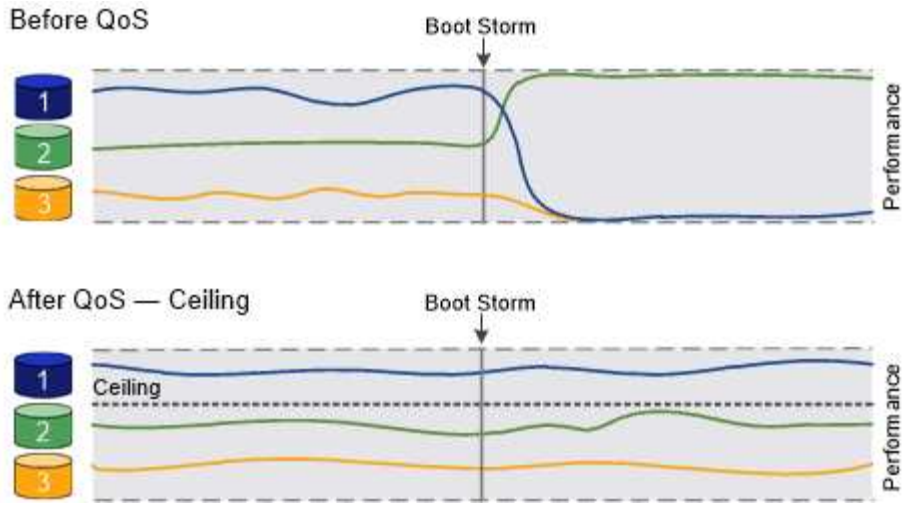
您可以使用儲存服務品質（QoS）來保證關鍵工作負載的效能不會因競爭工作負載而降級。您可以在競爭的工作負載上設定處理量上限、以限制其對系統資源的影響、或為關鍵工作負載設定處理量下限、以確保其符合最低處理量目標、無論競爭的工作負載有何需求。您甚至可以針對相同的工作負載設定上限和樓層。

關於處理量上限（**QoS**上限）

處理量上限會將工作負載的處理量限制為最大IOPS或Mbps、或IOPS和Mbps。在下圖中、工作負載2的處理量上限可確保工作負載1和3不會「凸起」。

_原則群組_定義一或多個工作負載的處理量上限。工作負載代表_storage物件的I/O作業：_磁碟區、檔案、qtree或LUN、或SVM中的所有磁碟區、檔案、qtree或LUN。您可以在建立原則群組時指定上限、也可以等到監控工作負載之後再指定上限。

> 工作負載的處理量可能超過指定上限10%、尤其是當工作負載處理量發生快速變化時。處理突發的上限可能超過50%。當權杖累積率高達150%時、單一節點上就會發生突發事件



關於處理量層（**QoS**下限）

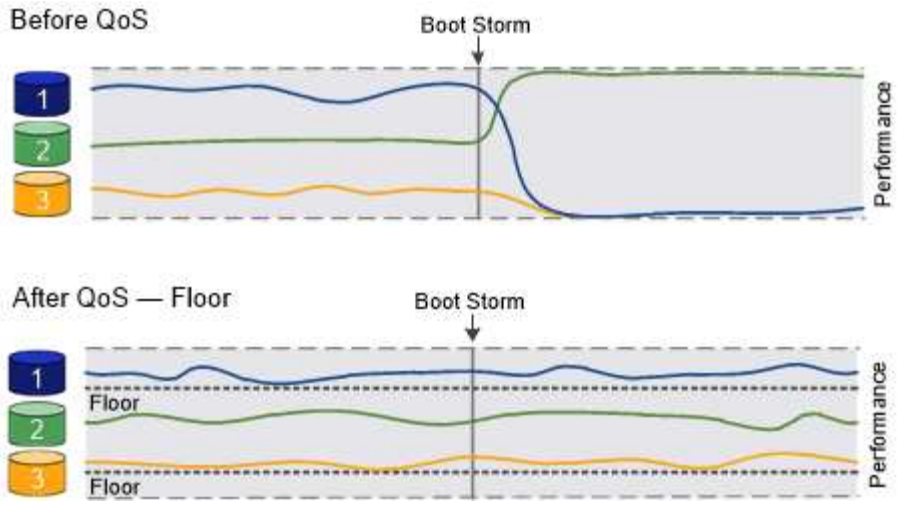
處理量層保證工作負載的處理量不會低於 IOPS 或 Mbps 的最低數量、或 IOPS 和 Mbps 。在下圖中、工作負載1和工作負載3的處理量層級可確保它們符合最低處理量目標、無論工作負載2的需求為何。

> 如範例所示、處理量上限會直接調節處理量。處理量最低層會間接調節處理量、將已設定最低層的工作負載設為優先順序。

您可以在建立原則群組時指定樓層、也可以等到監控工作負載之後再指定樓層。

從 ONTAP 9.13.1 開始、您可以使用設定 SVM 範圍的處理量層 [adaptive-qos-templates]。在 9.13.1 之前的 ONTAP 版本中、定義處理量層的原則群組無法套用至 SVM 。

> 在更新於ONTAP VMware版本9.7之前的版本中、當有足夠的可用效能容量時、就能保證處理量的樓層數。
>
> 在VMware 9.7及更新版本中、即使可用的效能容量不足、也能保證處理量的樓層數。ONTAP這種新的樓層行為稱為Floor v2。為了達成保證、第v2層級可能會導致工作負載延遲更高、而不會出現處理量層或工作環境超過場地設定的情況。第v2層同時適用於QoS和調適性QoS。
>
> ONTAP 9.7P6 及更新版本提供啟用 / 停用第 2 層樓的新行為選項。工作負載在執行關鍵作業時、可能會低於指定的樓層、例如 `volume move trigger-cutover`。即使有足夠的可用容量且未執行關鍵作業、工作負載的處理量仍可能低於指定樓層達5%。如果場地配置過度、而且沒有效能容量、則部分工作負載可能會落在指定樓層以下。



關於共享和非共享的**QoS**原則群組

從ONTAP S得9.4開始、您可以使用非共享的QoS原則群組、來指定定義的處理量上限或樓層分別套用至每個成員工作負載。共享原則群組的行為取決於原則類型：

- 對於處理量上限、指派給共用原則群組的工作負載總處理量不得超過指定上限。
- 對於處理量層、共用原則群組只能套用至單一工作負載。

關於調適性**QoS**

通常、您指派給儲存物件的原則群組值會固定。當儲存物件大小變更時、您需要手動變更值。例如、增加磁碟區上使用的空間量、通常需要為磁碟區指定的處理量上限相應增加。

_Adaptive QoS_會自動將原則群組值調整為工作負載大小、並隨著工作負載大小的變更、維持IOPS與TBs的比率。當您在大型部署中管理數百或數千個工作負載時、這是一項重大優勢。

您通常會使用調適性QoS來調整處理量上限、但也可以使用它來管理處理量層（當工作負載大小增加時）。工作負載大小是以儲存物件的已配置空間或儲存物件所使用的空間表示。

> 在ONTAP 更新版本的更新版本中、可在處理量層使用已用的空間。不支援ONTAP 使用於效能不符合更新版本的資料層。

- _allocated space_原則會根據儲存物件的名義大小、維持IOPS/TB|GB比率。如果比率為100 IOPS/GB、則150 GB的磁碟區只要磁碟區維持該大小、就會有15,000 IOPS的處理量上限。如果磁碟區大小調整為300 GB、調適性QoS會將處理量上限調整為30、000 IOPS。
- _used space_原則（預設值）會根據儲存效率前的實際資料量、維持IOPS/TB|GB比率。如果比率為100 IOPS/GB、則儲存100 GB資料的150 GB磁碟區的處理量上限為10、000 IOPS。隨著使用空間量的變化、調適性QoS會根據比率調整處理量上限。

從功能支援的9.5開始ONTAP 、您可以為應用程式指定I/O區塊大小、以IOPS和Mbps來表示處理量限制。MBps限制是根據區塊大小乘以IOPS限制計算而得。例如、IOPS限制為6144IOPS/TB的I/O區塊大小為32K、會產生192 MBps的Mbps限制。

處理量上限和樓層的行為如下：

- 當工作負載指派給調適性QoS原則群組時、上限或樓層會立即更新。

- 調整調適性QoS原則群組中的工作負載大小時、上限或樓層大約會在五分鐘內更新。

在進行更新之前、處理量必須增加至少10 IOPS。

調適性QoS原則群組永遠不會共用：定義的處理量上限或樓層會個別套用至每個成員的工作負載。

從 ONTAP 9.6 開始、透過 SSD 的 ONTAP Select Premium 即可支援處理量層。

調適性原則群組範本

從 ONTAP 9.13.1 開始、您可以在 SVM 上設定調適性 QoS 範本。可調整的原則群組範本可讓您設定 SVM 中所有磁碟區的處理量層和上限。

自適應原則群組範本只能在建立 SVM 之後設定。使用 `vserver modify` 命令 `-qos-adaptive-policy-group-template` 設定原則的參數。

當您設定調適性原則群組範本時、在設定原則之後建立或移轉的磁碟區會自動繼承原則。指派原則範本時、SVM 上現有的任何磁碟區都不會受到影響。如果停用 SVM 上的原則、任何後來移轉到 SVM 或在 SVM 上建立的磁碟區都不會收到原則。停用調適性原則群組範本不會影響繼承原則範本的磁碟區、因為這些磁碟區會保留原則範本。

如需詳細資訊、請參閱 設定調適性原則群組範本。

一般支援

下表顯示支援處理量上限、處理量層和調適性QoS的差異。

資源或功能	處理量上限	處理量最低	處理量層**v2**	調適性**QoS**
版本9 ONTAP	全部	9.2 及更新版本	9.7 及更新版本	9.3 及更新版本
平台	全部	• AFF • C190 * • 採用SSD *的高階版ONTAP Select	• AFF • C190 • 搭載SSD的高階版ONTAP Select	全部
通訊協定	全部	全部	全部	全部
FabricPool	是的	是的、如果分層原則設定為「無」、而且雲端中沒有區塊。	是的、如果分層原則設定為「無」、而且雲端中沒有區塊。	否
SnapMirror同步	是的	否	否	是的

C190 與 ONTAP Select 支援從 ONTAP 9.6 版本開始。

處理量上限支援的工作負載

下表顯示ONTAP 支援各個版本的工作負載、以支援不同版本的處理量上限。不支援根磁碟區、負載共用鏡像和資料保護鏡像。

工作負載支援-上限	**ONTAP 9.0**	**ONTAP 9.1**	**ONTAP 9.2**	**ONTAP 9.3**	**ONTAP 9.4 - 9.7**	更新版本**ONTAP**
Volume	是的	是的	是的	是的	是的	是的
檔案	是的	是的	是的	是的	是的	是的
LUN	是的	是的	是的	是的	是的	是的
SVM	是的	是的	是的	是的	是的	是的
流通量FlexGroup	否	否	否	是的	是的	是的
qtree *	否	否	否	否	否	是的
每個原則群組有多個工作負載	是的	是的	是的	是的	是的	是的
非共用原則群組	否	否	否	否	是的	是的

從 ONTAP 9.8 開始、 FlexVol 和 FlexGroup 磁碟區的 qtree 支援 NFS 存取、並啟用 NFS 。從ONTAP 推出支援SMB的支援範圍起、FlexVol 從推出支援SMB的功能、即可從功能支援功能支援使用功能的功能性功能、從功能性功能表中的qtree和FlexGroup 功能表中、存取SMB。

處理量層的支援工作負載

下表顯示ONTAP 支援各個版本之資料中心的工作負載。不支援根磁碟區、負載共用鏡像和資料保護鏡像。

工作負載支援-**Floor**	**ONTAP 9.2**	**ONTAP 9.3**	**ONTAP 9.4 - 9.7**	**ONTAP 9.8 - 9.13.0**	**ONTAP 9.13.1** 及更新版本
Volume	是的	是的	是的	是的	是的
檔案	否	是的	是的	是的	是的
LUN	是的	是的	是的	是的	是的
SVM	否	否	否	否	是的
流通量FlexGroup	否	否	是的	是的	是的
qtree *	否	否	否	是的	是的

工作負載支援-Floor	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 - 9.13.0	ONTAP 9.13.1 及更新版本
每個原則群組有多個工作負載	否	否	是的	是的	是的
非共用原則群組	否	否	是的	是的	是的

* 從 ONTAP 9.8 開始、 FlexVol 的 qtree 和啟用 NFS 的 FlexGroup 磁碟區都支援 NFS 存取。從ONTAP 推出支援SMB的支援範圍起、FlexVol 從推出支援SMB的功能、即可從功能支援功能支援使用功能的功能性功能、從功能性功能表中的qtree和FlexGroup 功能表中、存取SMB。

支援調適性**QoS**的工作負載

下表顯示ONTAP 支援各更新版本的調適性QoS的工作負載。不支援根磁碟區、負載共用鏡像和資料保護鏡像。

工作負載支援：調適性QoS	ONTAP 9.3	ONTAP 9.4 - 9.13.0	ONTAP 9.13.1 及更新版本
Volume	是的	是的	是的
檔案	否	是的	是的
LUN	否	是的	是的
SVM	否	否	是的
流通量FlexGroup	否	是的	是的
每個原則群組有多個工作負載	是的	是的	是的
非共用原則群組	是的	是的	是的

工作負載和原則群組的最大數量

下表顯示ONTAP 各個版本的工作負載和原則群組數量上限。

工作負載支援	ONTAP 9.3 及更早版本	更新版本ONTAP
每個叢集的工作負載上限	12、000	40、000
每個節點的工作負載上限	12、000	40、000
原則群組上限	12、000	12、000

啟用或停用處理量樓層**v2**

您可以啟用AFF 或停用支援速度的v2。預設為啟用。啟用第v2層時、如果控制器使用頻繁、而其他工作負載的延遲較高、則可滿足處理量層級的需求。第v2層同時適用於QoS和調適性QoS。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 輸入下列其中一個命令：

如果您想要...	使用此命令：
停用樓層v2	`qos settings throughput-floors-v2 -enable false`
啟用樓層v2	`qos settings throughput-floors-v2 -enable true`

> 若要在MetroCluster 一個不穩定叢集中停用處理量層v2、您必須執行
>
> `qos settings throughput-floors-v2 -enable false`
>
> 在來源叢集和目的地叢集上執行命令。

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

儲存**QoS**工作流程

如果您已經知道想要使用QoS管理的工作負載效能需求、可以在建立原則群組時指定處理量限制。否則、您可以等到監控工作負載之後再指定限制。

利用**QoS**設定處理量上限

您可以使用 `max-throughput` 原則群組的欄位、可定義儲存物件工作負載的處理量上限（QoS Max）。您可以在建立或修改儲存物件時套用原則群組。

您需要的產品

- 您必須是叢集管理員、才能建立原則群組。
- 您必須是叢集管理員、才能將原則群組套用至SVM。

關於這項工作

- 從ONTAP S得9.4開始、您可以使用非共享的QoS原則群組、來指定定義的處理量上限會個別套用至每個成員工作負載。否則、原則群組會是_shared：_指派給原則群組的工作負載總處理量不能超過指定上限。

  設定 `-is-shared=false` 適用於 `qos policy-group create` 用於指定非共享策略組的命令。

- 您可以指定IOPS、MB/s或IOPS、MB/s等上限的處理量限制如果您同時指定IOPS和MB/s、則會強制執行先達到的限制。

> 如果您為相同的工作負載設定上限和樓層、則只能指定上限的處理量限制（以IOPS為單位）。

- 受QoS限制的儲存物件必須由原則群組所屬的SVM所包含。多個原則群組可以屬於同一個SVM。
- 如果原則群組包含物件或其子物件屬於原則群組、則無法將儲存物件指派給原則群組。
- 將原則群組套用至相同類型的儲存物件、是QoS最佳實務做法。

步驟

1. 建立原則群組：

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   如需完整的命令語法、請參閱手冊頁。您可以使用 `qos policy-group modify` 用於調整處理量上限的命令。

   下列命令會建立共用原則群組 `pg-vs1` 最大處理量為 5 、 000 IOPS ：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   下列命令會建立非共用原則群組 `pg-vs3` 最高處理量為 100 IOPS 和 400 kb/S ：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   下列命令會建立非共用原則群組 `pg-vs4` 無處理量限制：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. 將原則群組套用至SVM、檔案、磁碟區或LUN：

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   如需完整的命令語法、請參閱手冊頁。您可以使用 *`storage_object`* `modify` 將不同原則群組套用至儲存物件的命令。

   下列命令會套用原則群組 `pg-vs1` 至 SVM `vs1`：

   ```
   cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
   ```

   下列命令會套用原則群組 `pg-app` 磁碟區 `app1` 和 `app2`：

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. 監控原則群組效能：

   `qos statistics performance show`

   如需完整的命令語法、請參閱手冊頁。

   > 監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示原則群組效能：

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. 監控工作負載效能：

   `qos statistics workload performance show`

   如需完整的命令語法、請參閱手冊頁。

   > 監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示工作負載效能：

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

您可以使用 `qos statistics workload latency show` 命令以檢視 QoS 工作負載的詳細延遲統計資料。

使用**QoS**設定處理量層

您可以使用 `min-throughput` 原則群組的欄位、可定義儲存物件工作負載的處理量層（QoS 最小值）。您可以在建立或修改儲存物件時套用原則群組。從ONTAP 功能性的問題9.8開始、您可以指定處理量層（以IOPS或Mbps為單位）、或是IOPS和Mbps。

開始之前

- 您必須執行ONTAP 的是版本不含更新版本的版本。從ONTAP NetApp 9.2開始提供處理量層。
- 您必須是叢集管理員、才能建立原則群組。
- 從 ONTAP 9.13.1 開始、您可以使用在 SVM 層級強制執行處理量層級 調適性原則群組範本。您無法在具有 QoS 原則群組的 SVM 上設定調適性原則群組範本。

關於這項工作

- 從ONTAP S得9.4開始、您可以使用非共享的QoS原則群組來指定要個別套用定義的處理量層級至每個成員工作負載。這是處理量層的原則群組可套用至多個工作負載的唯一條件。

  設定 `-is-shared=false` 適用於 `qos policy-group create` 指定非共用原則群組的命令。

- 如果節點或Aggregate上的效能容量（保留空間）不足、則工作負載的處理量可能會低於指定樓層。
- 受QoS限制的儲存物件必須由原則群組所屬的SVM所包含。多個原則群組可以屬於同一個SVM。
- 將原則群組套用至相同類型的儲存物件、是QoS最佳實務做法。
- 定義處理量層的原則群組無法套用至SVM。

步驟

1. 如所述、檢查節點或集合體上是否有足夠的效能容量 "識別剩餘的效能容量"。
2. 建立原則群組：

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   如需完整的命令語法、請參閱ONTAP 您的版本資訊手冊頁。您可以使用 `qos policy-group modify` 調整處理量樓層的命令。

   下列命令會建立共用原則群組 `pg-vs2` 最低處理量為 1 、 000 IOPS ：

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   下列命令會建立非共用原則群組 `pg-vs4` 無處理量限制：

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
-is-shared false
```

3. 將原則群組套用至磁碟區或LUN：

   storage_object create -vserver *SVM* -qos-policy-group *policy_group*

   如需完整的命令語法、請參閱手冊頁。您可以使用 _storage_object_modify 將不同原則群組套用至儲存物件的命令。

   下列命令會套用原則群組 pg-app2 磁碟區 app2：

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

4. 監控原則群組效能：

   qos statistics performance show

   如需完整的命令語法、請參閱手冊頁。

   > 監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示原則群組效能：

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. 監控工作負載效能：

   qos statistics workload performance show

   如需完整的命令語法、請參閱手冊頁。

   > 監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示工作負載效能：

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

> 您可以使用 `qos statistics workload latency show` 命令以檢視 QoS 工作負載的詳細延遲統計資料。

使用調適性**QoS**原則群組

您可以使用_Adaptive QoS_原則群組、自動調整處理量上限或樓層與磁碟區大小、並在磁碟區大小變更時、維持IOPS與TBs的比率。當您在大型部署中管理數百或數千個工作負載時、這是一項重大優勢。

開始之前

- 您必須執行 ONTAP 9.3 或更新版本。自ONTAP 功能性QoS原則群組開始提供、從功能性的9.3開始提供。
- 您必須是叢集管理員、才能建立原則群組。

關於這項工作

儲存物件可以是調適性原則群組或非調適性原則群組的成員、但不能同時是兩者。儲存物件的SVM和原則必須相同。儲存物件必須處於線上狀態。

調適性QoS原則群組永遠不會共用：定義的處理量上限或樓層會個別套用至每個成員的工作負載。

處理量限制與儲存物件大小的比率、取決於下列欄位的互動：

- `expected-iops` 是每個配置的 TB|GB 的最低預期 IOPS 。

> `expected-iops` 僅在 `AFF` 平台上保證。 `expected-iops` 只有當分層原則設定為「無」且雲端中沒有區塊時、 `FabricPool` 才保證適用。 `expected-iops` 保證不會與 `SnapMirror` 同步關係有關的磁碟區。

- `peak-iops` 是每個已分配或已使用的最大可能 IOPS TB|GB 。
- `expected-iops-allocation` 指定是將分配的空間（預設）還是已使用的空間用於預期的 IOPS 。

> `expected-iops-allocation` 可在 ONTAP 9.5 或更新版本中取得。不支援ONTAP 此功能。

- `peak-iops-allocation` 指定是使用分配的空間還是使用的空間（預設） `peak-iops`。

- `absolute-min-iops` 為 IOPS 的絕對最小值。您可以將此欄位用於非常小的儲存物件。它會同時取代兩者 `peak-iops` 和/或 `expected-iops` 何時 `absolute-min-iops` 大於計算值 `expected-iops`。

  例如、如果您設定 `expected-iops` 以 1 、 000 IOPS / TB 為單位、且磁碟區大小小於 1 GB `expected-iops` 將為分數 IOP 。計算所得的 `peak-iops` 將會是更小的一部分。您可以透過設定來避免這種情況 `absolute-min-iops` 至實際值。

- `block-size` 指定應用程式 I/O 區塊大小。預設值為 32K 。有效值為8K、16K、32K、64K、any。任何表示不會強制執行區塊大小。

有三個預設的調適性QoS原則群組可供使用、如下表所示。您可以將這些原則群組直接套用至磁碟區。

預設原則群組	預期IOPS / TB	IOPS / TB尖峰	絕對最小IOPS
`extreme`	6 、 144	12288/3	1000
`performance`	2 、 048	4 、 096	500
`value`	128/128	512	75

如果儲存物件包含物件或其子物件屬於原則群組、則無法將其指派給原則群組。下表列出限制。

如果您指派...	然後您就無法指派...
SVM到原則群組	SVM所包含的任何儲存物件至原則群組
磁碟區至原則群組	磁碟區包含SVM或任何子LUN至原則群組
LUN至原則群組	LUN包含磁碟區或SVM至原則群組
檔案至原則群組	檔案包含磁碟區或SVM至原則群組

步驟

1. 建立可調適的QoS原則群組：

   ```
   qos adaptive-policy-group create -policy group policy_group -vserver SVM
   -expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
   -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
   space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
   ```

   如需完整的命令語法、請參閱手冊頁。

   > `-expected-iops-allocation` 和 `-block-size` 可在 ONTAP 9.5 或更新版本中取得。上述選項不受ONTAP 支援於支援的版本不包括在內。

   下列命令會建立調適性 QoS 原則群組 `adpg-app1` 與 `-expected-iops` 設為 300 IOPS / TB 、 `-peak-iops` 設為 1 、 000 IOPS / TB 、 `-peak-iops-allocation` 設定為 `used-space`和 `-absolute-

`min-iops` 設為 50 IOPS ：

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. 將調適性QoS原則群組套用至磁碟區：

   `volume create -vserver SVM -volume volume -aggregate aggregate -size number_of TB|GB -qos-adaptive-policy-group policy_group`

   如需完整的命令語法、請參閱手冊頁。

   下列命令會套用調適性 QoS 原則群組 `adpg-app1` 至 Volume `app1`：

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

   下列命令會套用預設的調適性 QoS 原則群組 `extreme` 到新的 Volume `app4` 和現有的 Volume `app5`。為原則群組定義的處理量上限會套用至磁碟區 `app4` 和 `app5` 個別：

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

設定調適性原則群組範本

從 ONTAP 9.13.1 開始、您可以使用調適性原則群組範本、在 SVM 層級強制執行處理量樓層和天花板。

關於這項工作

- 調適性原則群組範本是預設原則 `apg1`。您可以隨時修改原則。只能使用 CLI 或 ONTAP REST API 設定、而且只能套用至現有的 SVM 。
- 調適性原則群組範本只會影響在設定原則之後、在 SVM 上建立或移轉到 SVM 的磁碟區。SVM 上的現有磁碟區會保留其現有狀態。

  如果停用調適性原則群組範本、 SVM 上的磁碟區會保留其現有原則。只有後續在 SVM 上建立或移轉到 SVM 的磁碟區、才會受到停用影響。

- 您無法在具有 QoS 原則群組的 SVM 上設定調適性原則群組範本。
- 調適性原則群組範本是專為 AFF 平台所設計。可在其他平台上設定調適性原則群組範本、但原則可能無法

強制執行最低處理量。同樣地、您也可以將調適性原則群組範本新增至 FabricPool Aggregate 中的 SVM 、或是新增至不支援最低處理量的 Aggregate 、但不會強制執行處理量區。

- 如果 SVM 是在 MetroCluster 組態或 SnapMirror 關係中、則會在鏡射 SVM 上強制執行調適性原則群組範本。

步驟

1. 修改 SVM 以套用調適性原則群組範本：
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. 確認已設定原則：
   `vserver show -fields qos-adaptive-policy-group`

使用Unified Manager監控叢集效能

有了VMware、您可以最大化可用度、並維持對NetApp VMware及VMware儲存基礎架構的控制、以提升擴充性、支援能力、效能及安全性。Active IQ Unified Manager AFF FAS

不間斷地監控系統健全狀況並傳送警示、讓您的組織能夠釋出IT員工資源。Active IQ Unified Manager您可以從單一儀表板立即檢視儲存狀態、並透過建議的行動來快速解決問題。

資料管理之所以能簡化、是因為您可以探索、監控及接收通知、主動管理儲存設備並快速解決問題。 由於您可以從單一儀表板監控數PB的資料、並大規模管理資料、因此可提升管理效率。

有了VMware、您就能跟上瞬息萬變的業務需求、運用效能資料和進階分析技術來最佳化效能。Active IQ Unified Manager 報告功能可讓您存取標準報告或建立自訂營運報告、以滿足企業的特定需求。

相關連結：

- "深入瞭解 Active IQ Unified Manager"
- "Active IQ Unified Manager for VMware 入門"
- "Active IQ Unified Manager for Linus 入門指南"
- "Active IQ Unified Manager for Windows 快速入門"

利用VMware技術監控叢集效能Cloud Insights

NetApp Cloud Insights 解決方案是一套監控工具、可讓您清楚掌握完整的基礎架構。利用VMware、您可以監控、疑難排解及最佳化所有資源、包括公有雲和私有資料中心。Cloud Insights

提供兩種版本Cloud Insights

支援NetApp Data Fabric資產的設計專門用於監控及最佳化。Cloud Insights它提供進階分析功能、可在FAS 環境中免費連接所有NetApp資源、包括HCI和All Flash更新（AFF 例如、英文）。

支援NetApp Data Fabric的基礎架構元件不僅著重於支援NetApp Data Fabric的基礎架構元件、也著重於多廠商與多雲端環境。Cloud Insights有了豐富的功能、您就能獲得超過100項服務與資源的支援。

在當今的世界中、從內部部署資料中心到多個公有雲的資源都能發揮效用、因此從應用程式本身到儲存陣列後端

磁碟的完整畫面是非常重要的。對應用程式監控的額外支援（例如Kafka、MongoDB和Ngin像）可提供您在最佳使用率和最佳風險緩衝區下運作所需的資訊和知識。

這兩種版本（基本版和標準版）都能與NetApp Active IQ Unified Manager 產品整合。使用 Active IQ Unified Manager 的客戶可以在 Cloud Insights 使用者介面中看到加入資訊。在 Active IQ Unified Manager 上發佈的通知不會被忽略、而且可以與 Cloud Insights 中的事件相關聯。換句話說、您將獲得兩全其美的優勢。

監控、疑難排解及最佳化所有資源

協助您大幅縮短解決問題的時間、避免問題影響終端使用者。Cloud Insights 它也能協助您降低雲端基礎架構成本。 透過可據以行動的情報來保護資料、可降低內部威脅的曝險。

從公有雲到資料中心、整個混合式基礎架構都能在單一位置清楚掌握。Cloud Insights 您可以立即建立相關的儀表板、以便根據您的特定需求進行自訂。您也可以建立特定且與組織需求相關的目標警示和條件警示。

進階異常偵測功能可協助您在問題發生之前主動修正問題。 您可以自動檢視資源爭用和降級、以快速還原受影響的工作負載。 透過自動建立的階層關係、您堆疊中不同元件之間的疑難排解速度更快。

您可以在整個環境中找出未使用或已放棄的資源、協助您找出適當規模調整基礎架構並最佳化整體支出的機會。

支援以視覺化方式呈現系統拓撲、以瞭解Kubernetes架構。Cloud Insights您可以監控Kubernetes叢集的健全狀況、包括發生問題的節點、並在發現問題時放大。

利用先進的機器學習和異常偵測功能、針對內部威脅提供可據以行動的情報、協助您保護組織資料、避免遭惡意或遭入侵的使用者濫用。Cloud Insights

支援使用支援視覺化Kubernetes指標、讓您完全瞭解Pod、節點和叢集之間的關係。Cloud Insights您可以評估叢集或正常運作的Pod的健全狀況、以及目前正在處理的負載、讓您能夠掌控K8S叢集、同時控制部署的健全狀況和成本。

相關連結

- "深入瞭解 Cloud Insights"
- "開始使用 Cloud Insights"

稽核記錄

如何執行稽核記錄**ONTAP**

稽核日誌中記錄的管理活動會包含在標準AutoSupport 版的功能表報告中、而EMS訊息中也會包含某些記錄活動。您也可以將稽核記錄轉送到指定的目的地、並使用CLI或Web瀏覽器來顯示稽核記錄檔。

從版本的《Sy9.11.1》開始ONTAP 、您可以使用System Manager來顯示稽核記錄內容。

從 ONTAP 9.12.1 開始、 ONTAP 會針對稽核記錄提供竄改警示。ONTAP 會執行每日背景工作、檢查 audit.log 檔案是否遭到竄改、如果發現任何已變更或竄改的記錄檔、則會傳送 EMS 警示。

系統會記錄叢集上執行的管理活動、例如發出的要求、觸發要求的使用者、使用者的存取方法、以及要求的時間。ONTAP

管理活動可以是下列其中一種類型：

- 設定要求、通常適用於非顯示命令或作業
  - 這些要求會在您執行時發出 `create`、 `modify`或 `delete` 例如命令。
  - 預設會記錄設定要求。
- Get要求、可擷取資訊並在管理介面中顯示
  - 這些要求會在您執行時發出 `show` 例如命令。
  - 依預設不會記錄 GET 要求、但您可以控制是否從 ONTAP CLI 傳送 GET 要求 (`-cliget`）、來自 ONTAP API (`-ontapiget`）、或來自 REST API (`-httpget`）會記錄在檔案中。

ONTAP 會在中記錄管理活動 `/mroot/etc/log/mlog/audit.log` 節點的檔案。這裏記錄了三個Shell中用於CLI命令的命令（即clusterShell、nodesell和非交互式系統Shell（不記錄交互式系統Shell命令）以及API命令。稽核記錄包含時間戳記、可顯示叢集中的所有節點是否都同步時間。

。 `audit.log` 檔案是由 AutoSupport 工具傳送給指定的收件者。您也可以將內容安全地轉送到您指定的外部目的地、例如Splunk或syslog伺服器。

。 `audit.log` 檔案會每日旋轉。當檔案大小達到100 MB時、也會進行旋轉、並保留先前的48個複本（最多總共49個檔案）。稽核檔案執行每日旋轉時、不會產生任何EMS訊息。如果稽核檔案因為超過檔案大小限制而旋轉、則會產生EMS訊息。

變更以稽核**ONTAP** 記錄功能。**9.**

從 ONTAP 9 開始 `command-history.log` 檔案取代為 `audit.log`和 `mgwd.log` 檔案不再包含稽核資訊。如果您要升級ONTAP 至VMware版、請檢閱任何參考舊版檔案及其內容的指令碼或工具。

升級至 ONTAP 9 之後、即為現有的 `command-history.log` 檔案會保留。它們會以新的方式旋轉（刪除）`audit.log` 檔案會在中旋轉（建立）。

檢查的工具和指令碼 `command-history.log` 檔案可能會繼續運作、因為有的軟式連結 `command-history.log` 至 `audit.log` 在升級時建立。不過、檢查的工具和指令碼 `mgwd.log` 檔案將會失敗、因為該檔案不再包含稽核資訊。

此外、由於下列項目不被視為有用、導致不必要的記錄活動、因此在更新版本的版本中、不再包含稽核記錄：ONTAP

- 內部命令由ONTAP 執行（也就是、其中username=root）
- 命令別名（與指向的命令分開）

從ONTAP 功能支援的第9部分開始、您可以使用TCP和TLS傳輸協定、將稽核記錄安全地傳輸到外部目的地。

顯示稽核記錄內容

您可以顯示叢集的內容 `/mroot/etc/log/mlog/audit.log` 使用 ONTAP CLI 、系統管理員或網頁瀏覽器來建立檔案。

叢集的記錄檔項目包括：

時間

記錄項目時間戳記。

應用程式

用於連線至叢集的應用程式。可能的值範例如下 `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, 和 `service-processor`。

使用者

遠端使用者的使用者名稱。

州/省

稽核要求的目前狀態、可能是 `success`, `pending`, 或 `error`。

訊息

可選欄位、其中可能包含錯誤或命令狀態的其他資訊。

工作階段**ID**

接收要求的工作階段ID。每個SSH _S階段 作業_都會指派一個工作階段ID、而每個HTTP、ONTAPI或SNMP _REQUER__都會指派一個唯一的工作階段ID。

儲存 **VM**

使用者連線的SVM。

範圍

顯示 `svm` 當要求位於資料儲存 VM 上時、否則會顯示 `cluster`。

命令**ID**

在CLI工作階段中收到的每個命令的ID。這可讓您建立要求與回應的關聯。ZAPI、HTTP和SNMP要求沒有命令ID。

您可以從ONTAP 「系統ONTAP 管理員」的「系統管理程式」中、從「系統瀏覽器」、以「版本9.11.1」開頭、從「版本資訊」CLI顯示叢集的記錄項目。

系統管理員

- 若要顯示詳細目錄、請選取*事件與工作>稽核記錄*。+
  每一欄都有篩選、排序、搜尋、顯示和庫存類別的控制項。詳細目錄可下載為Excel活頁簿。
- 若要設定篩選條件、請按一下右上方的 * 篩選 * 按鈕、然後選取所需的欄位。+
  您也可以按一下工作階段 ID 連結、檢視在發生故障的工作階段中執行的所有命令。

CLI

若要顯示從叢集中多個節點合併的稽核項目、請輸入：

```
security audit log show [parameters]
```

您可以使用 `security audit log show` 用於顯示個別節點的稽核項目、或是從叢集中的多個節點合併的命令。您也可以顯示的內容 `/mroot/etc/log/mlog` 使用 Web 瀏覽器在單一節點上建立目錄。
如需詳細資料、請參閱手冊頁。

網頁瀏覽器

您可以顯示的內容 `/mroot/etc/log/mlog` 使用 Web 瀏覽器在單一節點上建立目錄。 "瞭解如何使用網頁瀏覽器存取節點的記錄檔、核心傾印檔和MIBA檔案"。

管理稽核取得要求設定

雖然預設會記錄設定要求、但不會記錄取得要求。不過、您可以控制是否從 ONTAP HTML 傳送 GET 要求 (`-httpget`） 、 ONTAP CLI (`-cliget`）或 ONTAP API (`-ontapiget`）會記錄在檔案中。

您可以從ONTAP 「系統ONTAP 管理程式」修改稽核記錄設定、從「系統管理程式」開始修改從「版本9.11.1」開始的記錄。

系統管理員

1. 選擇*事件與工作>稽核記錄*。
2. 按一下 ⚙ 在右上角、選擇要新增或移除的要求。

CLI

- 若要指定從 ONTAP CLI 或 API 取得要求應記錄在稽核記錄檔（ audit.log 檔案）中、除了預設的 Set 要求外、請輸入：
  ```
  security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget
  {on|off}]
  ```
- 若要顯示目前的設定、請輸入：
  ```
  security audit show
  ```

如需詳細資料、請參閱手冊頁。

管理稽核記錄目的地

您最多可將稽核記錄轉送至10個目的地。例如、您可以將記錄轉送至Splunk或syslog伺服

器、以供監控、分析或備份之用。

關於這項工作

若要設定轉送、您必須提供syslog或Splunk主機的IP位址、其連接埠號碼、傳輸傳輸傳輸傳輸協定、以及用於轉送記錄的syslog工具。 "深入瞭解syslog工具"。

您可以選取下列其中一個傳輸值：

未加密的**udp**

無安全性的使用者資料包傳輸協定（預設）

TCP未加密

傳輸控制傳輸協定、無安全性

TCP加密

傳輸層安全性（ TLS ） + 的傳輸控制傳輸協定
選取 TCP 加密傳輸協定時、可使用 * 驗證伺服器 * 選項。

您可以從ONTAP 「系統ONTAP 管理程式」從「功能性CLI」轉寄稽核記錄、從「功能性功能」開始、從「功能性功能」開始。

系統管理員

- 若要顯示稽核記錄目的地、請選取*叢集>設定*。+
  記錄目的地的計數會顯示在 * 通知管理方塊 * 中。按一下 ⋮ 以顯示詳細資料。
- 若要新增、修改或刪除稽核記錄目的地、請選取*事件與工作>稽核記錄*、然後按一下畫面右上角的*管理稽核目的地*。+
  按一下 + Add 或按一下 ⋮ 在*主機位址*欄中編輯或刪除項目。

CLI

1. 針對您要轉送稽核記錄的每個目的地、指定目的地IP位址或主機名稱及任何安全性選項。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - 如果是 `cluster log-forwarding create` 命令無法 ping 目的主機以驗證連線、命令失敗並顯示錯誤。雖然不建議使用、但請使用 `-force` 使用命令的參數會略過連線驗證。
   - 當您設定時 `-verify-server` 參數至 `true`，記錄轉送目的地的身分識別是透過驗證其憑證來驗證。您可以將值設為 `true` 僅當您選取時 `tcp-encrypted` 中的值 `-protocol` 欄位。

2. 使用驗證目的地記錄是否正確 `cluster log-forwarding show` 命令。

```
cluster1::> cluster log-forwarding show

                                                    Verify Syslog
Destination Host           Port   Protocol         Server Facility
-------------------------- ------ --------         ------ --------
192.168.123.96             514    udp-unencrypted  false  user
192.168.123.98             514    tcp-encrypted    true   user
2 entries were displayed.
```

如需詳細資料、請參閱手冊頁。

AutoSupport

使用**AutoSupport System Manager**管理各種功能

您可以使用系統管理員來管理 AutoSupport 帳戶的設定。

您可以執行下列程序：

檢視**AutoSupport** 畫面設定

您可以使用System Manager來檢視AutoSupport 您的還原帳戶設定。

步驟

1. 在System Manager中、按一下*叢集>設定*。

   在* AutoSupport 《》（《*》）區段中、會顯示下列資訊：

   - 狀態
   - 傳輸傳輸傳輸協定
   - Proxy伺服器
   - 寄件者電子郵件地址

2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 更多選項 * 。

   畫面上會顯示AutoSupport 有關「還原連線」和電子郵件設定的其他資訊。此外、也會列出訊息的傳輸歷程記錄。

產生並傳送**AutoSupport** 不一樣的資料

在System Manager中、您可以啟動AutoSupport 產生功能不全的訊息、並從收集資料的叢集節點或節點中進行選擇。

步驟

1. 在System Manager中、選取*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 產生並傳送 * 。
3. 輸入主旨。
4. 選取 * 收集資料來源 * 下的核取方塊、以指定要從中收集資料的節點。

測試連線**AutoSupport** 至功能不正常的情況

您可以從System Manager傳送測試訊息來驗證連線AutoSupport 至Sytra。

步驟

1. 在System Manager中、按一下*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 測試連線 * 。
3. 輸入訊息的主旨。

啟用或停用**AutoSupport** 功能

AutoSupport 為 NetApp 客戶提供備受肯定的商業效益、包括主動識別可能的組態問題、並加速解決支援案例。在新系統中、 AutoSupport 預設為啟用。如有必要、您可以使用系統管理員來停用 AutoSupport 監控儲存系統健全狀況並傳送通知訊息的功能。 停用後、您可以再次啟用AutoSupport 此功能。

關於這項工作

停用 AutoSupport 之前、請注意您正在關閉 NetApp 呼叫主機系統、您將會失去下列好處：

- * 健全狀況監控 * ： AutoSupport 會監控儲存系統的健全狀況、並將通知傳送給技術支援部門和您的內部支援組織。
- * 自動化 * ： AutoSupport 可自動報告支援案例。大多數的支援案例都會在客戶發現問題之前自動開啟。
- * 更快的解析度 * ：與不傳送 AutoSupport 資料的系統案例相比、傳送 AutoSupport 資料的系統在一半時間內就能解決其支援案例。
- * 更快的升級 * ： AutoSupport 為客戶的自助服務工作流程提供強大功能、例如系統管理員中的版本升級、附加元件、續約和韌體更新自動化。
- * 更多功能 * ：其他工具中的某些功能只有在啟用 AutoSupport 時才會運作、例如 BlueXP 中的某些工作流程。

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 禁用 * 。
3. 如果您想要再次啟用 AutoSupport 、請在 * AutoSupport * 區段中選取 ⋮，然後選擇 **Enable** 。

抑制支援案例的產生

從ONTAP 《支援要求》（Sytr9.10.1）開始、您可以使用System Manager傳送要求AutoSupport 到《支援案例》、以抑制支援案例的產生。

關於這項工作

若要抑制支援案例的產生、請指定您要抑制的節點和小時數。

如果AutoSupport 您不想在系統上執行維護時建立自動化案例、那麼抑制支援案例將特別有用。

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 抑制支援案例產生 * 。
3. 輸入您要進行抑制的時數。
4. 選取您要進行抑制的節點。

恢復產生支援案例

從ONTAP 《支援》9.10.1開始、您可以使用System Manager、AutoSupport 在受到抑制的情況下、從《支援案例》中恢復產生支援案例。

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 恢復支援案例產生 * 。
3. 選取您要恢復產生的節點。

編輯**AutoSupport** 功能設定

您可以使用System Manager修改AutoSupport 您的帳戶的連線和電子郵件設定。

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮，然後選擇 * 更多選項 * 。
3. 在 * 連線 * 區段或 * 電子郵件 * 區段中、選取 Edit 可修改任一部分的設置。

使用CLI管理AutoSupport 功能

管理AutoSupport 功能概述

此機制可主動監控系統健全狀況、並自動傳送訊息給NetApp技術支援、您的內部支援組織及支援合作夥伴。AutoSupport雖然根據預設會啟用技術支援的支援功能、但您必須設定正確的選項、並擁有有效的郵件主機、才能將訊息傳送給內部支援組織。AutoSupport

只有叢集管理員才能執行AutoSupport 資訊管理。儲存虛擬機器（SVM）管理員無法存取AutoSupport 任何功能。

當您第一次設定儲存系統時、預設會啟用此功能。AutoSupport啟用此功能24小時後、系統會開始傳送訊息給技術支援人員。AutoSupport AutoSupport您可以透過升級或還原系統、修改AutoSupport 版本的功能表組態、或將系統時間變更為24小時以外的時間、來縮短24小時的時間。

> 您可以AutoSupport 隨時停用、但應保持啟用狀態。啟用AutoSupport 支援功能可大幅加快問題的判斷速度、並在儲存系統發生問題時予以解決。根據預設、系統會收集AutoSupport 並儲存這些資訊到本機、即使您停用AutoSupport 了某些功能。

如需有關 AutoSupport 的詳細資訊，請參閱 NetApp 支援網站。

相關資訊

- "NetApp支援"
- "深入瞭AutoSupport 解ONTAP 有關使用者可在列舉的功能表中使用的功能"

使用 AutoSupport 與 Active IQ Digital Advisor

這個功能的元件會收集遙測資料並傳送給分析人員。AutoSupport ONTAPActive IQ Digital Advisor 會分析來自 AutoSupport 的資料，並提供主動式防護與最佳化功能。利用人工智慧、Active IQ 即可識別潛在問題、並在問題影響企業之前協助您解決問題。

透過雲端型入口網站和行動應用程式、提供可據以行動的預測分析和主動式支援、讓您能夠在全球混合雲中最佳化資料基礎架構。Active IQ所有擁有有效的NetApp客戶都能從NetApp獲得資料導向的見解和建議Active IQ （功能因產品和支援層而異）SupportEdge 。

以下是Active IQ 您可以利用下列功能來執行的作業：

- 規劃升級。可識別環境中的問題、這些問題可透過升級至更新版本的VMware知識來解決、而升級顧問元件則可協助您規劃成功的升級方案。Active IQ ONTAP
- 檢視系統健全狀況。您的「不健全狀況」儀表板會回報任何問題、並協助您修正這些問題。Active IQ監控系統容量、確保儲存空間永遠不會耗盡。檢視系統的支援案例。
- 管理效能：顯示系統效能的時間比您在System Manager中看到的更長。Active IQ找出影響您效能的組態和

系統問題。

- 最大化效率。檢視儲存效率指標、找出在更少空間中儲存更多資料的方法。
- 檢視庫存與組態。顯示完整的庫存、軟體和硬體組態資訊。Active IQ查看服務合約何時到期並續約、以確保您仍享有支援。

相關資訊

"NetApp 文件：Active IQ Digital Advisor"

"產品Active IQ 發表"

"部門服務SupportEdge"

何時及何處**AutoSupport** 傳送資訊

根據訊息類型、將訊息傳送給不同的收件者。AutoSupport瞭解AutoSupport 何時何地發送消息可協助您瞭解透過電子郵件接收的訊息、或是在Active IQ 本網站上查看（先前稱為My AutoSupport 原地）。

除非另有指定、否則下表中的設定是的參數 `system node autosupport modify` 命令。

事件觸發的訊息

當系統發生需要採取修正行動的事件時AutoSupport 、則會自動傳送事件觸發的訊息。

訊息傳送時	訊息傳送位置
回應EMS中的觸發事件AutoSupport	中指定的位址 `-to` 和 `-noteto`。（僅會傳送影響服務的重大事件。） 中指定的位址 `-partner-address` 技術支援、如果 `-support` 設為 `enable`

排程的訊息

自動定期傳送數則訊息。AutoSupport

訊息傳送時	訊息傳送位置
每日（依預設、於上午12：00之間傳送和上午1：00作為記錄訊息）	中指定的位址 `-partner-address` 技術支援、如果 `-support` 設為 `enable`
每日（依預設、於上午12：00之間傳送和上午1：00效能訊息） `-perf` 參數設定為 `true`	合作夥伴地址中指定的地址 技術支援、如果 `-support` 設為 `enable`

訊息傳送時	訊息傳送位置
每週（依預設、星期日的傳送時間為上午12：00和上午1：00）	中指定的位址 `-partner-address` 技術支援、如果 `-support` 設為 `enable`

手動觸發的訊息

您可以手動初始化AutoSupport 或重新傳送一個消息。

訊息傳送時	訊息傳送位置
您可以使用手動初始化訊息 `system node autosupport invoke` 命令	如果使用指定 URI `-uri` 中的參數 `system node autosupport invoke` 命令會將訊息傳送至該 URI 。 如果 `-uri` 如果省略、訊息會傳送至中指定的位址 `-to` 和 `-partner-address`。此訊息也會傳送給技術支援人員、如果有的話 `-support` 設為 `enable`。
您可以使用手動初始化訊息 `system node autosupport invoke-core-upload` 命令	如果使用指定 URI `-uri` 中的參數 `system node autosupport invoke-core-upload` 命令會將訊息傳送至該 URI 、核心傾印檔案會上傳至 URI 。 如果 `-uri` 在中省略 `system node autosupport invoke-core-upload` 命令會將訊息傳送給技術支援人員、核心傾印檔案會上傳至技術支援網站。 這兩種情況都需要這樣做 `-support` 設為 `enable` 和 `-transport` 設為 `https` 或 `http`。 由於核心傾印檔案太大、因此訊息不會傳送至中指定的位址 `-to` 和 `-partner-addresses` 參數。
您可以使用手動初始化訊息 `system node autosupport invoke-performance-archive` 命令	如果使用指定 URI `-uri` 中的參數 `system node autosupport invoke-performance-archive` 命令會將訊息傳送至該 URI 、效能封存檔案會上傳至 URI 。 如果 `-uri` 在中省略 `system node autosupport invoke-performance-archive`、訊息會傳送給技術支援、效能歸檔檔案會上傳至技術支援網站。 這兩種情況都需要這樣做 `-support` 設為 `enable` 和 `-transport` 設為 `https` 或 `http`。 由於效能歸檔檔案的大小很大、因此訊息不會傳送至中指定的位址 `-to` 和 `-partner-addresses` 參數。

訊息傳送時	訊息傳送位置
您可以使用手動重新傳送過去的訊息 `system node autosupport history retransmit` 命令	僅限您在中指定的 URI `-uri` 的參數 `system node autosupport history retransmit` 命令

由技術支援所觸發的訊息

技術支援人員AutoSupport 可以使用AutoSupport 「支援不受需求」功能、向支援中心索取訊息。

訊息傳送時	訊息傳送位置
當獲取交付指示以產生新的資訊提供訊息時AutoSupport AutoSupport	中指定的位址 `-partner-address` 技術支援、如果 `-support` 設為 `enable` 和 `-transport` 設為 `https`
當獲得傳遞指示以重新傳送過去的消息時AutoSupport AutoSupport	技術支援、如果 `-support` 設為 `enable` 和 `-transport` 設為 `https`
當您取得交付指示、以產生新的資訊檔來上傳核心傾印或效能歸檔檔案時AutoSupport AutoSupport	技術支援、如果 `-support` 設為 `enable` 和 `-transport` 設為 `https`。核心傾印或效能歸檔檔案會上傳至技術支援網站。

如何建立及傳送事件觸發的訊息**AutoSupport**

當EMS處理觸發事件時、會建立事件觸發的功能性訊息。AutoSupport AutoSupport事件觸發AutoSupport 的消息可警示收件者需要採取修正行動的問題、並僅包含與問題相關的資訊。您可以自訂要納入哪些內容、以及接收訊息的人員。

使用下列程序來建立及傳送事件觸發的功能性訊息：AutoSupport AutoSupport

1. 當EMS處理觸發事件時、EMS會傳送AutoSupport EISO要求。

   觸發事件是 AutoSupport 目的地和名稱開頭為的 EMS 事件 `callhome.` 前置碼：

2. 建立事件觸發的消息。AutoSupport AutoSupport

   從與觸發程序相關的子系統收集基本資訊和疑難排解資訊、以建立訊息、其中僅包含與觸發事件相關的資訊。AutoSupport

   每個觸發程序都會有一組預設的子系統。不過、您可以選擇使用將其他子系統與觸發程式建立關聯 `system node autosupport trigger modify` 命令。

3. AutoSupport 會將事件觸發的 AutoSupport 訊息傳送給定義的收件者 `system node autosupport modify` 命令 `-to`、 `-noteto`、 `-partner-address`和 `-support` 參數。

   您可以使用啟用和停用特定觸發程序的 AutoSupport 訊息傳送 `system node autosupport trigger modify` 命令 `-to` 和 `-noteto` 參數。

針對特定事件傳送的資料範例

。 `storage shelf PSU failed` EMS 事件會觸發訊息、其中包含 Mandatory 、 Log Files 、 Storage 、 RAID 、 HA 、 平台、網路子系統、以及來自 Mandatory 、 Log Files 和 Storage 子系統的疑難排解資料。

您決定要在任何為回應未來而傳送的 AutoSupport 訊息中包含 NFS 相關資料 `storage shelf PSU failed` 事件。您可以輸入下列命令來啟用 NFS 的疑難排解層級資料 `callhome.shlf.ps.fault` 事件：

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

請注意 `callhome.` 首碼會從刪除 `callhome.shlf.ps.fault` 使用時的事件 `system node autosupport trigger` 命令、或當 AutoSupport 和 EMS 事件在 CLI 中參照時。

各種類型的消息及其內容**AutoSupport**

支援子系統的狀態資訊包含在內。AutoSupport瞭解AutoSupport 包含哪些資訊可協助您解讀或回覆您在電子郵件中收到的訊息、或是Active IQ 在本網站上檢視（先前稱為「我AutoSupport 的」）。

訊息類型	訊息所包含的資料類型
事件觸發	包含事件發生所在特定子系統相關內容敏感資料的檔案
每日	記錄檔
效能	過去24小時內取樣的效能資料
每週	組態與狀態資料
由觸發 `system node autosupport invoke` 命令	取決於中指定的值 `-type` 參數： • `test` 傳送含有一些基本資料的使用者觸發訊息。 此訊息也會觸發技術支援人員使用自動回覆電子郵件至任何指定的電子郵件地址 `-to` 選項、讓您確認正在接收 AutoSupport 訊息。 • `performance` 傳送效能資料。 • `all` 傳送使用者觸發的訊息、其中包含一組類似每週訊息的完整資料、包括每個子系統的疑難排解資料。 技術支援部門通常會要求提供此訊息。

訊息類型	訊息所包含的資料類型
由觸發 `system node autosupport invoke-core-upload` 命令	節點的核心傾印檔案
由觸發 `system node autosupport invoke-performance-archive` 命令	效能歸檔檔案的指定時間段
由AutoSupport NetApp按需觸發	根據需求、可索取新訊息或過去訊息：AutoSupport • 視 AutoSupport 集合類型而定、可以是新訊息 `test`、 `all`或 `performance`。 • 過去的訊息取決於重新傳送的訊息類型。 AutoSupport OnDemand 可要求產生新訊息，並將下列檔案上傳至 NetApp 支援網站："mysupport.netapp.com"： • 核心傾印 • 效能歸檔

什麼是子系統**AutoSupport**

每個子系統都提供AutoSupport 基本的疑難排解資訊、這些資訊可用於資訊的傳達。每個子系統也會與觸發事件相關聯、AutoSupport 讓資訊僅從子系統收集與觸發事件相關的資訊。

此功能可收集內容相關的內容。AutoSupport您可以使用檢視子系統的相關資訊、並觸發事件 `system node autosupport trigger show` 命令。

規模與時間預算**AutoSupport**

根據子系統來收集資訊、並針對每個子系統的內容實施規模和時間預算。AutoSupport隨著儲存系統的成長、AutoSupport 支援不必要的資源來控制AutoSupport 不必要的資料負載、進而提供可擴充的AutoSupport 功能來提供不必要的資料。

如果子系統內容超出其大小或時間預算、則停止收集資訊並將其刪減。AutoSupport AutoSupport如果內容無法輕易刪減（例如二進位檔案）、AutoSupport 請將內容還原。

只有在NetApp支援部門要求時、您才應該修改預設的規模和時間預算。您也可以使用檢閱子系統的預設大小和時間預算 `autosupport manifest show` 命令。

以事件觸發**AutoSupport** 的資訊訊息傳送檔案

事件觸發AutoSupport 的部分訊息僅包含子系統的基本資訊和疑難排解資訊、這些子系統與導致AutoSupport 產生訊息的事件有關。特定資料可協助NetApp支援與支援合作夥伴疑難排解問題。

使用下列條件來控制事件觸發的消息中的內容：AutoSupport AutoSupport

- 包含哪些子系統

  資料會分組為子系統、包括常用子系統、例如記錄檔、以及特定子系統、例如RAID。每個事件都會觸發一則訊息、其中只包含來自特定子系統的資料。

- 每個隨附子系統的詳細資料層級

  每個隨附子系統的資料均以基本或疑難排解層級提供。

您可以使用檢視所有可能的事件、並決定每個事件的相關訊息中包含哪些子系統 `system node autosupport trigger show` 命令 `-instance` 參數。

除了每個事件預設包含的子系統之外、您也可以使用在基本或疑難排解層級新增其他子系統 `system node autosupport trigger modify` 命令。

以**AutoSupport** 消息形式傳送的記錄檔

支援部門的技術人員可利用包含數個重要記錄檔的資訊、來檢閱最近的系統活動。AutoSupport

啟用「記錄檔」子系統時、所有AutoSupport 類型的資訊均可能包含下列記錄檔：

記錄檔	檔案中包含的資料量
• 的記錄檔 `/mroot/etc/log/mlog/` 目錄 • 訊息記錄檔	自從上次AutoSupport 顯示的資訊不全訊息後、記錄中只會新增一行、直到達到指定的上限為止。如此可確保AutoSupport 不重疊的資料、能夠產生獨特且相關的資訊。 （合作夥伴提供的記錄檔為例外、合作夥伴則包含允許的最大資料量。）
• 的記錄檔 `/mroot/etc/log/shelflog/` 目錄 • 的記錄檔 `/mroot/etc/log/acp/` 目錄 • 事件管理系統（EMS）記錄資料	最新的資料行、最多可達指定的上限。

在不同版本的版本之間、可變更不含任何資訊的訊息內容AutoSupport 。ONTAP

以每週**AutoSupport** 更新訊息傳送的檔案

每週AutoSupport 更新訊息包含額外的組態和狀態資料、有助於追蹤系統隨時間變化。

以下資訊會以每週AutoSupport 的資訊傳送：

- 每個子系統的基本資訊
- 所選內容 `/mroot/etc` 目錄檔案

- 記錄檔
- 提供系統資訊的命令輸出
- 其他資訊、包括複寫資料庫（RDB）資訊、服務統計資料等

如何透過技術支援取得隨需供應指示**AutoSupport**

AutoSupport OnDemand 會定期與技術支援人員通訊，以取得傳送、重新傳送、拒絕 AutoSupport 訊息以及將大型檔案上傳至 NetApp 支援網站的交付指示。利用支援的支援功能、可隨需傳送不需等待每週執行的更新訊息。AutoSupport AutoSupport AutoSupport

根據需求提供下列元件：AutoSupport

- 在每個節點上執行的隨需用戶端AutoSupport
- 駐留在技術支援中的隨需服務AutoSupport

《支援需求》用戶端會定期輪詢《支援需求》服務、以取得技術支援的交付指示。AutoSupport AutoSupport例如、技術支援人員可以使用AutoSupport 《支援不再需求的支援服務」來要求AutoSupport 產生新的資訊。當《不再需求》用戶端輪詢《不再需求》服務時、用戶端會取得交付指示、並根據要求隨需傳送新的《不滿意》訊息。AutoSupport AutoSupport AutoSupport

根據預設、系統會啟用「隨需」AutoSupport 。不過AutoSupport 、由於某些AutoSupport 功能不全、所以需要使用某些功能、才能繼續與技術支援人員溝通。當符合下列需求時、即可自動與技術支援人員通訊：AutoSupport

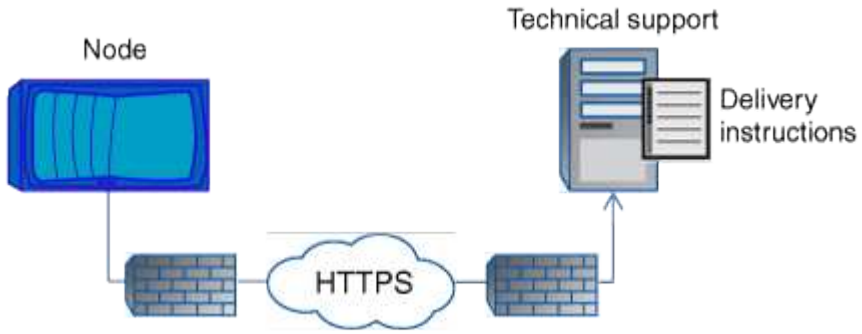
- 啟用了支援。AutoSupport
- 將支援功能設定為傳送訊息給技術支援。AutoSupport
- 將支援使用HTTPS傳輸傳輸傳輸協定。AutoSupport

《支援不限需求的用戶端」AutoSupport 會將HTTPS要求傳送至AutoSupport 傳送該訊息的相同技術支援位置。不接受傳入連線的不適用。AutoSupport

> 支援部門使用「zhi」使用者帳戶與技術支援部門溝通。AutoSupport AutoSupport無法刪除此帳戶。ONTAP

如果您想要停用 AutoSupport OnDemand 、但仍保持啟用 AutoSupport 、請使用命令： `system node autosupport modify -ondemand-state disable`。

下圖顯示AutoSupport 瞭如何使用支援功能向技術支援部門傳送HTTPS要求、以取得交付指示。



交付指示可包括AutoSupport 要求執行下列事項的申請表：

- 產生新AutoSupport 的消息。

  技術支援部門可能會要求提供AutoSupport 新的資訊、以協助分類問題。

- 產生新的 AutoSupport 訊息，將核心傾印檔案或效能歸檔檔案上傳至 NetApp 支援網站。

  技術支援人員可能會要求核心傾印或效能歸檔檔案、以協助分類問題。

- 重新傳輸先前產生AutoSupport 的消息。

  如果由於交付失敗而未收到訊息、則會自動執行此要求。

- 停用針對AutoSupport 特定觸發事件傳送的功能。

  技術支援可能會停用未使用的資料交付。

透過電子郵件傳送的不完整訊息結構**AutoSupport**

當以電子郵件傳送某封消息時、該訊息會有標準主旨、簡短本文、以及以7z檔案格式傳送的大型附件、其中包含該資料。AutoSupport

> 如果將BIOS設定為隱藏私有資料、則會在標頭、主旨、本文及附件中省略或遮罩某些資訊、例如主機名稱。AutoSupport

主旨

由S不明 機制傳送的訊息主旨行AutoSupport 包含一個文字字串、可識別通知的原因。主旨行的格式如下：

系統名稱（訊息）_嚴重性_的HA群組通知

- _System_Name_是主機名稱或系統ID、視AutoSupport 乎整個系統的組態而定

本文

本文介紹下列資訊：AutoSupport

- 訊息的日期和時間戳記
- 產生訊息的節點上的版本ONTAP
- 產生訊息之節點的系統ID、序號和主機名稱
- 序列號AutoSupport
- SNMP聯絡人名稱與位置（若有指定）
- HA合作夥伴節點的系統ID和主機名稱

附加檔案

AutoSupport 訊息中的關鍵資訊包含在壓縮成 7z 檔案的檔案中 `body.7z` 並附加至訊息。

附件中包含的檔案是特定AutoSupport 於類型的消息。

支援的嚴重性類型**AutoSupport**

支援訊息的嚴重性類型可協助您瞭解每則訊息的用途、例如提請立即注意緊急問題、或僅提供資訊。AutoSupport

訊息具有下列嚴重性之一：

- 警示：警示訊息指出、如果您未採取任何行動、可能會發生更高層級的事件。

  您必須在24小時內針對警示訊息採取行動。

- 緊急：發生中斷時會顯示緊急訊息。

  您必須立即對緊急訊息採取行動。

- 錯誤：錯誤情況指出若您忽略、可能會發生什麼情況。
- 通知：正常但重大的情況。
- 資訊：資訊訊息提供問題的詳細資料、您可以忽略。
- 偵錯：偵錯層級訊息提供您應執行的指示。

如果您的內部支援組織透過AutoSupport 電子郵件接收到不確定訊息、嚴重性會顯示在電子郵件訊息的主旨行。

使用需求**AutoSupport**

您必須搭配使用 HTTPS 搭配 TLSv1.2 或安全 SMTP 、才能交付 AutoSupport 訊息、以提供最佳安全性、並支援所有最新的 AutoSupport 功能。任何其他傳輸協定所傳送的 AutoSupport 訊息都會遭到拒絕。

支援的傳輸協定

所有這些傳輸協定都會根據名稱解析的位址系列、在IPv4或IPv6上執行。

傳輸協定與連接埠	說明
連接埠443上的HTTPS	這是預設的傳輸協定。您應該盡可能使用此功能。 此傳輸協定支援AutoSupport 以「隨需支援」和上傳大型檔案。 除非停用驗證、否則遠端伺服器的憑證會根據根憑證進行驗證。 交付使用 HTTPS Put 要求。使用PUT時、如果傳輸期間要求失敗、則要求會在停止處重新啟動。如果接收要求的伺服器不支援 Put 、則交付會使用 HTTPS POST 要求。

傳輸協定與連接埠	說明
連接埠 80 上的 HTTP	此傳輸協定優先於SMTP。 此傳輸協定支援上傳大型檔案、但AutoSupport 不支援不支援使用 交付使用 HTTPS Put 要求。使用PUT時、如果傳輸期間要求失敗、則要求會在停止處重新啟動。如果接收要求的伺服器不支援 Put 、則交付會使用 HTTPS POST 要求。
連接埠25或其他連接埠上的SMTP	只有在網路連線不允許 HTTPS 時、才應使用此傳輸協定。 預設的連接埠值為25、但AutoSupport 您可以設定使用不同的連接埠。 使用SMTP時、請謹記下列限制： • 不支援以隨需提供和上傳大型檔案。AutoSupport • 資料未加密。 SMTP以純文字傳送資料、AutoSupport 讓您輕鬆攔截及讀取消息中的文字。 • 訊息長度和行長的限制可以引進。

如果您為AutoSupport 內部支援組織或支援合作夥伴組織設定特定電子郵件地址的功能、這些訊息一律會由SMTP傳送。

例如、如果您使用建議的傳輸協定來傳送訊息給技術支援、而且您也想要傳送訊息給內部支援組織、則訊息會分別使用HTTPS和SMTP傳輸。

此功能可限制每個傳輸協定的最大檔案大小。AutoSupportHTTP和HTTPS傳輸的預設設定為25 MB。預設的SMTP傳輸設定為5 MB。如果AutoSupport 不符合設定限制的情況下顯示的訊息大小、AutoSupport 那麼就會盡可能傳達訊息內容。您可以透過修改AutoSupport 功能區組態來編輯最大大小。請參閱 `system node autosupport modify` 詳細資訊請參閱手冊頁。

> 當您產生並傳送 AutoSupport 訊息，以將核心傾印或效能歸檔檔案上傳至 NetApp 支援網站或指定 URI 時，AutoSupport 會自動置換 HTTPS 和 HTTP 傳輸協定的檔案大小上限。自動置換只有在您使用上傳檔案時才適用 `system node autosupport invoke-core-upload` 或 `system node autosupport invoke-performance-archive` 命令。

組態需求

視您的網路組態而定、 HTTPS 傳輸協定可能需要額外的 Proxy URL 組態。如果 HTTPS 要傳送 AutoSupport 訊息給技術支援、而且您有代理伺服器、則必須識別該代理的 URL 。如果Proxy使用預設連接埠以外的連接埠（即3128）、您可以指定該Proxy的連接埠。您也可以指定Proxy驗證的使用者名稱和密碼。

如果您使用SMTP傳送AutoSupport 不必要訊息給內部支援組織或技術支援部門、則必須設定外部郵件伺服器。

儲存系統無法做為郵件伺服器運作、您的站台需要外部郵件伺服器才能傳送郵件。郵件伺服器必須是在SMTP連接埠（25）或其他連接埠上接聽的主機、而且必須設定為傳送和接收8位元的多用途網際網路郵件延伸（MIME）編碼。範例郵件主機包括執行SMTP伺服器的UNIX主機、例如：endmail程式和執行Microsoft Exchange伺服器的Windows伺服器。您可以擁有一或多個郵件主機。

設定**AutoSupport** 功能

您可以控制AutoSupport 是否及如何將資訊傳送至技術支援部門和內部支援組織、然後測試組態是否正確。

關於這項工作

在發行版的更新版本中、您可以同時在叢集的所有節點上啟用及修改其組態。ONTAP AutoSupport當新節點加入叢集時、節點AutoSupport 會自動繼承叢集組態。您不需要個別更新每個節點上的組態。

> 從 ONTAP 9.5 開始、就是的範圍 `system node autosupport modify` 命令適用於整個叢集。AutoSupport 組態會在叢集中的所有節點上修改、即使在 `-node` 已指定選項。此選項會被忽略、但會保留此選項、以供CLI向後相容。
>
> 在 ONTAP 9.4 及更早版本中、的範圍是 `system node autosupport modify` 命令是特定於節點的。應該在叢集中的每個節點上修改此組態。AutoSupport

根據預設、AutoSupport 每個節點上都會啟用支援功能、以便使用HTTPS傳輸傳輸傳輸協定將訊息傳送給技術支援。

您必須搭配使用 HTTPS 搭配 TLSv1.2 或安全 SMTP 、才能交付 AutoSupport 訊息、以提供最佳安全性、並支援所有最新的 AutoSupport 功能。

步驟

1. 確保AutoSupport 啟用了功能：

```
system node autosupport modify -state enable
```

2. 如果您想要技術支援部門接收AutoSupport 到資訊不全、請使用下列命令：

```
system node autosupport modify -support enable
```

   如果您想要啟用AutoSupport 支援以搭配AutoSupport 使用的功能、或是想要將核心傾印和效能歸檔檔案等大型檔案上傳至技術支援或指定的URL、則必須啟用此選項。

3. 如果技術支援已啟用接收AutoSupport 功能不全的訊息、請指定訊息所使用的傳輸傳輸傳輸協定。

   您可以從下列選項中選擇：

如果您想要...	然後設定的下列參數 `system node autosupport modify` 命令 ...

使用預設的HTTPS傳輸協定	a. 設定 `-transport` 至 `https`。 b. 如果您使用 Proxy 、請設定 `-proxy-url` 到您 Proxy 的 URL 。 此組態可支援AutoSupport 透過不必要的功能進行通訊、以及上傳大型檔案。
使用SMTP	設定 `-transport` 至 `smtp`。 此組態不支援AutoSupport 以「根據需求」或上傳大型檔案。

4. 如果您想要內部支援組織或支援合作夥AutoSupport 伴接收到各種消息、請執行下列動作：
   a. 設定的下列參數來識別組織中的收件者 `system node autosupport modify` 命令：

設定此參數…	對此…
`-to`	內部支援組織最多五個以逗號分隔的個別電子郵件地址或通訊群組清單、可接收關鍵AutoSupport 的消息
`-noteto`	內部支援組織最多五個以逗號分隔的個別電子郵件地址或通訊群組清單、將會收到AutoSupport 專為行動電話和其他行動裝置所設計的關鍵字版資訊
`-partner-address`	支援合作夥伴組織中最多五個以逗號分隔的個別電子郵件地址或通訊群組清單、將會接收所有AutoSupport 的消息

   b. 使用列出目的地、檢查位址是否正確設定 `system node autosupport destinations show` 命令。
5. 如果您要傳送訊息給內部支援組織、或是選擇 SMTP 傳輸訊息給技術支援、請設定的下列參數來設定 SMTP `system node autosupport modify` 命令：
   - 設定 `-mail-hosts` 至一或多個郵件主機、以逗號分隔。

     您最多可以設定五個。

   您可以在郵件主機名稱之後指定一個冒號和連接埠編號、為每個郵件主機設定連接埠值：例如、`mymailhost.example.com:5678`，其中 5678 是郵件主機的連接埠。

   - 設定 `-from` 傳送 AutoSupport 訊息的電子郵件地址。
6. 設定DNS。
7. 或者、如果您想要變更特定設定、請新增命令選項：

如果您想要執行此動作…	然後設定的下列參數 `system node autosupport modify` 命令 …

移除、遮罩或編碼訊息中的敏感資料、以隱藏私有資料	設定 `-remove-private-data` 至 `true`。如果您從變更 `false` 至 `true`，所有 AutoSupport 歷史記錄和所有相關文件都將被刪除。
停止以週期AutoSupport 性的資訊訊息傳送效能資料	設定 `-perf` 至 `false`。

8. 使用檢查整體組態 `system node autosupport show` 命令 `-node` 參數。
9. 使用驗證 AutoSupport 作業 `system node autosupport check show` 命令。

   如果回報有任何問題、請使用 `system node autosupport check show-details` 命令以檢視更多資訊。

10. 測試AutoSupport 正在傳送和接收的不實訊息：

    a. 使用 `system node autosupport invoke` 命令 `-type` 參數設為 `test`。

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. 確認NetApp正在接收AutoSupport 您的資訊：

    系統節點AutoSupport 的不正常歷程顯示節點為本機節點

最新傳出的 AutoSupport 訊息狀態最終應變更為 `sent-successful` 適用於所有適當的傳輸協定目的地。

a. 您也可以選擇檢查您為設定的任何地址的電子郵件、確定 AutoSupport 訊息已傳送至您的內部支援組織或支援合作夥伴 `-to`、 `-noteto`或 `-partner-address` 的參數 `system node autosupport modify` 命令。

上傳核心傾印檔案

儲存核心傾印檔案時、會產生事件訊息。如果啟用此功能並將其設定為傳送訊息給NetApp支援部門、則會傳輸一則消息、並傳送自動電子郵件確認訊息給您。AutoSupport AutoSupport

您需要的產品

- 您必須使用AutoSupport 下列設定來設定不必要功能：
  - 節點上啟用了支援。AutoSupport
  - 將支援功能設定為傳送訊息給技術支援。AutoSupport
  - 將支援使用HTTP或HTTPS傳輸傳輸傳輸傳輸協定。AutoSupport

    傳送內含大型檔案（例如核心傾印檔案）的訊息時、不支援該SMTP傳輸傳輸傳輸傳輸傳輸協定。

關於這項工作

您也可以使用透過 AutoSupport 服務透過 HTTPS 上傳核心傾印檔案 `system node autosupport invoke-core-upload` 命令、如果 NetApp 支援部門要求的話。

"如何將檔案上傳至NetApp"

步驟

1. 使用檢視節點的核心傾印檔案 `system node coredump show` 命令。

   在下列範例中、會顯示本機節點的核心傾印檔案：

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. 產生 AutoSupport 訊息、並使用上傳核心傾印檔案 `system node autosupport invoke-core-upload` 命令。

   在下列範例中，會產生一則 AutoSupport 訊息並傳送至預設位置（即技術支援部門），同時將核心傾印檔案上傳至預設位置（即 NetApp 支援網站）：

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   在下列範例中AutoSupport 、會產生一個SURIING訊息並傳送至URI中指定的位置、核心傾印檔案會上傳至URI：

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

上傳效能歸檔檔案

您可以產生AutoSupport 並傳送包含效能歸檔的消息。根據預設，NetApp 技術支援部門會收到 AutoSupport 訊息，效能歸檔則是上傳至 NetApp 支援網站。您可以指定訊息和上傳的替代目的地。

您需要的產品

- 您必須使用AutoSupport 下列設定來設定不必要功能：
  - 節點上啟用了支援。AutoSupport
  - 將支援功能設定為傳送訊息給技術支援。AutoSupport
  - 將支援使用HTTP或HTTPS傳輸傳輸傳輸傳輸協定。AutoSupport

    傳送包含大型檔案（例如效能歸檔檔案）的訊息時、不支援該SMTP傳輸傳輸傳輸傳輸傳輸協定。

關於這項工作

您必須為要上傳的效能歸檔資料指定開始日期。大多數儲存系統會將效能歸檔保留兩週、讓您指定兩週前的開始日期。例如、如果今天是1月15日、您可以指定1月2日的開始日期。

步驟

1. 產生 AutoSupport 訊息、並使用上傳效能封存檔案 `system node autosupport invoke-performance-archive` 命令。

   在下列範例中，2015 年 1 月 12 日起的每 4 小時效能歸檔檔案被新增至 AutoSupport 訊息中，同時上傳至預設位置（即 NetApp 支援網站）：

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   在下列範例中、2015年1月12日起的4小時效能歸檔檔案會新增至AutoSupport 一份消息、並上傳至URI指定的位置：

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

取得**AutoSupport** 資訊說明

您所收到的資訊可透過《Syslog Translator》取得。AutoSupport ONTAP

步驟

1. 前往 "系統記錄轉換器"。
2. 在「版本*」欄位中、輸入**ONTAP** 您所使用的版本。在「搜尋字串*」欄位中、輸入「呼叫首頁」。選擇*翻譯*。
3. Syslog轉換程式會依字母順序列出符合您輸入訊息字串的所有事件。

管理**AutoSupport** 功能的命令

您可以使用 `system node autosupport` 命令可變更或檢視 AutoSupport 組態、顯示先前 AutoSupport 訊息的相關資訊、以及傳送、重新傳送或取消 AutoSupport 訊息。

設定**AutoSupport** 功能

如果您想要...	使用此命令...
控制AutoSupport 是否傳送任何不實訊息	`system node autosupport modify` 使用 `-state` 參數

如果您想要...	使用此命令...
控制AutoSupport 是否將不實訊息傳送至技術支援	`system node autosupport modify` 使用 `-support` 參數
設定AutoSupport 功能不完善或修改AutoSupport 功能不完善的組態	`system node autosupport modify`
針對AutoSupport 個別觸發事件、啟用並停用內部支援組織的資訊不整合、並指定要納入回應個別觸發事件之訊息的子系統報告	`system node autosupport trigger modify`

顯示**AutoSupport** 有關此功能的資訊

如果您想要...	使用此命令...
顯示AutoSupport 此功能的組態	`system node autosupport show` 使用 `-node` 參數
檢視接收AutoSupport 到不實訊息的所有位址和URL摘要	`system node autosupport destinations show`
針對AutoSupport 個別觸發事件、顯示哪些資訊會傳送給您的內部支援組織	`system node autosupport trigger show`
顯示AutoSupport 錶板配置狀態、以及傳送至不同目的地	`system node autosupport check show`
顯示AutoSupport 詳細的資訊、包括設定的資訊、以及傳送到不同目的地的資訊	`system node autosupport check show-details`

顯示關於過去**AutoSupport** 的資訊

如果您想要...	使用此命令...
顯示50 AutoSupport 則最新版的一或多則新聞資訊	`system node autosupport history show`
顯示AutoSupport 最近產生的資訊、以將核心傾印或效能歸檔檔案上傳至技術支援網站或指定的URI	`system node autosupport history show-upload-details`
檢視AutoSupport 資訊資訊、包括針對訊息收集的每個檔案名稱和大小、以及任何錯誤	`system node autosupport manifest show`

傳送、重新傳送或取消**AutoSupport** 等字訊息

如果您想要...	使用此命令...
重新傳輸以AutoSupport 其自身的不一致編號識別的本機儲存的不一致訊息AutoSupport 如果您重新傳送AutoSupport 一個消息、且支援部門已收到該訊息、則支援系統不會建立重複的案例。另一方面、如果支援部門未收到該訊息、AutoSupport 則當必要時、該系統會分析訊息並建立案例。	`system node autosupport history retransmit`
產生AutoSupport 並傳送一個資訊不全的訊息、例如用於測試目的	`system node autosupport invoke` 使用 `-force` 即使 AutoSupport 已停用、仍可傳送訊息的參數。使用 `-uri` 將訊息傳送至指定目的地而非設定目的地的參數。
取消AutoSupport 訊息	`system node autosupport history cancel`

相關資訊

"指令數ONTAP"

資訊包含在**AutoSupport** 資訊清單中

此資訊清單可讓您詳細檢視針對每個支援訊息所收集的檔案。AutoSupport AutoSupport此資訊清單也包含有關當無法收集所需檔案時、收集錯誤的資訊。AutoSupport AutoSupport

此資訊清單包含下列資訊：AutoSupport

- 消息的序號AutoSupport
- 哪些檔案AutoSupport 包含AutoSupport 在消息中
- 每個檔案的大小（以位元組為單位）
- 資訊清單集合的狀態AutoSupport
- 錯誤說明、如果AutoSupport 無法收集一或多個檔案

您可以使用檢視 AutoSupport 資訊清單 `system node autosupport manifest show` 命令。

所有的資訊均包含此資訊清單、並以XML格式呈現、這表示您可以使用一般的XML檢視器來閱讀、或是使用此資訊鏈（先前稱為「我的資訊」）入口網站來檢視。AutoSupport AutoSupport Active IQ AutoSupport

排程維護期間的個案抑制**AutoSupport**

利用抑制支援的案例功能、您可以避免不必要的案例被列入排程維護時段的訊息所觸發。AutoSupport AutoSupport

若要隱藏 AutoSupport 個案、您必須手動呼叫具有特殊格式文字字串的 AutoSupport 訊息： `MAINT=xh`。 `x` 為維護期間的持續時間、以小時為單位。

相關資訊

"如何在排程的維護期間、隱藏自動建立個案"

疑難排解**AutoSupport** 未收到訊息時的問題

如果系統未傳送AutoSupport 此資訊、您可以判斷AutoSupport 這是因為無法產生訊息、還是無法傳送訊息。

步驟

1. 使用檢查訊息的傳送狀態 `system node autosupport history show` 命令。
2. 讀取狀態。

此狀態	方法
正在初始化	收集程序正在開始。如果此狀態是暫時性的、一切都很好。但是、如果此狀態持續存在、則會發生問題。
集合失敗	無法在假脫機目錄中建立不含任何功能的內容。AutoSupport AutoSupport您可以輸入來檢視 AutoSupport 嘗試收集的資料 `system node autosupport history show -detail` 命令。
收集進行中	正在收集的是一些不含知識的內容。AutoSupport AutoSupport您可以輸入來檢視 AutoSupport 正在收集的內容 `system node autosupport manifest show` 命令。
已佇列	系統會排入佇列以供傳送、但尚未傳送。AutoSupport
傳輸	目前正在傳送訊息。AutoSupport
已成功傳送	成功傳達訊息。AutoSupport您可以輸入來找出 AutoSupport 傳送訊息的位置 `system node autosupport history show -delivery` 命令。
忽略	不提供訊息的目的地。AutoSupport您可以輸入來檢視交付詳細資料 `system node autosupport history show -delivery` 命令。
重新佇列	嘗試傳送訊息、但嘗試失敗。AutoSupport因此AutoSupport 、將訊息放回傳送佇列中、以便再次嘗試傳送。您可以輸入來檢視錯誤 `system node autosupport history show` 命令。
傳輸失敗	無法以指定次數傳送訊息、並停止嘗試傳送訊息。AutoSupport您可以輸入來檢視錯誤 `system node autosupport history show` 命令。
隨需忽略	雖然成功處理了這個消息、但《不再是我的選擇了。AutoSupport AutoSupport

3. 執行下列其中一項動作：

以取得此狀態	請這麼做
初始化或收集失敗	聯絡NetApp支援部門、因為AutoSupport 無法產生訊息。請提及下列知識庫文章： "無法提供：狀態卡在初始化中AutoSupport"
忽略、重新佇列或傳輸失敗	檢查目的地是否已正確設定為使用SMTP、HTTP或HTTPS、因為AutoSupport 無法傳送訊息。

疑難排解**AutoSupport** 透過**HTTP**或**HTTPS**傳送的資訊

如果系統未傳送預期AutoSupport 的更新訊息、而您使用HTTP或HTTPS、或自動更新功能無法運作、您可以檢查許多設定來解決問題。

您需要的產品

您應該已經確認基本的網路連線和DNS查詢：

- 您的節點管理LIF必須處於作業和管理狀態。
- 您必須能夠從叢集管理LIF ping同一子網路上正常運作的主機（而非任何節點上的LIF）。
- 您必須能夠從叢集管理LIF ping子網路外正常運作的主機。
- 您必須能夠使用主機名稱（而非IP位址）、從叢集管理LIF ping子網路外的正常運作主機。

關於這項工作

這些步驟適用於您已判斷AutoSupport 出無法透過HTTP或HTTPS傳送訊息的情況。

如果您遇到錯誤或無法完成此程序中的步驟、請先判斷並解決此問題、然後再繼續下一步。

步驟

1. 顯示AutoSupport 資訊子系統的詳細狀態：

   ```
   system node autosupport check show-details
   ```

   這包括透過AutoSupport 傳送測試訊息來驗證與景點的連線能力、並提供AutoSupport 一份清單、列出您的列舉設定中可能發生的錯誤。

2. 驗證節點管理LIF的狀態：

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   - `status-oper` 和 `status-admin` 欄位應傳回 "`up" 。

3. 記下SVM名稱、LIF名稱及LIF IP位址以供日後使用。
4. 確認DNS已啟用且設定正確：

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

5. 解決AutoSupport 由該消息傳回的任何錯誤：

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   如需疑難排解任何傳回錯誤的協助、請參閱 "《》（Transport HTTPS和HTTP）解決方案指南ONTAP AutoSupport"。

6. 確認叢集可以成功存取所需的伺服器和網際網路：

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > 地址 `support.netapp.com` 本身不會回應 ping / traceroute 、但每一跳的資訊非常寶貴。

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   如果其中任何一條路由無法運作、請使用大多數協力廠商網路用戶端上的「'traceroute」或「`TRACERT」公用程式、嘗試從與叢集位於同一子網路上的正常運作主機發出相同的路由。這有助於判斷問題是發生在您的網路組態或叢集組態中。

7. 如果AutoSupport 您使用HTTPS作為您的傳輸傳輸協定、請確定HTTPS流量可以離開您的網路：

   a. 在與叢集管理LIF相同的子網路上設定Web用戶端。

      確保所有組態參數的值與AutoSupport 使用相同的組態設定值相同、包括使用相同的Proxy伺服器、使用者名稱、密碼和連接埠。

   b. 存取 `https://support.netapp.com` 使用 Web 用戶端。

      存取應該會成功。如果不是、請確定所有防火牆均已正確設定、以允許HTTPS和DNS流量、而且Proxy伺服器的設定正確。如需設定support.netapp.com靜態名稱解析的詳細資訊、請參閱知識庫文章 "如何將主機項目新增至ONTAP support.netapp.com?的功能表"

8. 從ONTAP 《支援物件9.10.1》開始、如果您啟用「自動更新」功能、請確定您已將HTTPS連線至下列其他URL：

   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

疑難排解**AutoSupport** 透過**SMTP**傳送訊息的問題

如果系統無法透過AutoSupport SMTP傳送不實訊息、您可以檢查許多設定來解決問題。

您需要的產品

您應該已經確認基本的網路連線和DNS查詢：

- 您的節點管理LIF必須處於作業和管理狀態。
- 您必須能夠從叢集管理LIF ping同一子網路上正常運作的主機（而非任何節點上的LIF）。
- 您必須能夠從叢集管理LIF ping子網路外正常運作的主機。
- 您必須能夠使用主機名稱（而非IP位址）、從叢集管理LIF ping子網路外的正常運作主機。

關於這項工作

這些步驟適用於判斷AutoSupport 出無法透過SMTP傳送訊息的情況。

如果您遇到錯誤或無法完成此程序中的步驟、請先判斷並解決此問題、然後再繼續下一步。

除非ONTAP 另有說明、否則所有命令都會在指令行介面上輸入。

步驟

1. 驗證節點管理LIF的狀態：

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   - `status-oper` 和 `status-admin` 欄位應會傳回 `up`。

2. 記下SVM名稱、LIF名稱及LIF IP位址以供日後使用。
3. 確認DNS已啟用且設定正確：

   vserver services name-service dns show

4. 顯示AutoSupport 所有設定供下列對象使用的伺服器：

   system node autosupport show -fields mail-hosts

   記錄顯示的所有伺服器名稱。

5. 針對上一步所顯示的每部伺服器、以及 `support.netapp.com`、請確定節點可以連線到伺服器或 URL ：

   network traceroute -node local -destination *server_name*

   如果其中任何一條路由無法運作、請使用大多數協力廠商網路用戶端上的「'traceroute」或「`TRACERT」公用程式、嘗試從與叢集位於同一子網路上的正常運作主機發出相同的路由。這有助於判斷問題是發生在您的網路組態或叢集組態中。

6. 登入指定為郵件主機的主機、並確保它可以處理下列的SMTP要求：

   netstat -aAn|grep 25

   `25` 是接聽程式 SMTP 連接埠號碼。

   此時會顯示類似下列文字的訊息：

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 從其他主機、開啟與郵件主機之SMTP連接埠的遠端登入工作階段：

   telnet *mailhost* 25

   此時會顯示類似下列文字的訊息：

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. 在登入提示字元時、請確定訊息可以從您的郵件主機轉送：

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` 是您網路的網域名稱。

   如果傳回錯誤、指出中繼遭拒、則不會在郵件主機上啟用中繼。請聯絡您的系統管理員。

9. 在登入提示字元下、傳送測試訊息：

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   > 請確定您自己在一行輸入最後一個期間（.）。期間會向郵件主機指出訊息已完成。

   如果傳回錯誤、表示您的郵件主機設定不正確。請聯絡您的系統管理員。

10. 從這個指令行介面、將一份不實的測試訊息傳送到您有權存取的信任電子郵件地址：ONTAP AutoSupport

    system node autosupport invoke -node local -type test

11. 尋找嘗試的順序編號：

    system node autosupport history show -node local -destination smtp

    根據時間戳記尋找嘗試的順序編號。這可能是最近的嘗試。

12. 顯示測試訊息嘗試的錯誤：

    system node autosupport history show -node local -seq-num seq_num -fields error

    如果顯示錯誤 `Login denied`，您的 SMTP 伺服器不接受叢集管理 LIF 的傳送要求。如果您不想變更為使

用HTTPS作為傳輸傳輸協定、請聯絡您的站台網路管理員、設定以解決此問題的SMTP閘道。

如果此測試成功、但傳送至mailto：autosupport@netapp.com的同一訊息卻沒有、請確定所有的SMTP郵件主機都已啟用了SMTP轉送、或使用HTTPS作為傳輸傳輸傳輸傳輸傳輸協定。

如果連本機管理電子郵件帳戶的訊息都未成功、請確認您的SMTP伺服器已設定為轉送具有下列兩項特性的附件：

- 「'7z'」字尾
- 「application/x-7x-compressed」MIME類型。

疑難排解**AutoSupport VMware**子系統

- `system node check show` 命令可用於驗證和疑難排解任何與 AutoSupport 組態和交付相關的問題。

步驟

1. 使用下列命令來顯示AutoSupport 資訊子系統的狀態。

使用此命令...	若要這麼做...
`system node autosupport check show`	顯示AutoSupport 整個的資訊子系統狀態、例如AutoSupport ：http或HTTPS目的地的狀態、AutoSupport 不支援的SMTP目的地、AutoSupport 不支援的伺服器和AutoSupport 不支援的組態
`system node autosupport check show-details`	顯示AutoSupport 詳細的資訊、例如錯誤的詳細說明和修正行動

健全狀況監控

監控系統健全狀況總覽

健全狀況監視器會主動監控叢集中的特定關鍵情況、並在偵測到故障或風險時發出警示。如果有作用中警示、系統健全狀況狀態會報告叢集的降級狀態。這些警示包括回應降級系統健全狀況所需的資訊。

如果狀態為降級、您可以檢視問題的詳細資料、包括可能原因和建議的還原動作。解決問題之後、系統健全狀況狀態會自動返回「OK（確定）」。

系統健全狀況狀態反映多個獨立的健全狀況監視器。個別健全狀況監視器的降級狀態會導致整體系統健全狀況的降級狀態。

如需ONTAP 有關支援叢集交換器以監控叢集內系統健全狀況的詳細資訊、請參閱_E__ Hardware Universe 。

"支援的交換器Hardware Universe"

如需叢集交換器健全狀況監視器（CSHM）AutoSupport 功能介紹訊息的原因、以及解決這些警示所需採取的必要行動、請參閱知識庫文章。

"資訊：Health Monitor Process CSHM AutoSupport"

健全狀況監控的運作方式

個別健全狀況監視器有一組原則、可在特定情況發生時觸發警示。瞭解健全狀況監控的運作方式、可協助您回應問題並控制未來警示。

健全狀況監控包含下列元件：

- 特定子系統的個別健全狀況監視器、每個子系統都有自己的健全狀況狀態

  例如、儲存子系統具有節點連線健全狀況監視器。

- 整合個別健全狀況監視器健全狀況狀態的整體系統健全狀況監視器

  任何單一子系統的降級狀態、都會導致整個系統的降級狀態。如果沒有子系統發出警示、則整體系統狀態為「OK（正常）」。

每個健全狀況監視器均由下列關鍵元素組成：

- 警示：健全狀況監視器可能會發出警示

  每個警示都有定義、其中包含警示嚴重性及其可能原因等詳細資料。

- 可識別每個警示觸發時間的健全狀況原則

  每個健全狀況原則都有規則運算式、這是觸發警示的確切條件或變更。

健全狀況監視器會持續監控及驗證其子系統中的資源、以確保狀況或狀態變更。當條件或狀態變更符合健全狀況原則中的規則表示式時、健全狀況監視器會發出警示。警示會使子系統的健全狀況狀態和整體系統健全狀況狀態降級。

回應系統健全狀況警示的方法

當系統健全狀況警示發生時、您可以確認該警示、深入瞭解該警示、修復基礎狀況、並防止其再次發生。

當健全狀況監視器發出警示時、您可以使用下列任一方式回應：

- 取得警示的相關資訊、包括受影響的資源、警示嚴重性、可能原因、可能影響及修正行動。
- 取得警示的詳細資訊、例如警示發出時間、以及是否有其他人已確認警示。
- 取得受影響資源或子系統狀態的相關健全狀況資訊、例如特定機櫃或磁碟。
- 確認警示、指出有人正在處理此問題、並將自己識別為「Acknowledger」。
- 請採取警示中提供的修正行動來解決問題、例如修正纜線以解決連線問題。
- 如果系統未自動清除警示、請刪除警示。

- 隱藏警示、以防止其影響子系統的健全狀況狀態。

  當您瞭解問題時、隱藏功能非常實用。隱藏警示之後、仍可能發生、但當發生抑制警示時、子系統健全狀況會顯示為「ok、with -suppressed」（「ok、with -suppressed」）。

系統健全狀況警示自訂

您可以啟用及停用定義警示觸發時間的系統健全狀況原則、來控制健全狀況監視器產生的警示。這可讓您針對特定環境自訂健全狀況監控系統。

您可以透過顯示所產生警示的詳細資訊、或顯示特定健全狀況監視器、節點或警示ID的原則定義、來學習原則名稱。

停用健全狀況原則與隱藏警示不同。當您隱藏警示時、它不會影響子系統的健全狀況狀態、但仍會發出警示。

如果停用原則、則在原則規則運算式中定義的條件或狀態將不再觸發警示。

您要停用的警示範例

例如、假設發生對您不實用的警示。您可以使用 `system health alert show -instance` 命令以取得警示的原則 ID 。您可以使用中的原則 ID `system health policy definition show` 命令以檢視原則的相關資訊。檢閱規則運算式和原則的其他相關資訊之後、您決定停用原則。您可以使用 `system health policy definition modify` 停用原則的命令。

健全狀況警示如何觸發**AutoSupport** 訊息和事件

系統健全狀況警示會觸發AutoSupport 事件管理系統（EMS）中的訊息和事件、讓您AutoSupport 除了直接使用健全狀況監控系統之外、還能使用消息和EMS來監控系統的健全狀況。

系統AutoSupport 會在發出警示後五分鐘內傳送一則資訊不整訊息。除了複製上一週相同資源的警示和可能原因的警示之外、本資訊還會包含上一次顯示的所有警示。AutoSupport AutoSupport

部分警示不會觸發AutoSupport 資訊不均。如果AutoSupport 健全狀況原則停用AutoSupport 傳送功能、警示不會觸發資訊不全。例如、健全狀況原則AutoSupport 可能預設會停用不含資訊的訊息、因為AutoSupport 當問題發生時、資訊技術已經產生訊息。您可以使用設定原則、使其不會觸發 AutoSupport 訊息 `system health policy definition modify` 命令。

您可以使用檢視上週傳送的所有警示觸發 AutoSupport 訊息清單 `system health autosupport trigger history show` 命令。

警示也會觸發EMS產生事件。每次建立警示及清除警示時、都會產生一個事件。

可用的叢集健全狀況監視器

有多個健全狀況監視器可監控叢集的不同部分。健全狀況監視器可ONTAP 偵測事件、傳送警示給您、並在清除事件時刪除事件、協助您從錯誤中恢復。

健全狀況監視器名稱（識別碼）	子系統名稱（識別碼）	目的
叢集交換器（叢集交換器）	交換器（交換器健全狀況）	監控叢集網路交換器和管理網路交換器的溫度、使用率、介面組態、備援（僅限叢集網路交換器）、以及風扇和電源供應器作業。叢集交換器健全狀況監視器透過SNMP與交換器通訊。預設設定為：SNMPv2c。 從ONTAP 功能表9.2開始、此監視器可偵測並報告叢集交換器自上次輪詢期間後重新開機的時間。
支援的架構MetroCluster	交換器	監控MetroCluster 支援此功能的後端架構拓撲、並偵測錯誤的組態、例如不正確的佈線和分區、以及ISL故障。
系統健全狀況MetroCluster	互連、RAID和儲存設備	監控FC-VI介面卡、FC啟動器介面卡、左後集合體和磁碟、以及叢集間連接埠
節點連線（節點連線）	CIFS不中斷營運（CIF-NDO）	監控SMB連線、以確保不中斷營運至Hyper-V應用程式。
儲存設備（SAS連線）	在節點層級監控磁碟櫃、磁碟和介面卡、以取得適當的路徑和連線。	系統
不適用	彙總來自其他健全狀況監視器的資訊。	系統連線（系統連線）

自動接收系統健全狀況警示

您可以使用手動檢視系統健全狀況警示 `system health alert show` 命令。不過、您應該訂閱特定的事件管理系統（EMS）訊息、以便在健全狀況監視器產生警示時自動接收通知。

關於這項工作

下列程序說明如何設定所有hm.alert.malled訊息和所有hm.alert.Cleared訊息的通知。

所有hm.alert.malled訊息和所有hm.alert.Cleared訊息均包含SNMP設陷。SNMP 設陷的名稱為 `HealthMonitorAlertRaised` 和 `HealthMonitorAlertCleared`。如需SNMP設陷的相關資訊、請參閱_網路管理指南_。

步驟

1. 使用 `event destination create` 用於定義要將 EMS 訊息傳送至哪個目的地的命令。

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. 使用 `event route add-destinations` 路由的命令 `hm.alert.raised` 訊息和 `hm.alert.cleared` 傳送至目的地的訊息。

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

相關資訊

"網路管理"

回應降級的系統健全狀況

當系統的健全狀況狀態降級時、您可以顯示警示、讀取可能的原因和修正動作、顯示降級子系統的相關資訊、以及解決問題。也會顯示隱藏的警示、以便您修改這些警示、並查看是否已確認。

關於這項工作

您可以透過檢視 AutoSupport 訊息或 EMS 事件、或使用、來發現已產生警示 `system health` 命令。

步驟

1. 使用 `system health alert show` 命令以檢視影響系統健全狀況的警示。
2. 請閱讀警示的可能原因、可能影響及修正行動、以判斷您是否可以解決問題或需要更多資訊。
3. 如果您需要更多資訊、請使用 `system health alert show -instance` 命令以檢視警示可用的其他資訊。
4. 使用 `system health alert modify` 命令 `-acknowledge` 參數、表示您正在處理特定警示。
5. 請採取修正行動、以解決如所述的問題 `Corrective Actions` 警示中的欄位。

   修正行動可能包括重新啟動系統。

   解決問題時、警示會自動清除。如果子系統沒有其他警示、子系統的健全狀況會變更為 `OK`。如果所有子系統的健全狀況均正常、則整體系統健全狀況狀態會變更為 `OK`。

6. 使用 `system health status show` 確認系統健全狀況狀態的命令 `OK`。

   如果系統健全狀況狀態不是 `OK`，請重複此程序。

回應降級系統健全狀況的範例

藉由檢閱缺少兩條節點路徑的機櫃所造成的降級系統健全狀況的特定範例、您可以查看當

回應警示時CLI顯示的內容。

啟動ONTAP 功能後、您會檢查系統健全狀況、發現狀態已降級：

```
      cluster1::>system health status show
        Status
        ---------------
        degraded
```

您會顯示警示、以瞭解問題所在位置、並看到機櫃2沒有兩個節點1路徑：

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

您可以顯示警示的詳細資料、以取得更多資訊、包括警示ID：

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

您認可警示、表示您正在處理警示。

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

您可以修復機櫃2和節點1之間的纜線、然後重新啟動系統。然後再次檢查系統健全狀況、並查看狀態 OK：

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

設定探索叢集和管理網路交換器

叢集交換器健全狀況監視器會自動嘗試使用Cisco探索傳輸協定（CDP）來探索叢集和管理網路交換器。如果健全狀況監視器無法自動探索交換器、或您不想使用CDP進行自動探索、則必須設定健全狀況監視器。

關於這項工作

。 `system cluster-switch show` 命令會列出健全狀況監視器探索到的交換器。如果您在該清單中沒有看到您預期看到的交換器、則健全狀況監視器將無法自動探索它。

步驟

1. 如果您要使用CDP進行自動探索、請執行下列動作：

   a. 確定交換器上已啟用Cisco探索傳輸協定（CDP）。

      請參閱交換器文件以取得相關指示。

   b. 在叢集中的每個節點上執行下列命令、以驗證CDP是否已啟用或停用：

      `run -node node_name -command options cdpd.enable`

      如果已啟用CDP、請前往步驟d如果停用CDP、請前往步驟C

   c. 執行下列命令以啟用CDP：

      `run -node node_name -command options cdpd.enable on`

   請等待五分鐘、然後再繼續下一步。

   a. 使用 `system cluster-switch show` 命令來驗證 ONTAP 現在是否可以自動探索交換器。

2. 如果健全狀況監視器無法自動探索交換器、請使用 `system cluster-switch create` 設定交換器探索的命令：

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   請等待五分鐘、然後再繼續下一步。

3. 使用 `system cluster-switch show` 命令來驗證 ONTAP 是否能探索您新增資訊的交換器。

完成後

確認健全狀況監視器可以監控您的交換器。

驗證叢集與管理網路交換器的監控

叢集交換器健全狀況監視器會自動嘗試監控其探索到的交換器、但如果交換器設定不正確、則可能不會自動進行監控。您應該確認健全狀況監視器已正確設定、以監控交換器。

步驟

1. 若要識別叢集交換器健全狀況監視器發現的交換器、請輸入下列命令：

   更新版本**ONTAP**

   ```
   system switch ethernet show
   ```

   更新版本**ONTAP**

   ```
   system cluster-switch show
   ```

   如果是 `Model` 欄顯示值 `OTHER`，則 ONTAP 無法監控交換器。ONTAP 將值設為 `OTHER` 如果它自動探索的交換器不支援用於健全狀況監控。

   > 如果命令輸出中沒有顯示交換器、您必須設定探索交換器。

2. 升級至受支援的最新交換器軟體，並參照至從 NetApp 支援網站下載的組態檔（RCF）。

   "NetApp支援下載頁面"

   交換器RCF中的社群字串必須與健全狀況監視器設定為使用的社群字串相符。依預設、健全狀況監視器會使用社群字串 `cshm1!`。

   > 目前、健全狀況監視器僅支援SNMPv2。

   如果您需要變更叢集監控的交換器相關資訊、可以使用下列命令來修改健全狀況監控使用的社群字串：

   更新版本**ONTAP**

   ```
   system switch ethernet modify
   ```

   更新版本**ONTAP**

   ```
   system cluster-switch modify
   ```

3. 確認交換器的管理連接埠已連線至管理網路。

   執行SNMP查詢時需要此連線。

用於監控系統健全狀況的命令

您可以使用 `system health` 顯示系統資源健全狀況資訊、回應警示及設定未來警示的命令。使用CLI命令可讓您深入檢視設定健全狀況監控的方式資訊。命令的手冊頁包含更多資訊。

顯示系統健全狀況的狀態

如果您想要...	使用此命令...
顯示系統的健全狀況狀態、反映個別健全狀況監視器的整體狀態	`system health status show`
顯示子系統的健全狀況狀態、以便進行健全狀況監控	`system health subsystem show`

顯示節點連線狀態

如果您想要...	使用此命令...
顯示從節點連線至儲存櫃的詳細資料、包括連接埠資訊、HBA連接埠速度、I/O處理量、以及每秒I/O作業速率	`storage shelf show -connectivity` 使用 `-instance` 顯示每個機櫃詳細資訊的參數。
顯示磁碟機和陣列LUN的相關資訊、包括可用空間、機櫃和機櫃編號、以及擁有節點名稱	`storage disk show` 使用 `-instance` 參數顯示每個磁碟機的詳細資訊。
顯示儲存櫃連接埠的詳細資訊、包括連接埠類型、速度和狀態	`storage port show` 使用 `-instance` 參數以顯示每個介面卡的詳細資訊。

管理叢集、儲存設備及管理網路交換器的探索

如果您想要...	使用此命令..（更新版本：**ONTAP**	使用此命令..（更新版本：**9.7**）**ONTAP**
顯示叢集監控的交換器	`system switch ethernet show`	`system cluster-switch show`
顯示叢集目前監控的交換器、包括您刪除的交換器（如命令輸出中的「原因」欄所示）、以及網路存取叢集和管理網路交換器所需的組態資訊。 此命令可在進階權限層級使用。	`system switch ethernet show-all`	`system cluster-switch show-all`

如果您想要...	使用此命令..（更新版本：ONTAP	使用此命令..（更新版本：9.7）ONTAP
設定探索未探索到的交換器	`system switch ethernet create`	`system cluster-switch create`
修改叢集監控的交換器相關資訊（例如、裝置名稱、IP位址、SNMP版本和社群字串）	`system switch ethernet modify`	`system cluster-switch modify`
停用交換器監控	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
停用探索及監控交換器、並刪除交換器組態資訊	`system switch ethernet delete`	`system cluster-switch delete`
永久移除儲存在資料庫中的交換器組態資訊（如此會重新啟用交換器的自動探索）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
啟用自動記錄功能、以AutoSupport利發送資訊。	`system switch ethernet log`	`system cluster-switch log`

回應產生的警示

如果您想要...	使用此命令...
顯示已產生警示的相關資訊、例如觸發警示的資源和節點、以及警示的嚴重性和可能原因	`system health alert show`
顯示每個產生警示的相關資訊	`system health alert show -instance`
表示有人正在處理警示	`system health alert modify`
確認警示	`system health alert modify -acknowledge`
隱藏後續警示、使其不影響子系統的健全狀況	`system health alert modify -suppress`
刪除未自動清除的警示	`system health alert delete`
顯示AutoSupport 上週觸發警示的有關資訊、例如、判斷警示是否觸發AutoSupport 了一個故障訊息	`system health autosupport trigger history show`

設定未來警示

如果您想要...	使用此命令...
啟用或停用控制特定資源狀態是否發出特定警示的原則	`system health policy definition modify`

顯示如何設定健全狀況監控的相關資訊

如果您想要...	使用此命令...
顯示健全狀況監視器的相關資訊、例如其節點、名稱、子系統和狀態	`system health config show` 使用 `-instance` 顯示每個健全狀況監視器的詳細資訊的參數。
顯示健全狀況監視器可能產生之警示的相關資訊	`system health alert definition show` 使用 `-instance` 顯示每個警示定義的詳細資訊的參數。
顯示有關健全狀況監視原則的資訊、以決定何時發出警示	`system health policy definition show` 使用 `-instance` 參數以顯示每個原則的詳細資訊。使用其他參數來篩選警示清單、例如依原則狀態（已啟用或未啟用）、健全狀況監視器、警示等。

顯示環境資訊

感應器可協助您監控系統的環境元件。您可以顯示的環境感測器相關資訊包括其類型、名稱、狀態、值和臨界值警告。

步驟

1. 若要顯示環境感應器的相關資訊、請使用 `system node environment sensors show` 命令。

檔案系統分析

檔案系統分析總覽

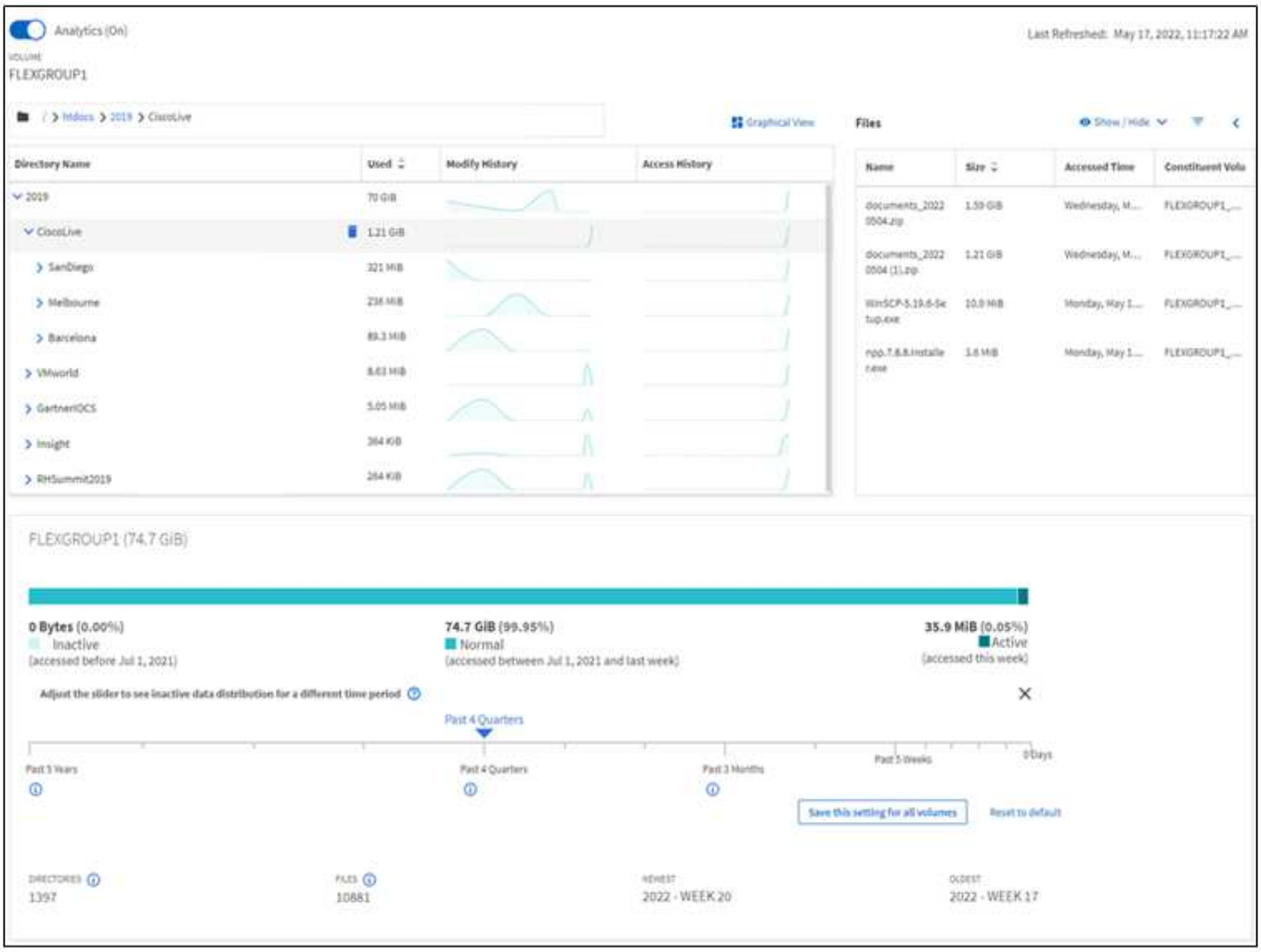
檔案系統分析（FSA）是ONTAP 在更新版本9.8中首次推出、可即時查看ONTAP FlexGroup 檔案使用率及內部的儲存容量趨勢、包括更新版本。FlexVol這項原生功能可免除外部工具的需求、並提供關鍵見解、讓您瞭解如何運用儲存設備、以及是否有機會針對您的業務需求最佳化儲存設備。

有了 FSA 、您就能在 NAS 中查看 Volume 檔案系統階層的所有層級。例如、您可以在儲存VM（SVM）、Volume、目錄和檔案層級取得使用量和容量洞見。您可以使用FSA來回答下列問題：

- 我的儲存設備中有哪些空間、還有哪些大型檔案可以移至其他儲存位置？
- 哪些是我最活躍的磁碟區、目錄和檔案？我的儲存效能是否已針對使用者的需求最佳化？
- 上個月新增了多少資料？
- 誰是我最活躍或最不活躍的儲存使用者？
- 我的主要儲存設備上有多少閒置或靜止資料？我可以將資料移至成本較低的冷層嗎？
- 我的計畫性服務品質變更是否會對存取經常存取的重要檔案造成負面影響？

檔案系統分析已整合至ONTAP 《Sytricity System Manager》。System Manager中的檢視可提供：

- 即時可見度、有效管理及營運資料
- 即時資料收集與集合體
- 子目錄和檔案大小與數量、以及相關的效能設定檔
- 修改及存取歷程記錄的檔案保存時間分佈圖



支援的**Volume**類型

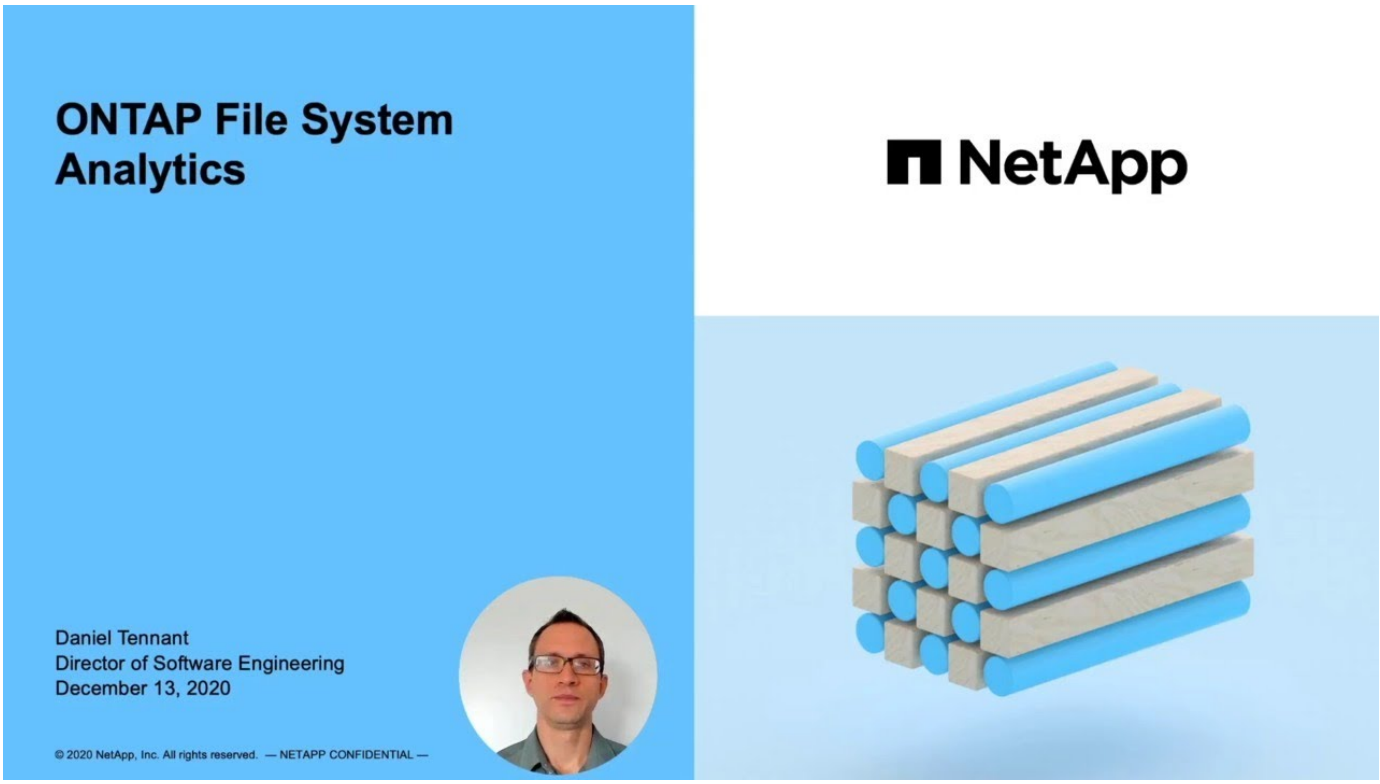
檔案系統分析的設計旨在提供使用中NAS資料的磁碟區可見度、FlexCache 但不包括SnapMirror快取和SnapMirror目的地磁碟區。

檔案系統分析功能可用度

每個 ONTAP 版本都擴大了檔案系統分析的範圍。

	ONTAP 9.14.1.	**ONTAP 9.13.1.12 .9.11.9.1 1.**	**ONTAP 9.12.1**	零點**9.11. 1. ONTAP**	零點**9.10. 1 ONTAP**	部分**9.9.1 ONTAP**	部分**9.8 ONTAP**
系統管理程式中的視覺化功能	✓	✓	✓	✓	✓	✓	✓
容量分析	✓	✓	✓	✓	✓	✓	✓
非作用中資料資訊	✓	✓	✓	✓	✓	✓	✓
支援Data ONTAP 從VMware 7-Mode轉換的Volume	✓	✓	✓	✓	✓	✓	
能夠在System Manager中自訂非作用中期間	✓	✓	✓	✓	✓	✓	
Volume層級活動追蹤	✓	✓	✓	✓	✓		
將活動追蹤資料下載至CSV	✓	✓	✓	✓	✓		
SVM層級的活動追蹤	✓	✓	✓	✓			
時間表	✓	✓	✓	✓			
使用分析	✓	✓	✓				
預設啟用檔案系統分析的選項	✓	✓					
初始化掃描進度監視器	✓						

深入瞭解檔案系統分析



進一步閱讀

- "TR 4687：ONTAP 《關於分析檔案系統的最佳實務準則》"
- "知識庫：開啟NetApp ONTAP 功能的NetApp功能檔系統分析後、延遲時間會大幅或波動"

啟用檔案系統分析

若要收集及顯示容量分析等使用資料、您必須在磁碟區上啟用檔案系統分析。

關於這項工作

- 從功能支援的9.8開始ONTAP 、您可以在新的或現有的磁碟區上啟用檔案系統分析功能。如果您將系統升級ONTAP 至支援更新版本的支援版本9.8、請務必先完成所有的升級程序、再啟用檔案系統分析功能。
- 視磁碟區的大小和內容而定、啟用分析可能需要一些時間、ONTAP 而無法在磁碟區中處理現有資料。系統管理程式會顯示進度、並在完成時顯示分析資料。如果您需要更精確的初始化進度資訊、可以使用 ONTAP CLI 命令 `volume analytics show`。

  從 ONTAP 9.14.1 開始、 ONTAP 除了提供影響掃描進度的節流事件通知外、還提供初始化掃描的進度追蹤。

  如需初始化掃描的其他考量事項、請參閱 掃描考量。

步驟

您可以使用ONTAP 支援功能支援檔案系統分析的功能、包括使用支援功能的系統管理程式或CLI。

系統管理員

在**209.8**和**9.9.1**中**ONTAP**	從**ONTAP** 功能部分**9.10.1**開始
1.選擇*儲存>磁碟區*。 2.選取所需的Volume、然後選取* Explorer’s 。 **3.**選取*啟用分析*或*停用分析。	1.選擇*儲存>磁碟區*。 2.選取所需的Volume。從個別Volume功能表中、選取*檔案系統>檔案總管*。 3.選取*啟用分析*或*停用分析*。

CLI

使用 **CLI** 啟用檔案系統分析

1. 執行下列命令：
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`
   根據預設、命令會在前景執行； ONTAP 會顯示進度、並在完成時顯示分析資料。如果您需要更精確的資訊、可以使用在背景執行命令 `-foreground false` 選項、然後使用 `volume analytics show` 用於在 CLI 中顯示初始化進度的命令。
2. 成功啟用檔案系統分析之後、請使用系統管理員或 ONTAP REST API 來顯示分析資料。

修改預設檔案系統分析設定

從 ONTAP 9.13.1 開始、您可以修改 SVM 或叢集設定、以在新磁碟區上預設啟用檔案系統分析。

系統管理員

如果您使用的是 System Manager 、您可以修改儲存 VM 或叢集設定、以在建立 Volume 時啟用容量分析和活動追蹤。預設啟用功能僅適用於修改設定後建立的磁碟區、而非現有的磁碟區。

修改叢集上的檔案系統分析設定

1. 在 System Manager 中、瀏覽至 叢集設定 。
2. 在 叢集設定 中、檢閱檔案系統設定標籤。若要修改設定、請選取 ⚙ 圖示。
3. 在「 活動追蹤 」欄位中、輸入 SVM 的名稱、以預設為啟用「活動追蹤」。將此欄位保留空白、將會在所有 SVM 上停用「活動追蹤」。

   取消核取「在新的儲存 VM 上啟用」核取方塊、即可在新的儲存 VM 上預設停用「活動追蹤」。

4. 在「 分析 」欄位中、輸入您要依預設啟用容量分析的儲存 VM 名稱。將欄位保留空白、將會在所有 SVM 上停用容量分析。

   取消核取「在新的儲存 VM 上啟用」核取方塊、即可在新的儲存 VM 上依預設停用容量分析。

5. 選擇 儲存 。

修改 **SVM** 上的檔案系統分析設定

1. 選擇要修改的 SVM 、然後選擇 儲存 **VM** 設定 。
2. 在「 檔案系統分析 」卡中、使用切換來啟用或停用儲存 VM 上所有新磁碟區的「活動追蹤」和「容量分析」。

CLI

您可以使用 ONTAP CLI 將儲存 VM 設定為在新磁碟區上預設啟用檔案系統分析。

依預設、在 **SVM** 上啟用檔案系統分析

1. 修改 SVM 以在所有新建立的磁碟區上、依預設啟用容量分析和活動追蹤：
   `vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto -enable-analytics true`

檢視檔案系統活動

啟用檔案系統分析（FSA）之後、您可以檢視所選磁碟區的根目錄內容、並依據每個子樹狀結構中所使用的空間進行排序。

選取任何檔案系統物件以瀏覽檔案系統、並顯示目錄中每個物件的詳細資訊。目錄的相關資訊也可以圖形方式顯示。隨著時間推移、每個子樹狀結構都會顯示歷史資料。如果目錄超過3000個、則不會對已用空間進行排序。

檔案總管

檔案系統分析*檔案總管*畫面包含三個區域：

- 目錄與子目錄的樹狀檢視；可展開的清單、顯示名稱、大小、修改歷程記錄及存取歷程記錄。
- 檔案；顯示目錄清單中所選物件的名稱、大小和存取時間。

- 目錄清單中所選物件的作用中和非作用中資料比較。

  從0到9：9.1開始ONTAP 、您可以自訂要報告的範圍。預設值為一年。根據這些自訂、您可以採取修正行動、例如移動磁碟區和修改分層原則。

預設會顯示存取時間。不過、如果已從 CLI 變更磁碟區預設值（透過設定 `-atime-update` 選項 `false` 使用 `volume modify` 命令）、則只會顯示上次修改的時間。例如：

- 樹狀檢視不會顯示*存取歷程記錄*。
- 檔案檢視畫面將會變更。
- 作用中 / 非作用中的資料檢視將根據修改時間而定 (`mtime`）。

使用這些顯示器、您可以檢查下列項目：

- 檔案系統位置佔用的空間最大
- 目錄樹狀結構的詳細資訊、包括目錄和子目錄內的檔案和子目錄數
- 包含舊資料的檔案系統位置（例如、Scratch、Temp或記錄樹狀結構）

在解讀FSA輸出時、請謹記以下幾點：

- FSA會顯示資料使用的位置和時間、而非處理的資料量。例如、最近存取或修改的檔案佔用大量空間、並不一定表示系統處理負載過高。
- 「* Volume Explorer*」標籤計算FSA空間使用量的方式、可能與其他工具不同。尤其是、如果磁碟區已啟用儲存效率功能、相較於* Volume Overview 所報告的使用量、可能會有顯著差異。這是因為 Volume Explorer’s（磁碟區總管）索引標籤不包含效率節約效益。
- 由於目錄顯示區的空間限制、因此無法在_List View_中檢視大於8層的目錄深度。若要檢視深度超過8層的目錄、您必須切換至_Graphical View_、找到所需的目錄、然後切換回_List View_。如此可在顯示器中增加額外的螢幕空間。

步驟

1. 檢視所選磁碟區的根目錄內容：

在**209.8**和**9.9.1**中**ONTAP**	從**ONTAP** 功能部分**9.10.1**開始
單擊* Storage（儲存設備）> Volumes（磁碟區）、選擇所需的磁碟區、然後單擊 Explorer’s *。	選取*儲存>磁碟區*、然後選取所需的磁碟區。從個別Volume功能表中、選取*檔案系統>檔案總管*。

啟用「活動追蹤」

從 ONTAP 9.10.1 開始、檔案系統分析包含「活動追蹤」功能、可讓您識別常用物件並將資料下載為 CSV 檔案。從《S209.11.1活動ONTAP 追蹤（Activ練習 追蹤）」開始、活動追蹤已擴大至SVM範圍。此外、從《系統管理程式》（System Manager）的《活動追蹤》（Activicity Tracking, System Manager）也開始提供活動追蹤的時間表、讓您最多可以查看五分鐘的「活動追蹤」資料。ONTAP

「活動追蹤」可監控四種類別：

- 目錄
- 檔案
- 用戶端
- 使用者

對於每個受監控的類別、「活動追蹤」會顯示讀取IOPs、寫入IOPs、讀取流量和寫入流量。「活動追蹤」查詢每10到15秒會重新整理一次、以說明系統在前五秒間隔內出現的熱點。

活動追蹤資訊是大約的、資料的準確度取決於傳入I/O流量的分配。

在Volume層級的System Manager中檢視「活動追蹤」時、只有展開Volume的功能表會主動重新整理。如果任何磁碟區的檢視都已收合、則在展開磁碟區顯示之前、這些磁碟區不會重新整理。您可以使用*暫停重新整理*按鈕來停止重新整理。活動資料可以CSV格式下載、以顯示所選磁碟區擷取的所有時間點資料。

從《支援資料時程表ONTAP 》9.11.1開始、您可以將熱點活動記錄在磁碟區或SVM上、每五秒持續更新一次、並保留前五分鐘的資料。時間軸資料只會保留給頁面可見區域的欄位。如果您摺疊追蹤類別或捲動、使時間表不在檢視範圍內、時間表將停止收集資料。根據預設、當您離開「活動」索引標籤時、時間表會停用、並自動停用。

針對單一**Volume**啟用「活動追蹤」

您可以使用 ONTAP 系統管理員或 CLI 啟用活動追蹤。

關於這項工作

如果您搭配ONTAP 使用RBAC搭配使用REST API或System Manager、則必須建立自訂角色、才能管理「活動追蹤」的存取權限。請參閱 角色型存取控制 此程序。

系統管理員

步驟

1. 選擇*儲存>磁碟區*。選取所需的Volume。從個別Volume功能表中、選取File System（檔案系統）、然後選取「活動」索引標籤。
2. 確保*活動追蹤*已開啟、以檢視熱門目錄、檔案、用戶端和使用者的個別報告。
3. 若要在不重新整理的情況下更深入地分析資料、請選取*暫停重新整理*。您也可以下載資料以取得報告的CSV記錄。

CLI

步驟

1. 啟用活動追蹤：

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 使用命令檢查磁碟區的「活動追蹤」狀態是否為開啟或關閉：

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 啟用後、請使用ONTAP 「靜態系統管理程式」或ONTAP 「靜態API」來顯示「活動追蹤」資料。

啟用多個磁碟區的「活動追蹤」

您可以使用 System Manager 或 CLI 為多個磁碟區啟用「活動追蹤」。

關於這項工作

如果您搭配ONTAP 使用RBAC搭配使用REST API或System Manager、則必須建立自訂角色、才能管理「活動追蹤」的存取權限。請參閱 角色型存取控制 此程序。

系統管理員

針對特定磁碟區啟用

1. 選擇*儲存>磁碟區*。選取所需的Volume。從個別Volume功能表中、選取File System（檔案系統）、然後選取「活動」索引標籤。
2. 選取您要啟用「活動追蹤」的磁碟區。在Volume清單頂端、選取*更多選項*按鈕。選取*啟用活動追蹤*。
3. 若要在SVM層級檢視「活動追蹤」、請從*儲存設備> Volumes *選取您要檢視的特定SVM。導覽至「檔案系統」索引標籤、接著是「活動」、您會看到已啟用「活動追蹤」的磁碟區資料。

為所有磁碟區啟用

1. 選擇*儲存>磁碟區*。從功能表中選取SVM。
2. 瀏覽至*檔案系統*索引標籤、選擇*更多*索引標籤、即可在SVM中的所有磁碟區上啟用「活動追蹤」。

CLI

從 ONTAP 9.13.1 開始、您可以使用 ONTAP CLI 為多個磁碟區啟用「活動追蹤」。

步驟

1. 啟用活動追蹤：

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   使用 * 為指定儲存 VM 上的所有磁碟區啟用「活動追蹤」。

   使用 ！接著是 Volume 名稱、以啟用 SVM 上所有磁碟區的「活動追蹤」、但命名磁碟區除外。

2. 確認作業成功：

   ```
   volume show -fields activity-tracking-state
   ```

3. 啟用後、請使用ONTAP 「靜態系統管理程式」或ONTAP 「靜態API」來顯示「活動追蹤」資料。

啟用使用分析

從 ONTAP 9.12.1 開始、您可以啟用使用分析功能、查看磁碟區內的哪些目錄使用的空間最大。您可以檢視磁碟區中的目錄總數或磁碟區中的檔案總數。報告僅限於使用最多空間的 25 個目錄。

大型目錄的分析資料會每 15 分鐘重新整理一次。您可以檢查頁面頂端上次重新整理的時間戳記、以監控最近的重新整理。您也可以按一下 [下載] 按鈕，將資料下載至 Excel 活頁簿。下載作業會在背景執行、並顯示所選磁

碟區最近回報的資訊。如果掃描傳回時沒有任何結果、請確定磁碟區已上線。例如、事件將導致檔案系統分析重新建立其大型目錄清單。SnapRestore

步驟

1. 選擇*儲存>磁碟區*。選取所需的Volume。
2. 從個別Volume功能表中、選取*檔案系統*。然後選取「使用率」索引標籤。
3. 切換*分析*交換器以啟用使用分析。
4. System Manager會顯示一個長條圖、以遞減順序識別大小最大的目錄。

> 收集熱門目錄清單時、可能會顯示部分資料或根本沒有資料。ONTAP掃描進度可在掃描期間顯示的「使用情況」索引標籤中找到。

若要深入瞭解特定目錄、您可以 檢視檔案系統上的活動。

根據分析採取修正行動

從功能支援的9.9開始ONTAP 、您可以直接從「檔案系統分析」顯示器、根據目前的資料和想要的結果、採取修正行動。

刪除目錄與檔案

在檔案總管畫面中、您可以選取要刪除的目錄或個別檔案。目錄會以低延遲的快速目錄刪除功能刪除。（FAST目錄刪除功能也可從ONTAP 不啟用分析功能的情況下從版本號《支援》中開始使用。）

步驟

1. 按一下「儲存設備>磁碟區」、然後按一下「檔案總管」。

   當您將游標暫留在檔案或資料夾上時、會出現刪除選項。一次只能刪除一個物件。

> 刪除目錄和檔案時、新的儲存容量值不會立即顯示。

在儲存層中指派媒體成本、以比較非使用中資料儲存位置的成本

媒體成本是您根據儲存成本評估所指派的價值、代表您選擇的每GB貨幣。設定後、System Manager會使用指派的媒體成本、在您移動磁碟區時、將預估的節約成本用於專案。

您設定的媒體成本並非持續性的、只能針對單一瀏覽器工作階段進行設定。

步驟

1. 按一下 * 儲存 > Tiers* 、然後按一下所需的本機層（集合）方塊中的 * 設定媒體成本 * 。

   請務必選取作用中和非作用中的層級、以便進行比較。

2. 輸入貨幣類型和金額。

   當您輸入或變更媒體成本時、所有媒體類型都會進行變更。

移動磁碟區以降低儲存成本

根據分析顯示和媒體成本比較、您可以將磁碟區移至本機層中較便宜的儲存設備。

一次只能比較及移動一個Volume。

步驟

1. 啟用媒體成本顯示之後、按一下*儲存設備>層級*、然後按一下*磁碟區*。
2. 若要比較磁碟區的目的地選項、請按一下 ⋮ 對於該磁碟區、請按一下*移動*。
3. 在* Select目的地本機層*顯示中、選取目的地層以顯示預估成本差異。
4. 在比較選項之後、選取所需的階層、然後按一下*移動*。

以角色為基礎的存取控制：檔案系統分析

從《銷售資訊》9.12開始ONTAP 、ONTAP 這個功能包括預先定義的角色型存取控制（RBAC）角色、稱為 `admin-no-fsa`。。 `admin-no-fsa` 角色會授予系統管理員層級的權限、但會防止使用者執行與相關的作業 `files` 端點（例如檔案系統分析）、位於ONTAP Rest CLI、REST API和System Manager中。

如需的詳細資訊、請參閱 `admin-no-fsa` 角色、請參閱 叢集管理員的預先定義角色。

如果您使用ONTAP 的是ONTAP 發行版本不低於《支援資訊》9.12.1的版本、則需要建立專屬角色來控制檔案系統分析的存取。在ONTAP 版本的不含ONTAP 更新版本《R129.12.1.1》中、您必須透過ONTAP 《The R1221》或ONTAP 《The R1221 API》來設定RBAC權限。

系統管理員

從ONTAP 《支援資料》9.12.1開始、您可以使用System Manager設定檔案系統分析的RBAC權限。

步驟

1. 選擇*叢集>設定*。在「安全性」下、瀏覽至*使用者與角色*、然後選取 →。
2. 在*角色*下、選取 + Add 。
3. 提供角色名稱。在「角色屬性」下、提供適當的權限來設定使用者角色的存取或限制 "API 端點"。請參閱下表、瞭解設定檔案系統分析存取或限制的主要路徑和次要路徑。

限制	主要路徑	次要路徑
Volume活動追蹤	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVM上的活動追蹤	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
所有檔案系統分析作業	`/api/storage/volumes`	`/:uuid/files`

   您可以使用 `/*/` 而非UUID、可在端點設定所有磁碟區或SVM的原則。

   選擇每個端點的存取權限。

4. 選擇*保存*。
5. 若要將角色指派給使用者、請參閱 控制系統管理員存取權。

CLI

如果您使用ONTAP 的是ONTAP 版本不低於《21》的《21》、請使用ONTAP 《21》的《21》CLI建立自訂角色。

步驟

1. 建立預設角色以存取所有功能。

在建立限制角色之前、必須先完成這項作業、以確保「活動追蹤」上的角色僅受到限制：

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

2. 建立限制角色：

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

3. 授權角色存取SVM的Web服務：

   - `rest` 用於 REST API 呼叫
   - `security` 提供密碼保護
   - `sysmgr` 供 System Manager 存取

   ```
   vserver services web access create -vserver svm-name -name_ -name rest
   -role storageAdmin

   vserver services web access create -vserver svm-name -name security
   -role storageAdmin
   ```

```
vserver services web access create -vserver svm-name -name sysmgr -role
storageAdmin
```

4. 建立使用者。

   您必須針對要套用至使用者的每個應用程式、發出不同的create命令。在同一位使用者上多次呼叫建立、只會將所有應用程式套用至該位使用者、而不會每次都建立新的使用者。。 `http` 應用程式類型參數適用於 ONTAP REST API 和系統管理員。

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

5. 有了新的使用者認證資料、您現在可以登入System Manager、或使用ONTAP REST API來存取檔案系統分析資料。

更多資訊

- 叢集管理員的預先定義角色
- 使用 System Manager 控制系統管理員存取
- "深入瞭解RBAC角色和ONTAP REST API"

檔案系統分析考量

您應該瞭解與實作檔案系統分析相關的特定使用限制和潛在效能影響。

受SVM保護的關係

如果您已在包含SVM的磁碟區上啟用檔案系統分析功能、則分析資料不會複寫到目的地SVM。如果來源SVM必須在還原作業中重新同步、則您必須在還原後手動重新啟用所需磁碟區的分析功能。

效能考量

在某些情況下、啟用檔案系統分析可能會對初始中繼資料收集期間的效能造成負面影響。這是最常出現在使用率最大的系統上。為了避免在這類系統上啟用分析功能、您可以使用ONTAP 《支援系統管理程式》的效能監控工具。

如果延遲明顯增加、請參閱知識庫文章 "開啟NetApp ONTAP 功能的「NetApp功能性檔案系統分析」後、延遲時間會大幅或波動"。

掃描考量

當您啟用容量分析時、 ONTAP 會執行容量分析的初始化掃描。掃描會存取已啟用容量分析之 Volume 中所有檔案的中繼資料。掃描期間不會讀取檔案資料。從 ONTAP 9.14.1 開始、您可以使用 REST API 、系統管理員的檔案總管 索引標籤、或使用來追蹤掃描進度 `volume analytics show` CLI命令。如果發生節流事件、ONTAP 會提供通知。

掃描完成後、檔案系統分析會隨著檔案系統變更而即時更新、無需再次執行掃描。

掃描所需時間與磁碟區上的目錄和檔案數量成比例。由於掃描會收集中繼資料、因此檔案大小不會影響掃描時間。

如需初始化掃描的詳細資訊、請參閱 "TR-4867 ：檔案系統分析的最佳實務準則"。

最佳實務做法

您應該在不共用集合體的磁碟區上開始掃描。您可以使用命令查看目前裝載哪些磁碟區的集合體：

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

掃描執行時、磁碟區會繼續處理用戶端流量。建議您在預期用戶端流量較低的期間開始掃描。

如果用戶端流量增加、就會消耗系統資源、導致掃描所需時間較長。

從 ONTAP 9.12.1 開始、您可以在系統管理員和 ONTAP CLI 中暫停資料收集。

- 如果您使用的是 ONTAP CLI ：
  - 您可以使用命令暫停資料收集： `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - 一旦用戶端流量變慢、您就可以使用命令繼續資料收集： `volume analytics initialization resume -vserver svm_name -volume volume_name`
- 如果您使用的是 System Manager 、請在 Volume 功能表的 * 檔案總管 * 檢視中、使用 * 暫停資料收集 * 和 * 恢復資料收集 * 按鈕來管理掃描。

EMS 組態

EMS 組態概觀

您可以設定ONTAP 支援功能支援功能、將重要的EMS（事件管理系統）事件通知直接傳送至電子郵件地址、syslog伺服器、簡易管理網路傳輸協定（SNMP）traphost或Webhook應用程式、以便立即通知您需要立即注意的系統問題。

由於重要事件通知預設不會啟用、因此您需要設定EMS、將通知傳送至電子郵件地址、syslog伺服器、SNMP traphost或Webhook應用程式。

檢閱的特定版本 "《EMS參考資料》（英文ONTAP ）"。

如果您的EMS事件對應使用過時ONTAP 的支援功能（例如事件目的地、事件路由）、建議您更新對應。 "瞭解如何從已過時ONTAP 的等字指令更新EMS對應"。

使用System Manager設定EMS事件通知和篩選器

您可以使用System Manager來設定事件管理系統（EMS）傳送事件通知的方式、以便在系統問題需要您立即注意時通知您。

版本ONTAP	有了System Manager、您可以…
更新版本ONTAP	將事件傳送至遠端syslog伺服器時、請指定傳輸層安全性（TLS）傳輸協定。
更新版本ONTAP	設定電子郵件地址、syslog伺服器、Webhook應用程式、以及SNMP traphosts。
零點9.7至9.10.0 ONTAP	僅設定SNMP traphosts。 您可以使用ONTAP CLI設定其他EMS目的地。 請參閱 "EMS 組態概觀"。

您可以執行下列程序：

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

相關資訊

- "《環管系統參考資料》ONTAP"
- "使用CLI設定SNMP traphosts以接收事件通知"

新增**EMS**事件通知目的地

您可以使用System Manager來指定要將EMS訊息傳送到何處。

從S廳9.12.1開始ONTAP 、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。如需詳細資訊、請參閱 `event notification destination create` 手冊頁。

步驟

1. 按一下*叢集>設定*。
2. 在*通知管理*區段中、按一下 ⋮，然後單擊*查看事件目的地*。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 按一下 + Add 。
5. 指定名稱、EMS目的地類型及篩選條件。

> 如有需要、您可以新增篩選條件。 按一下「新增事件篩選器」。

6. 視您選取的EMS目的地類型而定、請指定下列項目：

若要設定…	指定或選取…
SNMP traphost	• TrapHost名稱
電子郵件 （從9.10.1開始）	• 目的地電子郵件地址 • 郵件伺服器 • 寄件者電子郵件地址
系統記錄伺服器 （從9.10.1開始）	• 伺服器的主機名稱或IP位址 • 系統記錄連接埠（從9.12.1開始） • 系統記錄傳輸（從9.12.1開始） 選取「* TCP Encrypted （ TCP加密*）」可啟用傳輸層安全性（TLS）傳輸協定。如果未輸入* Syslog連接埠*的值、則會根據* Syslog transport*選項使用預設值。
Webhook （從9.10.1開始）	• Webhook URL • 用戶端驗證（選取此選項以指定用戶端憑證）

建立新的**EMS**事件通知篩選器

從ONTAP 《E59.10.1》開始、您可以使用System Manager定義新的自訂篩選條件、以指定處理EMS通知的規則。

步驟

1. 按一下*叢集>設定*。

2. 在*通知管理*區段中、按一下 ⋮，然後單擊 * 查看事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 按一下 + Add 。
5. 指定名稱、然後選取是要從現有事件篩選器複製規則、還是要新增規則。
6. 視您的選擇而定、請執行下列步驟：

如果您選擇……	然後執行下列步驟…
從現有事件篩選器複製規則	1. 選取現有的事件篩選器。 2. 修改現有規則。 3. 如有需要、請按一下以新增其他規則 + Add 。
新增規則	指定每個新規則的類型、名稱模式、嚴重性及SNMP設陷類型。

編輯**EMS**事件通知目的地

從ONTAP 版本支援的版本起、您可以使用System Manager來變更事件通知目的地資訊。

步驟

1. 按一下*叢集>設定*。
2. 在*通知管理*區段中、按一下 ⋮，然後單擊*查看事件目的地*。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 在事件目的地名稱旁、按一下 ⋮，然後單擊*編輯*。
5. 修改事件目的地資訊、然後按一下「儲存」。

編輯**EMS**事件通知篩選器

從ONTAP 功能更新至功能更新至功能更新、您可以使用System Manager修改自訂的篩選條件、以變更事件通知的處理方式。

> 您無法修改系統定義的篩選條件。

步驟

1. 按一下*叢集>設定*。
2. 在*通知管理*區段中、按一下 ⋮，然後單擊 * 查看事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁、按一下 ⋮，然後單擊*編輯*。
5. 修改事件篩選器資訊、然後按一下「儲存」。

刪除**EMS**事件通知目的地

從ONTAP 《支援範本》（《支援範本》）9.10.1開始、您可以使用System Manager刪除EMS事件通知目的

地。

> 您無法刪除SNMP目的地。

步驟

1. 按一下*叢集>設定*。
2. 在*通知管理*區段中、按一下 ⋮，然後單擊 * 查看事件目的地 * 。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 在事件目的地名稱旁、按一下 ⋮，然後單擊 * 刪除 * 。

刪除**EMS**事件通知篩選器

從《軟件及應用程式》（2019）9.10.1開始ONTAP 、您可以使用System Manager刪除自訂的篩選條件。

> 您無法刪除系統定義的篩選條件。

步驟

1. 按一下*叢集>設定*。
2. 在*通知管理*區段中、按一下 ⋮，然後單擊 * 查看事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁、按一下 ⋮，然後單擊*刪除*。

使用**CLI**設定**EMS**事件通知

EMS 組態工作流程

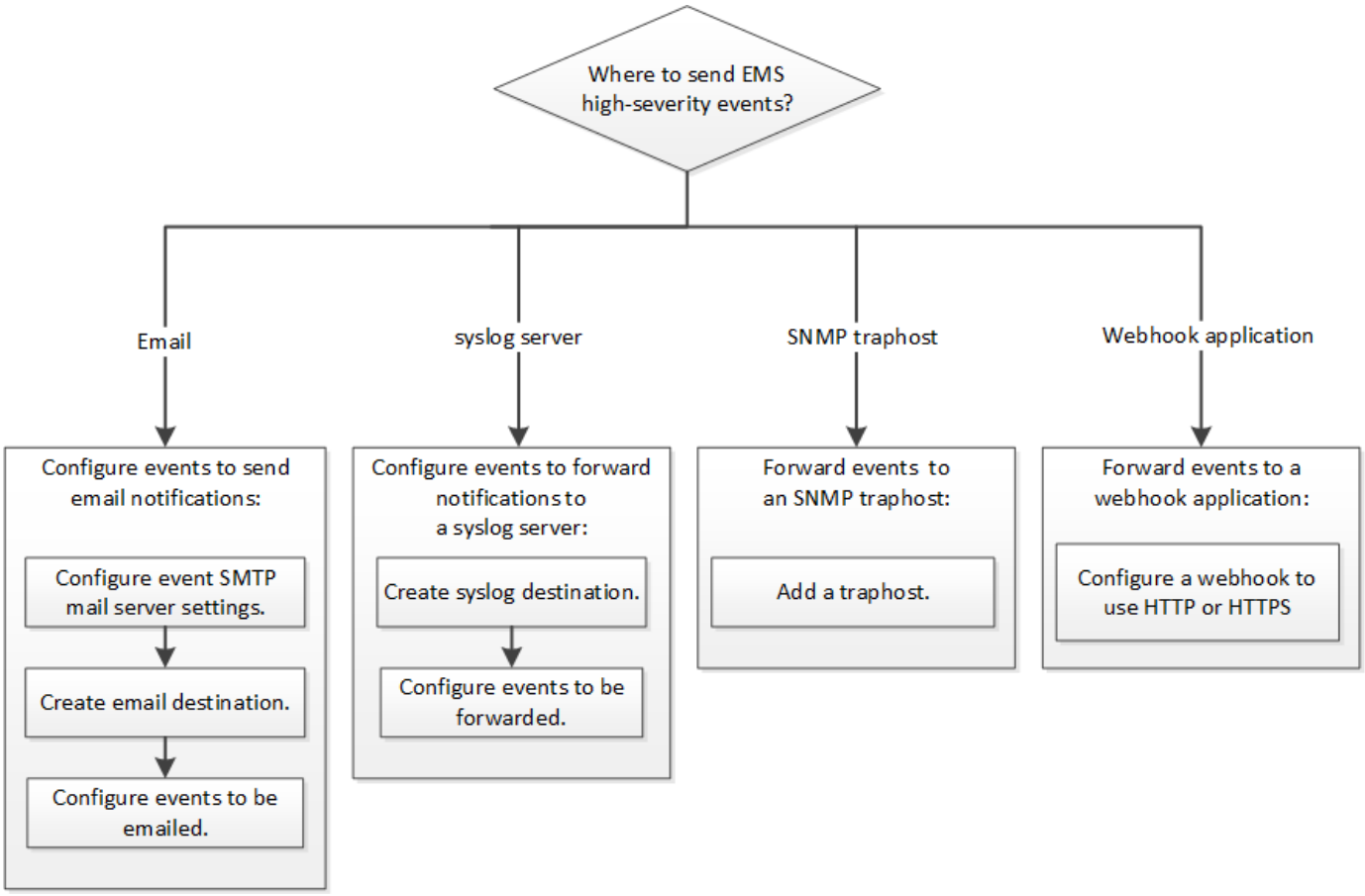
您必須將重要的EMS事件通知設定為以電子郵件傳送、轉送至syslog伺服器、轉送至SNMP traphost、或轉送至Webhook應用程式。這有助於您及時採取修正行動、避免系統中斷。

關於這項工作

如果您的環境已包含syslog伺服器、可用來彙總來自其他系統（例如伺服器和應用程式）的記錄事件、那麼使用syslog伺服器也能更輕鬆地從儲存系統發出重要的事件通知。

如果您的環境尚未包含syslog伺服器、則使用電子郵件進行重要事件通知會更容易。

如果您已將事件通知轉送到SNMP traphost、則可能需要監控該traphost是否有重要事件。



選擇

- 設定EMS以傳送事件通知。

如果您需要…	請參閱此…
將重要事件通知傳送至電子郵件地址的EMS	設定重要的EMS事件以傳送電子郵件通知
EMS可將重要事件通知轉送至syslog伺服器	設定重要的EMS事件、將通知轉送到syslog伺服器
如果您想要EMS將事件通知轉送到SNMP traphost	設定SNMP traphosts以接收事件通知
如果您想要EMS將事件通知轉送到Webhook應用程式	設定重要的EMS事件、將通知轉送到Webhook應用程式

設定重要的**EMS**事件以傳送電子郵件通知

若要接收最重要事件的電子郵件通知、您必須將EMS設定為針對重要活動的事件傳送電子郵件訊息。

您需要的產品

必須在叢集上設定DNS、才能解析電子郵件地址。

關於這項工作

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 設定事件的SMTP郵件伺服器設定：

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. 建立事件通知的電子郵件目的地：

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. 設定重要事件以傳送電子郵件通知：

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

設定重要的**EMS**事件、將通知轉送到**syslog**伺服器

若要在syslog伺服器上記錄最嚴重事件的通知、您必須將EMS設定為轉送重要活動訊號的事件通知。

您需要的產品

必須在叢集上設定DNS、才能解析syslog伺服器名稱。

關於這項工作

如果您的環境尚未包含用於事件通知的syslog伺服器、您必須先建立一個。如果您的環境中已包含用於記錄其他系統事件的syslog伺服器、您可能會想要使用該伺服器來處理重要的事件通知。

您可以在ONTAP 叢集執行時、在CLI輸入命令來執行此工作。

從S廳9.12.1開始ONTAP 、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。有兩個新參數可供使用：

`tcp-encrypted`

何時 `tcp-encrypted` 為指定 `syslog-transport`、ONTAP 驗證目的地主機的憑證來驗證其身分。預設值為 `udp-unencrypted`。

`syslog-port`

預設值 `syslog-port` 參數取決於的設定 `syslog-transport` 參數。如果 `syslog-transport` 設為 `tcp-encrypted`、 `syslog-port` 預設值為6514。

如需詳細資訊、請參閱 `event notification destination create` 手冊頁。

步驟

1. 建立重要事件的syslog伺服器目的地：

   ```
   event notification destination create -name syslog-ems -syslog syslog-server-
   ```

address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}

從ONTAP 功能變數9.12.1開始、可以指定下列值 `syslog-transport`：

- `udp-unencrypted` 無安全性的使用者資料包傳輸協定
- `tcp-unencrypted` 無安全性的傳輸控制傳輸協定
- `tcp-encrypted` -傳輸層安全性（TLS）的傳輸控制傳輸協定

預設傳輸協定為 `udp-unencrypted`。

2. 設定重要事件以將通知轉送到syslog伺服器：

   event notification create -filter-name *important-events* -destinations *syslog-ems*

設定**SNMP traphosts**以接收事件通知

若要在SNMP traphost上接收事件通知、您必須設定traphost。

您需要的產品

- 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。

關於這項工作

如果您尚未設定SNMP traphost來接收事件通知（SNMP設陷）、則必須新增一個。

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 如果您的環境尚未設定SNMP traphost來接收事件通知、請新增一個：

   system snmp traphost add -peer-address *snmp_traphost_name*

   SNMP預設支援的所有事件通知都會轉送到SNMP traphost。

設定重要的**EMS**事件、將通知轉送到**Webhook**應用程式

您可以設定ONTAP 將重要事件通知轉送至Webhook應用程式。所需的組態步驟取決於您選擇的安全性層級。

準備設定**EMS**事件轉送

在設定ONTAP 將事件通知轉送到Webhook應用程式之前、您應該考慮幾個概念和要求。

Webhook應用程式

您需要能夠接收ONTAP 不必要事件通知的Webhook應用程式。Webhook是使用者定義的回撥例行工作、可延伸執行遠端應用程式或伺服器的功能。Webhooks是由用戶端呼叫或啟動（本例ONTAP 為示例）、方法是將HTTP要求傳送至目的地URL。具體而言ONTAP 、將HTTP POST要求傳送至裝載Webhook應用程式的伺服器、以及以XML格式設定的事件通知詳細資料。

安全選項

視傳輸層安全性（TLS）傳輸協定的使用方式而定、有多種安全選項可供選擇。您選擇的選項會決定所需ONTAP 的功能組態。

> TLS是一種在網際網路上廣泛使用的密碼編譯傳輸協定。它使用一或多個公開金鑰憑證來提供隱私、資料完整性和驗證。這些憑證由信任的憑證授權單位核發。

HTTP

您可以使用HTTP來傳輸事件通知。使用此組態時、連線不安全。不驗證不驗證ONTAP 客戶端和Webhook應用程式的身分。此外、網路流量並未加密或受到保護。請參閱 "設定Webhook目的地以使用HTTP" 以取得組態詳細資料。

HTTPS

為了提高安全性、您可以在裝載Webhook例行工作的伺服器上安裝憑證。驗證Webhook應用程式伺服器及雙方身分的HTTPS傳輸協定、ONTAP 以確保網路流量的隱私性和完整性。請參閱 "設定 Webhook 目的地以使用 HTTPS" 以取得組態詳細資料。

HTTPS搭配相互驗證

您可以在ONTAP 發出Webbook要求的系統上安裝用戶端憑證、進一步強化HTTPS安全性。除了驗證Webhook應用程式伺服器的身分、並保護網路流量之外、Webhook應用程式還會驗證該客戶端的身分。ONTAP ONTAP這種雙向對等驗證稱為「相互TLS」。請參閱 "設定Webhook目的地使用HTTPS進行相互驗證" 以取得組態詳細資料。

相關資訊

- "傳輸層安全性（TLS）傳輸協定1.3版"

設定**Webhook**目的地以使用**HTTP**

您可以設定ONTAP 使用HTTP將事件通知轉送至Webhook應用程式。這是最不安全的選項、但設定起來最簡單。

步驟

1. 建立新目的地 `restapi-ems` 若要接收事件：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   在上述命令中、您必須使用* HTTP配置作為目的地。

2. 建立連結的通知 `important-events` 使用篩選 `restapi-ems` 目的地：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

設定 Webhook 目的地以使用 HTTPS

您可以設定 ONTAP 、使用 HTTPS 將事件通知轉寄至 Webhook 應用程式。使用伺服器憑證來確認Webhook應用程式的身分識別、以及保護網路流量。ONTAP

開始之前

- 為Webhook應用程式伺服器產生私密金鑰和憑證
- 讓root憑證可安裝在ONTAP 整個過程中

步驟

1. 在裝載Webhook應用程式的伺服器上安裝適當的伺服器私密金鑰和憑證。具體的組態步驟取決於伺服器。
2. 將伺服器根憑證安裝在ONTAP

   ```
   security certificate install -type server-ca
   ```

   命令會要求提供憑證。

3. 建立 `restapi-ems` 接收事件的目的地：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   在上述命令中、您必須使用* HTTPS *配置作為目的地。

4. 建立連結的通知 `important-events` 使用新的篩選器 `restapi-ems` 目的地：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

設定Webhook目的地使用HTTPS進行相互驗證

您可以設定ONTAP 將事件通知轉送至Webhook應用程式、使用HTTPS搭配相互驗證。使用此組態有兩個憑證。使用伺服器憑證來確認Webhook應用程式的身分、並保護網路流量。ONTAP此外、裝載Webhook的應用程式會使用用戶端憑證來確認ONTAP 該客戶端的身分。

開始之前

您必須先執行下列步驟、才能設定ONTAP 使用功能：

- 為Webhook應用程式伺服器產生私密金鑰和憑證
- 讓root憑證可安裝在ONTAP 整個過程中
- 為ONTAP 該驗證用戶端產生私密金鑰和憑證

步驟

1. 執行工作的前兩個步驟 "設定 Webhook 目的地以使用 HTTPS" 安裝伺服器憑證、ONTAP 以便驗證伺服器的身分。
2. 在Webhook應用程式中安裝適當的根和中繼憑證、以驗證用戶端憑證。
3. 將用戶端憑證安裝ONTAP 在下列項目中：

```
security certificate install -type client
```

命令會要求提供私密金鑰和憑證。

4. 建立 `restapi-ems` 接收事件的目的地：

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

在上述命令中、您必須使用* HTTPS *配置作為目的地。

5. 建立連結的通知 `important-events` 使用新的篩選器 `restapi-ems` 目的地：

```
event notification create -filter-name important-events -destinations restapi-
ems
```

更新過時的**EMS**事件對應

EMS事件對應模型

在版本不含故障碼的9.0之前ONTAP 、EMS事件只能根據事件名稱模式的相符結果對應至事件目的地。ONTAP 命令集 (`event destination`、 `event route`）使用此模型的 ONTAP 最新版本仍然可用，但從 ONTAP 9.0 開始已被淘汰。

從 ONTAP 9.0 開始、 ONTAP EMS 事件目的地對應的最佳實務做法是使用更具擴充性的事件篩選器模型、在多個欄位上使用進行模式比對 `event filter`、 `event notification`和 `event notification destination` 命令集。

如果您的 EMS 對應是使用過時的命令進行設定、您應該更新對應以使用 `event filter`、 `event notification`和 `event notification destination` 命令集。

事件目的地有兩種類型：

1. 系統產生的目的地：有五個系統產生的事件目的地（預設為建立）
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     某些系統產生的目的地是為了特殊目的而設計。例如、asup目的地會將CallHome.*事件路由到AutoSupport 位在畫面上的這個動作模組ONTAP 、以產生AutoSupport 各種訊息。

2. * 使用者建立的目的地 * ：這些目的地是使用手動建立的 `event destination create` 命令。

```
cluster-1::event*> destination show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

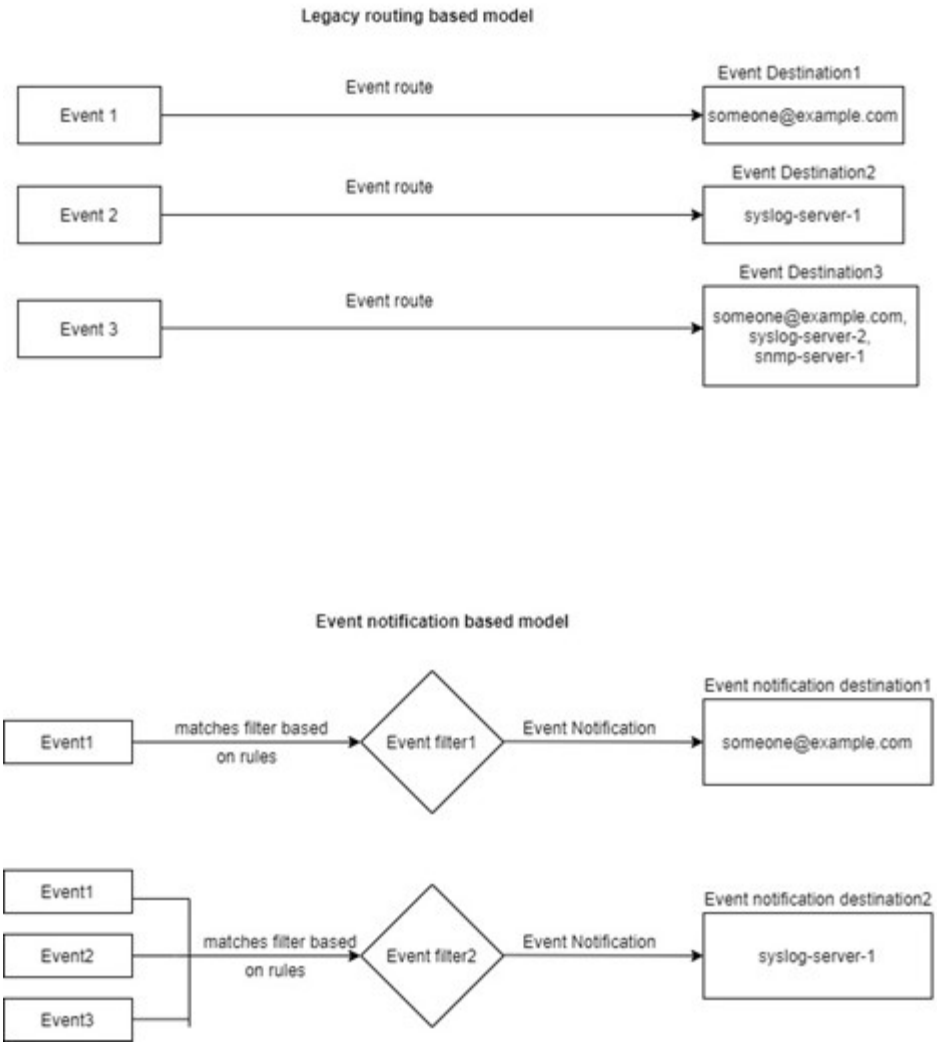
在過時的模型中、 EMS 事件會使用個別對應至目的地 `event route add-destinations` 命令。

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
--------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

全新且可擴充的EMS事件通知機制、是以事件篩選器和事件通知目的地為基礎。如需新事件通知機制的詳細資訊、請參閱下列知識庫文章：

- "事件管理系統概述ONTAP （適用於）。9."



更新**EMS**事件對應、以取代過時**ONTAP** 的**EISO**命令

如果您的 EMS 事件對應目前是使用過時的 ONTAP 命令集進行設定 (`event destination`、 `event route`）、您應該遵循此程序來更新對應以使用 `event filter`、 `event notification`和 `event notification destination` 命令集。

步驟

1. 使用列出系統中的所有事件目的地 `event destination show` 命令。

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. 針對每個目的地、使用列出對應至目的地的事件 `event route show -destinations <destination name>` 命令。

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                            Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort           NOTICE         test           0       0
raid.aggr.autoGrow.success         NOTICE         test           0       0
raid.aggr.lock.conflict            INFORMATIONAL  test           0       0
raid.aggr.log.CP.count             DEBUG          test           0       0
4 entries were displayed.
```

3. 建立對應的 `event filter` 其中包括所有這些事件子集。
例如、如果您只想要包含 `raid.aggr.*` 事件、請使用萬用字元 `message-name` 建立篩選器時的參數。您也可以為單一事件建立篩選器。

> 您最多可以建立50個事件篩選器。

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 建立 `event notification destination` 針對每個 `event destination` 端點（例如 SMTP/SNMP/Syslog ）

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. 將事件篩選器對應至事件通知目的地、以建立事件通知。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                      Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. 針對每個項目重複步驟 1-5 `event destination` 那有 `event route` 對應：

路由至 SNMP 目的地的事件應對應至 `snmp-traphost` 事件通知目的地。SNMP traphost目的地使用系統設定的SNMP traphost。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```