



# 事件、效能和健全狀況監控

## ONTAP 9

NetApp  
March 12, 2026

# 目錄

事件、效能和健全狀況監控	1
使用System Manager監控叢集效能	1
使用 ONTAP 系統管理器監控叢集效能	1
了解如何在 ONTAP System Manager 儀表板上查看叢集	1
在 ONTAP 系統管理員中辨識熱捲和其他對象	2
在 ONTAP 系統管理員中修改 QoS	3
在 ONTAP 系統管理員中監控風險	3
利用 ONTAP System Manager 洞察優化您的系統	5
在 ONTAP 系統管理員中設定本機 FPolicy	7
使用CLI監控及管理叢集效能	7
ONTAP效能管理工作流程	7
執行基礎架構檢查	8
管理工作負載	15
使用統一管理器監控和管理叢集效能	34
使用 ONTAP Unified Manager 監控叢集效能	34
了解ONTAP Active IQ Unified Manager效能監控與管理	35
監控效能	35
使用ONTAP Active IQ Digital Advisor檢視系統效能	45
使用 ONTAP 資料基礎架構洞察監控叢集效能	45
監控、疑難排解及最佳化所有資源	45
稽核記錄	46
瞭解 ONTAP 稽核記錄實作	46
瞭解 ONTAP 稽核記錄的變更	47
顯示 ONTAP 稽核記錄內容	47
管理 ONTAP 稽核 Get 要求設定	48
啟用ONTAP跨叢集審核	49
管理 ONTAP 稽核記錄目的地	50
AutoSupport	51
瞭解 AutoSupport	52
規劃	64
設定	70
使用 AutoSupport 上傳檔案	72
疑難排解	74
健全狀況監控	80
瞭解 ONTAP 系統健全狀況監控	80
瞭解 ONTAP 健全狀況監控元件	81
瞭解 ONTAP 系統健全狀況警示回應	81
瞭解 ONTAP 系統健全狀況警示自訂功能	82
瞭解 ONTAP AutoSupport 健全狀況警示觸發程序	82

瞭解可用的 ONTAP 叢集健全狀況監視器	83
自動接收 ONTAP 系統健全狀況警示	84
回應降級的 ONTAP 系統健全狀況	84
瞭解如何回應降級的 ONTAP 系統健全狀況	85
用於監控 ONTAP 系統健全狀況的命令	88
檢視 ONTAP 環境資訊	91
檔案系統分析	91
瞭解 ONTAP 檔案系統分析	91
啟用 ONTAP 檔案系統分析	93
使用 FSA 查看 ONTAP 檔案系統活動	96
使用 FSA 啟用 ONTAP 活動追蹤	98
使用 FSA 啟用 ONTAP 使用情況分析	100
根據 FSA 中的 ONTAP 分析採取糾正措施	101
透過 ONTAP 檔案系統分析，以角色為基礎的存取控制	102
ONTAP 檔案系統分析的考量事項	104
EMS 組態	106
瞭解 ONTAP EMS 組態	106
使用系統管理員設定 ONTAP EMS 事件通知和篩選器	106
使用 CLI 設定 EMS 事件通知	109
更新過時的 EMS 事件對應	115

# 事件、效能和健全狀況監控

## 使用System Manager監控叢集效能

### 使用 ONTAP 系統管理器監控叢集效能

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。

#### 關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASAA1K、ASAA90、ASAA70、ASA A50、ASA A30、ASAA20 或 ASA C30），請遵循[這些步驟](#)監控您的叢集效能。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

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。

### 了解如何在 ONTAP System Manager 儀表板上查看叢集

System Manager 儀表板可從單一位置快速完整地檢視 ONTAP 叢集。

使用 System Manager 儀表板、您可以一眼檢視重要警示和通知的相關資訊、儲存層和磁碟區的效率和容量、叢集中可用的節點、高可用度（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。

儀表板包含四個面板、如下所述：

#### 健全狀況

「健全狀況」檢視會顯示叢集中所有可搜尋節點整體健全狀況的相關資訊。

「健全狀況」檢視也會顯示叢集層級的錯誤和警告、例如未經設定的節點詳細資料、指出可修改以提升叢集效能的特性。

按一下 [→](#) 以展開「健全狀況」檢視、以取得叢集的概觀、例如叢集名稱、版本、叢集建立日期和時間等。您也可以監控與叢集相關節點健全狀況相關的統計資料。您可以管理標記、讓您群組和識別環境中的資源。Insights 區段可協助您最佳化系統的容量、安全性法規遵循及組態。

## 容量

容量檢視會顯示叢集的儲存空間。您可以檢視已使用的邏輯空間總計、已使用的實體空間總計、以及可用的磁碟空間。

您可以選擇向 ActiveIQ 註冊、以檢視歷史叢集資料。按一下 [→](#) 以展開容量檢視、以查看與叢集相關聯的階層概觀。您可以檢視每個階層的容量資訊：總空間、已用空間和可用空間。會顯示處理量、IOPS 和延遲的詳細資料。["在 System Manager 中深入瞭解這些容量測量"](#)。

您可以選擇使用容量檢視來新增本機層或雲端層。如需詳細資訊、請 ["檢視叢集的容量"](#) 參閱。

## 網路

「網路」檢視會顯示屬於網路一部分的實體連接埠、網路介面和儲存 VM。

「網路」檢視會顯示連線至網路的用戶端類型。每個網路連線的用戶端都會以數字表示（例如「NVMe / FC 16」）。選取數字以檢視每個網路元件的特定詳細資料。

按一下 [→](#) 以查看涵蓋網路上連接埠、網路介面、儲存 VM 和主機的廣泛全頁網路檢視。

## 效能

「效能」檢視會顯示效能統計資料、以協助監控 ONTAP 叢集的健全狀況和效率。這些統計資料包括主要的叢集效能指標、例如延遲、處理量和 IOPS、以圖表形式呈現。

「效能」檢視會依日期、小時、週或年、以不同的時間間隔顯示效能統計資料。您可以使用各種圖表快速分析叢集效能、並識別可能需要最佳化的特性。這項快速分析可協助您決定如何新增或移動工作負載。您也可以查看尖峰使用時間、以規劃可能的變更。

效能檢視會顯示與延遲、處理量和 IOPS 相關的整體效能指標。

從 9.15.1 開始、效能檢視會增強、以顯示與延遲、處理量和 IOPS 相關的讀取、寫入、其他和總效能指標圖表。其他度量包括任何非讀取或寫入的作業。

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。如果無法取得叢集效能的相關資訊、將不會顯示圖表。

按一下 [↗](#) 以查看各小時、日、週、月和年的效能指標全頁檢視。您也可以下載本機系統效能指標的報告。

## 在 ONTAP 系統管理員中辨識熱捲和其他對象

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。

## 在 ONTAP 系統管理員中修改 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  \* 編輯\*。

## 在 ONTAP 系統管理員中監控風險

從 ONTAP 9.10.0 開始、您可以使用系統管理員來監控 Active IQ 數位顧問（也稱為數位顧問）回報的風險。從版本《21》開始ONTAP、您可以使用System Manager來確認風險。

NetApp 數位顧問報告降低風險並改善儲存環境效能與效率的機會。有了 System Manager、您就能瞭解數位顧問所回報的風險、並獲得可據以行動的情報、協助您管理儲存設備、實現更高的可用度、改善安全性及最佳的儲存效能。

### 連結至您的數位顧問帳戶

若要從 Digital Advisor 接收風險相關資訊、您應該先從 System Manager 連結至 Digital Advisor 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 Digital Advisor 認證。
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 9.10.0 開始、您可以從系統管理員的儀表板檢視數位顧問報告的風險數。

### 開始之前

您必須建立從 System Manager 到 Digital Advisor 帳戶的連線。請參閱 [連結至您的數位顧問帳戶](#)。

### 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 9。10.0 開始、您可以從系統管理員檢視數位顧問報告的風險如何依影響區域分類。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

您必須建立從 System Manager 到 Digital Advisor 帳戶的連線。請參閱 [連結至您的數位顧問帳戶](#)。

### 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」



在您確認風險之後、需要幾分鐘時間才能將變更反映在數位顧問建議清單中。

### 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\*。



在您不承認風險之後、需要幾分鐘時間才能將變更反映在數位顧問建議清單中。

## 利用 **ONTAP System Manager** 洞察優化您的系統

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

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循[這些步驟](#)查看有助於您優化系統的見解。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

從ONTAP 9.11.1 開始，您可以在系統管理員中查看洞察，以協助您最佳化系統的容量、安全性合規性和配置。

- 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。如需更多資訊、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。
-  顯示與組態相關的洞見。
-  顯示所有洞見。

## 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。若要取消關注，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 、然後選取 \* 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。如果您之前忽略了某個見解，則可以透過確保核取方塊中有勾選來取消忽略它。
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 、然後選取 \* 匯出 \*。

## 在 ONTAP 系統管理員中設定本機 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["FPolicy組態類型"](#)參閱。

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。

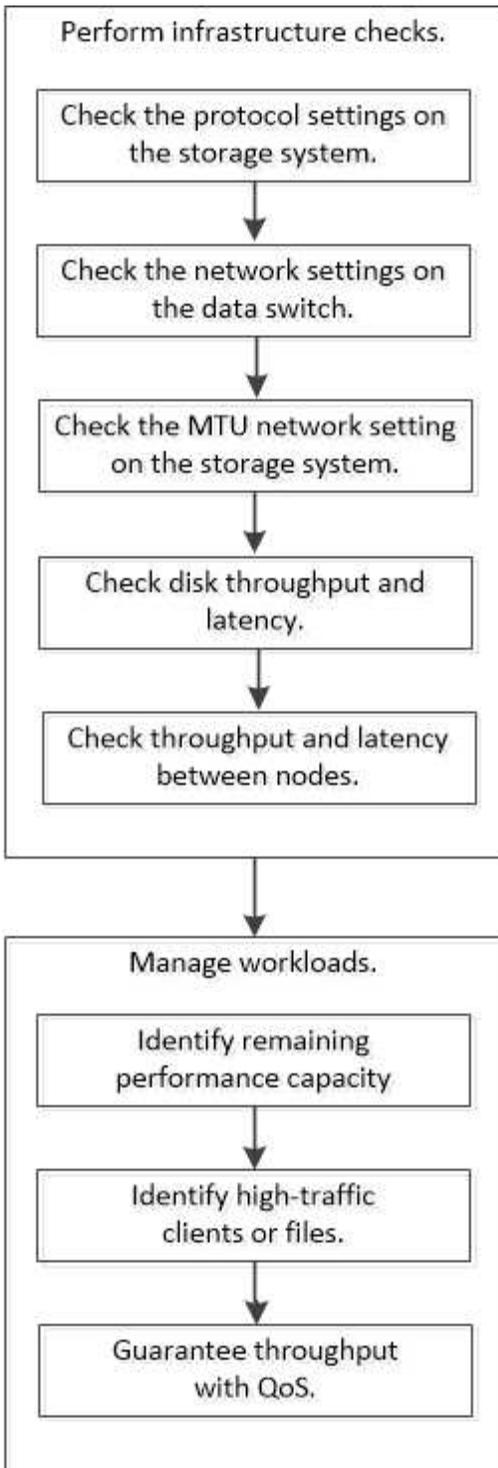
因此、強烈建議您修改擴充功能清單、以符合您環境的需求。請參閱 ["如何從系統管理員使用系統管理員建立的原生 FPolicy 組態中移除副檔名、以重新建立原則"](#)。

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

### ONTAP 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ONTAP NFS TCP 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。

## 開始之前

- 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ONTAP iSCSI TCP 讀取/寫入大小

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。

## 開始之前

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 -vserver 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ONTAP CIFS/SMB 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ONTAP FC 適配器連接埠速度

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。

## 開始之前

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
```

如"[指令參考資料ONTAP](#)"需詳細 `network fcp adapter modify` 資訊，請參閱。

2. 檢查連接埠介面卡的最大速度：

```
fcp adapter show -instance
```

如"[指令參考資料ONTAP](#)"需詳細 `fcp adapter show` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `network interface modify` 資訊，請參閱。

#### 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ONTAP網路設置

雖然您必須在用戶端、伺服器 and 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。

#### 步驟

1. 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ONTAP MTU 網路設置

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。如需更多資訊、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
```

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

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ONTAP磁碟吞吐量和延遲

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
      Disk      Node      Busy Total  Read  Write  Read   Write   *Latency
      -----  -
      (%)      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

```

#### 相關資訊

- ["統計磁碟顯示"](#)

#### 檢查節點之間的ONTAP吞吐量和延遲

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。

#### 開始之前

- 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
```

範例輸出（輸出詳細資料可能會因您的 ONTAP 版本而異）：

```
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
```

如"[指令參考資料ONTAP](#)"需詳細 `network test-path` 資訊，請參閱。

### 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

識別 **ONTAP** 中的剩餘效能容量

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。

開始之前

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"[指令參考資料ONTAP](#)"需詳細 `statistics start` 資訊，請參閱。

3. 顯示即時保留空間統計資訊：

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

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.

如"[指令參考資料ONTAP](#)"需詳細 `statistics show` 資訊，請參閱。

識別 **ONTAP** 中的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。

開始之前

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
```

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-vs4	nfs	668
172.17.180.169	vs3	siderop1-vs3	nfs	337
172.17.180.171	vs3	siderop1-vs3	nfs	142
172.17.180.170	vs3	siderop1-vs3	nfs	137
172.17.180.123	vs3	siderop1-vs3	nfs	137
172.17.180.171	vs4	siderop1-vs4	nfs	95
172.17.180.169	vs4	siderop1-vs4	nfs	92
172.17.180.123	vs4	siderop1-vs4	nfs	92
172.17.180.153	vs3	siderop1-vs3	nfs	0

如"指令參考資料ONTAP"需詳細 `statistics top client show` 資訊，請參閱。

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
```

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-vs4 22
/vol/vol1/vm69-write.dat     vol1      vs3 siderop1-vs3 6
/vol/vol2/vm171.dat          vol2      vs3 siderop1-vs3 2
/vol/vol2/vm169.dat          vol2      vs3 siderop1-vs3 2
/vol/vol2/p123.dat           vol2      vs4 siderop1-vs4 2
/vol/vol2/p123.dat           vol2      vs3 siderop1-vs3 2
/vol/vol1/vm171.dat          vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat          vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat          vol1      vs4 siderop1-vs3 2
/vol/vol1/p123.dat           vol1      vs4 siderop1-vs4 2

```

如"指令參考資料ONTAP"需詳細 `statistics top file show` 資訊，請參閱。

## 保證QoS的處理量

透過 **ONTAP** 中的 **QoS** 總覽來保證傳輸量

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。

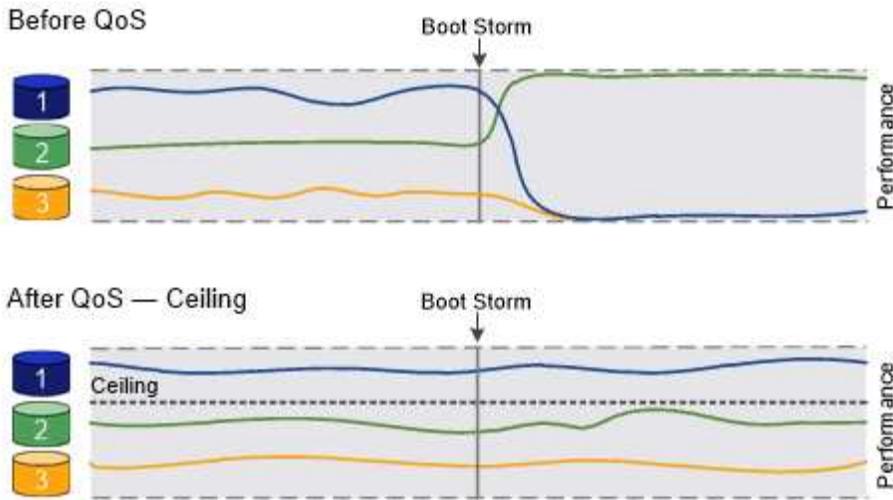
### 處理量上限 ( QoS 上限)

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、qtrees或LUN、或SVM中的所有磁碟區、檔案、qtrees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



### 處理量層（QoS 最低）

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。

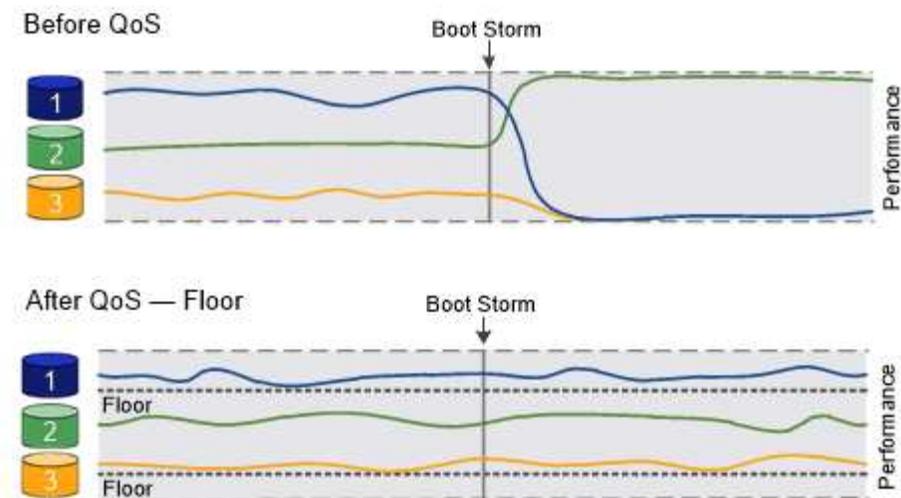
從 ONTAP 9.13.1 開始[[adaptive-qos-templates](#)]，您可以使用設定 SVM 範圍的處理量層。在 9.13.1 之前的 ONTAP 版本中、定義處理量層的原則群組無法套用至 SVM。



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。



### 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。

### 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	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 <sup>1</sup></li> <li>• ONTAP Select Premium 搭配 SSD <sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• 搭載SSD的高階版ONTAP Select</li> </ul>	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

<sup>1</sup> 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	更新版本ONTAP	ONTAP 9.7 至 9.4	ONTAP 9.3 及更早版本
Volume	是的	是的	是的
檔案	是的	是的	是的
LUN	是的	是的	是的
SVM	是的	是的	是的
流通量FlexGroup	是的	是的	是（僅限 ONTAP 9.3）
qtree <sup>1</sup>	是的	否	否
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	否

<sup>1</sup> 從ONTAP 9.9.1 開始，啟用 SMB 的FlexVol和FlexGroup磁碟區中的 qtree 也支援 SMB 存取。從ONTAP 9.8 開始，啟用 NFS 的FlexVol和FlexGroup磁碟區中的 qtree 支援 NFS 存取。

## 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	ONTAP 9.13.1 及更新版本	零點9.8至9.13.0 ONTAP	ONTAP 9.4 至 9.7	ONTAP 9.3
Volume	是的	是的	是的	是的
檔案	是的	是的	是的	是的
LUN	是的	是的	是的	是的
SVM	是的	否	否	否
流通量FlexGroup	是的	是的	是的	否
qtree <sup>1</sup>	是的	是的	否	否
每個原則群組有多個工作負載	是的	是的	是的	否
非共用原則群組	是的	是的	是的	否

<sup>1</sup> 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	ONTAP 9.13.1 及更新版本	零點9.4至9.13.0 ONTAP	ONTAP 9.3
Volume	是的	是的	是的
檔案	是的	是的	否
LUN	是的	是的	否
SVM	是的	否	否
流通量FlexGroup	是的	是的	否
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	更新版本ONTAP	ONTAP 9.3 及更早版本
每個叢集的工作負載上限	40、000	12、000
每個節點的工作負載上限	40、000	12、000
原則群組上限	12、000	12、000

### 啟用或停用ONTAP吞吐量底線 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	<code>qos settings throughput-floors-v2 -enable false</code>
啟用樓層v2	<code>qos settings throughput-floors-v2 -enable true</code>



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
```

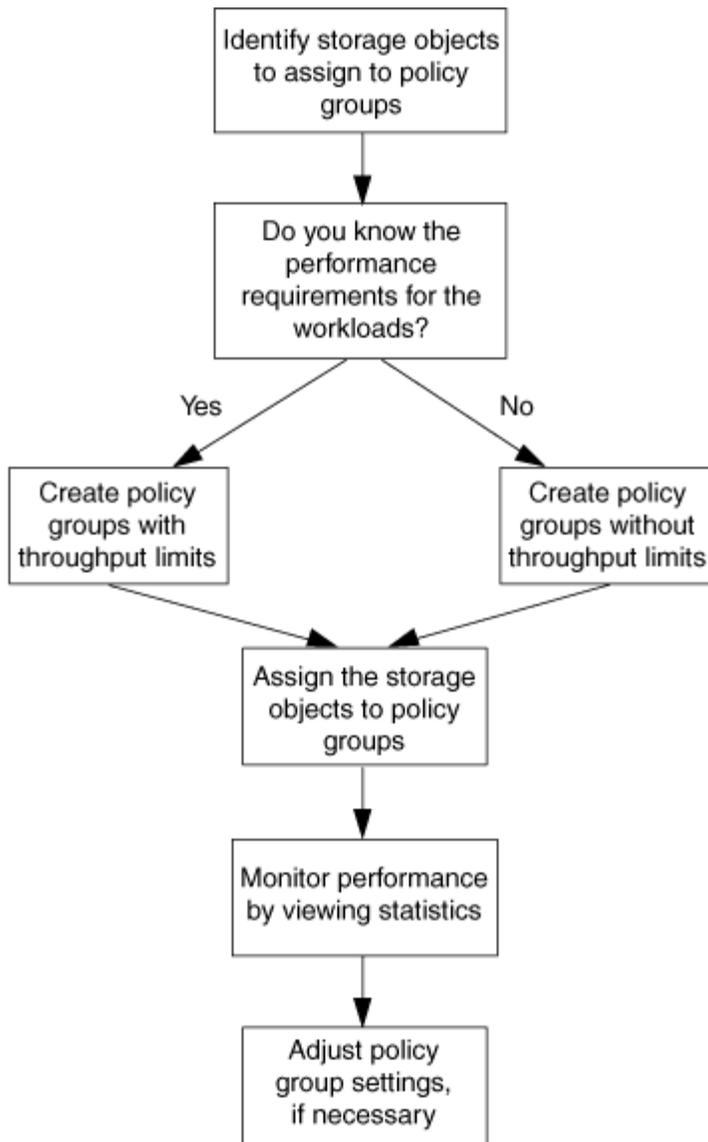
在來源叢集和目的地叢集上執行命令。

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

如"[指令參考資料ONTAP](#)"需詳細 `qos settings throughput-floors-v2` 資訊，請參閱。

#### ONTAP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。



#### QoS 策略群組分配限制

從ONTAP 9.18.1 開始，您可以使用嵌套的 QoS 策略，該策略允許將策略群組指派給包含物件（例如 SVM）及其子物件（例如磁碟區）。在多租用戶環境中，嵌套的 QoS 策略使管理員能夠將 SVM 上的 QoS 限制細分到 SVM 內的各個磁碟區和 qtree，從而能夠在運算環境中平衡儲存資源，同時還能優先處理關鍵任務工作負載。

以下物件對支援嵌套 QoS 策略：

- SVM 和 SVM 包含的FlexVol或FlexGroup磁碟區。
- FlexVol或FlexGroup卷以及卷內的 qtree。

對於嵌套的 QoS 策略，採用最嚴格的適用策略。

下表列出了各項限制。

如果您指派...	那麼你就無法將其指派到策略群組...
SVM到原則群組	SVM 中包含的任何儲存物件。  <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  如果您執行的是ONTAP 9.18.1，則 SVM 中所包含的FlexVol和FlexGroup磁碟區_可以_指派給策略群組。 </div>
磁碟區至原則群組	包含該磁碟區或任何子 LUN 的 SVM。  <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  如果您執行的是ONTAP 9.18.1 及更高版本，則包含磁碟區的 SVM _可以_指派給策略群組。此外，也可以分配FlexVol或FlexGroup磁碟區中的 qtree。 </div>
LUN至原則群組	包含 LUN 的磁碟區或 SVM
檔案至原則群組	包含文件的磁碟區或 SVM

#### 使用 ONTAP QoS 原則群組設定處理量上限

QoS 最大值或吞吐量上限可確保工作負載的吞吐量不會超過最大 IOPS 或 MBps 數量，或無論競爭工作負載為何，IOPS 和 MBps 都不會超過最大值。設定吞吐量上限可防止較不重要的工作負載消耗過多的效能資源，並降低更重要工作負載的效能。

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。

#### 開始之前

- 您必須是叢集管理員才能建立原則群組並將原則群組套用至 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` 指定非共用原則群組的命令。

- 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"[指令參考資料ONTAP](#)"需詳細 `qos policy-group create` 資訊，請參閱。

您可以使用 `qos policy-group modify` 命令來調整處理量上限。

以下範例建立共享策略群組 `pg-vs1`，最大吞吐量為 5,000 IOPS：

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

以下範例建立了一個非共享策略群組 `pg-vs3`，其最大處理量為 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
```

以下範例建立無吞吐量限制的非共用策略群組 `pg-vs4`：

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

如"[指令參考資料ONTAP](#)"需詳細 `qos policy-group modify` 資訊，請參閱。

### 2. 將原則群組套用至SVM、檔案、磁碟區或LUN：

```
vserver create -vserver <SVM> -qos-policy-group <policy_group>
```

您可以使用 `vserver modify` 指令將不同的策略群組套用到儲存物件。

以下範例將策略群組 `pg-vs1` 應用於 SVM `vs1`：

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

以下範例將策略群組 `pg-app` 應用於磁碟區 `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"[指令參考資料ONTAP](#)"需詳細 `qos statistics performance show` 資訊，請參閱。



監控叢集的效能。請勿使用主機上的工具來監控效能。

以下範例顯示原則群組效能：

```
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
```



監控叢集的效能。請勿使用主機上的工具來監控效能。

以下範例展示了工作負載效能：

```
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
```

如"[指令參考資料ONTAP](#)"需詳細 `qos statistics workload performance show` 資訊，請參閱。

您可以使用 `qos statistics workload latency show` 命令來檢視 QoS 工作負載的詳細延遲統計資料。如"[指令參考資料ONTAP](#)"需詳細 `qos statistics workload latency show` 資訊，請參閱。

使用 **ONTAP QoS** 原則群組設定處理量下限

QoS 最低標準或吞吐量下限保證工作負載的吞吐量不會低於最低 IOPS 或 MBps 值，或無論是否存在競爭工作負載，IOPS 和 MBps 值都不會低於最低值。設定吞吐量下限可確保關鍵工作負載獲得優先處理，並滿足最低效能要求。

您可以使用 `min-throughput` 欄位來定義策略群組的儲存物件工作負載吞吐量下限 (QoS Min)。您可以在建立或修改儲存物件時套用該策略群組。

開始之前

- 您必須是叢集管理員、才能建立原則群組。

關於這項工作

- 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。
- 從 ONTAP 9.8 開始、您可以指定 IOPS 或 MBps 或 IOPS 和 MBps 的處理量下限。
- 從 ONTAP 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"[指令參考資料ONTAP](#)"需詳細 `qos policy-group create` 資訊，請參閱。

以下範例建立共享策略群組 pg-vs2，其最小吞吐量為 1,000 IOPS：

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

以下範例建立無吞吐量限制的非共用策略群組 pg-vs4：

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

您可以使用 `qos policy-group modify` 指令來調整吞吐量下限。在 `qos policy-group modify` 中深入了解 "[指令參考資料ONTAP](#)"。

### 3. 將原則群組套用至磁碟區或LUN：

```
vserver create -vserver <SVM> -qos-policy-group <policy_group>
```

您可以使用 `vserver modify` 指令將不同的策略群組套用到儲存物件。

以下範例將策略群組 pg-app2 應用於磁碟區 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
```



監控叢集的效能。請勿使用主機上的工具來監控效能。

以下範例顯示原則群組效能：

```
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
```

如"[指令參考資料ONTAP](#)"需詳細 `qos statistics performance show` 資訊，請參閱。

## 5. 監控工作負載效能：

```
qos statistics workload performance show
```



監控叢集的效能。請勿使用主機上的工具來監控效能。

以下範例展示了工作負載效能：

```
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
```

如"[指令參考資料ONTAP](#)"需詳細 `qos statistics workload performance show` 資訊，請參閱。

您可以使用 `qos statistics workload latency show` 命令來檢視 QoS 工作負載的詳細延遲統計資料。如"[指令參考資料ONTAP](#)"需詳細 `qos statistics workload latency show` 資訊，請參閱。

使用 **ONTAP** 自適應 **QoS** 原則群組設定處理量

您可以使用 `_自適應 QoS_` 策略群組，根據磁碟區大小自動調整吞吐量上限或下限，從而在磁碟區大小變化時保持 IOPS 與 TB/GB 的比率。在大型部署中管理數百上千個工作負載時，這是一個顯著的優勢。

開始之前

- 您必須執行 ONTAP 9.3 或更新版本。
- 您必須是叢集管理員、才能建立原則群組。
- 要新增至策略群組的儲存物件必須是非自適應策略群組的成員

儲存物件可以是自適應原則群組或非自適應原則群組的成員，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。

#### 關於這項工作

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`` 是每分配 TB/GB 的最低預期 IOPS。



``expected-iops`` 僅在 AFF 平台上針對不在 SnapMirror 同步關係中的磁碟區提供保證。``expected-iops`` 僅在分層原則設為「none」且雲端中沒有區塊時，才針對 FabricPool 提供保證。

- ``peak-iops`` 是每分配或使用的 TB/GB 的最大可能 IOPS。
- `expected-iops-allocation`` 指定預期 IOPS 使用的是已分配空間（預設）還是已使用空間。  
``expected-iops-allocation is available beginning with ONTAP 9.5.`
- `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。

#### 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"[指令參考資料ONTAP](#)"需詳細 ``qos adaptive-policy-group create`` 資訊，請參閱。



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

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
```

## 預設自適應 QoS 策略群組

系統提供了三個預設的自適應 QoS 策略群組。您可以將這些策略群組直接套用到磁碟區。

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

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層。
- 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
```

## 使用統一管理器監控和管理叢集效能

### 使用 ONTAP 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 Linux 入門指南"](#)
- ["Active IQ Unified Manager for Windows 快速入門"](#)

## 了解ONTAP Active IQ Unified Manager效能監控與管理

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。
- 您正在使用 ONTAP 命令列介面來設定儲存服務品質 (QoS)。QoS 也可透過下列方式取得：
  - 系統管理員
  - 靜態API ONTAP
  - VMware vSphere適用的工具ONTAP
  - NetApp 服務層級經理 ( NSLM )
  - OnCommand Workflow Automation ( WFA )
- 您想要使用虛擬裝置安裝Active IQ Unified Manager，而不是基於 Linux 或 Windows 的安裝。
- 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

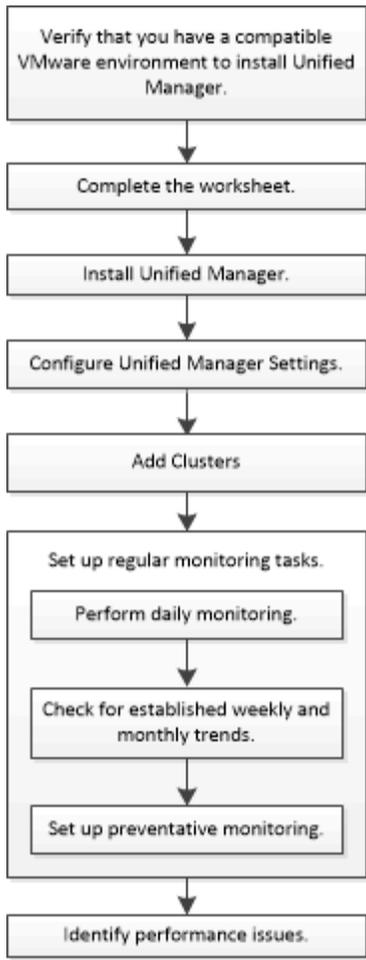
如果這些假設不符合您的情況、您應該看到下列資源：

- ["安裝過程Active IQ Unified Manager"](#)
- ["系統管理"](#)

## 監控效能

### 了解ONTAP Active IQ Unified Manager效能監控與維護工作流程

監控及維護叢集效能包括安裝Active IQ Unified Manager VMware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。



### 驗證ONTAP Active IQ Unified Manager的 VMware 環境需求

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。

### ONTAP Active IQ Unified Manager工作表

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

### 下載並部署ONTAP Active IQ Unified Manager

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。

### 配置初始ONTAP Active IQ Unified Manager設置

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。

### 指定要在Active IQ Unified Manager中監控的ONTAP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。

#### 開始之前

- 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ONTAP Active IQ Unified Manager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。

### 使用ONTAP Active IQ Unified Manager每周和每月的效能趨勢來識別效能問題

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。

### 設定ONTAP Active IQ Unified Manager效能閾值

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。

Object Counter Condition\* Average Latency ms/op 12 ms/op 15 ms/op

## 新增ONTAP Active IQ Unified Manager警報

事件是Active IQ Unified Manager在預定義條件發生時或效能計數器值超過閾值時自動產生的通知。事件可以幫助您識別正在監控的叢集中的效能問題。

您可以設定警報，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報。您可以指定通知頻率，並將腳本與警報相關聯。

## 開始之前

- 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](mailto: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](mailto: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 \*」。

#### 配置ONTAP Active IQ Unified Manager警報設定

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。

#### 開始之前

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 \*」。

## 識別ONTAP Active IQ Unified Manager中的效能問題

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ONTAP 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。Digital Advisor 顯示系統效能的時間比 System Manager 長。

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。

除了這項效能資料外、Digital Advisor 還能根據工作負載顯示儲存效率、並將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

- ["數位顧問文件"](#)
- ["數位顧問影片播放清單"](#)
- ["數位顧問Web入口網站"](#)

# 使用 ONTAP 資料基礎架構洞察監控叢集效能

NetApp 資料基礎架構洞察是一款監控工具，可讓您深入了解整個基礎架構。透過資料基礎架構洞察，您可以監控、排除故障並優化所有資源，包括公有雲和私有資料中心。

## 監控、疑難排解及最佳化所有資源

數據基礎設施洞察可協助您大幅減少解決問題的時間並防止問題影響最終用戶。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。

資料基礎設施洞察讓您可以在一個地方查看整個混合基礎設施 - 從公有雲到資料中心。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符合組織需求的目標式和條件式警示。

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。

資料基礎設施洞察可視化您的系統拓撲，以了解您的 Kubernetes 架構。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。

資料基礎設施洞察透過先進的機器學習和異常檢測為您提供有關內部威脅的可操作情報，幫助您保護組織資料免受惡意或受感染用戶的濫用。

資料基礎設施洞察可協助您視覺化 Kubernetes 指標，以便您可以充分了解 pod、節點和叢集之間的關係。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

- ["開始使用數據基礎設施洞察"](#)

## 稽核記錄

### 瞭解 ONTAP 稽核記錄實作

審計日誌中記錄的管理活動包含在標準AutoSupport報告中，某些日誌記錄活動包含在EMS 訊息中。您也可以將稽核日誌轉送至指定的目標位置，並可使用ONTAP CLI 或 Web 瀏覽器顯示稽核日誌檔案。

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。

從ONTAP 9.17.1 開始，以及從ONTAP 9.16.1 P4 和更高版本的 9.16.1 修補程式版本開始，"[還可以記錄使用跨群集操作從對等群集發起的遠端管理活動](#)"。這些活動包括使用者驅動的和源自另一個叢集的內部操作。

### ONTAP中記錄的管理活動

ONTAP記錄在叢集上執行的管理活動，例如發出了什麼請求、觸發請求的使用者、使用者的存取方式以及請求的時間。

管理活動可以是以下類型之一：

- **SET** 請求：
  - 這些請求通常適用於非顯示命令或操作。
  - 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 SET 請求。
- **GET** 請求：
  - 這些請求檢索資訊並將其顯示在管理介面中。
  - 這些要求會在您執行時發出 show 例如命令。
  - 預設不會記錄 GET 請求，但您可以控制是否從ONTAP CLI 發送 GET 請求(-cliget)，來自ONTAP API (-ontapiget)，或透過ONTAP REST API (-httpget) 記錄在文件中。

### 審計日誌記錄和輪換

ONTAP記錄管理活動 `/mroot/etc/log/mlog/audit.log` 節點的檔案。CLI指令 (clustershell、nodeshell 和非互動式 systemshell) 以及 API 指令均記錄在此。互動式 systemshell 指令不記錄。稽核日誌包含時間戳，用於顯示叢集中所有節點是否同步。

◦ 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。

啟用 GET 稽核時，請考慮設定日誌轉發，以避免因日誌快速輪替而導致資料遺失。有關更多信息，請參閱以下知識庫文章：["啟用稽核日誌轉發"](#)。

## 瞭解 ONTAP 稽核記錄的變更

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 ONTAP 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。可能值的範例包括 `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，可以是 `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`` 命令來顯示個別節點的稽核項目，或是從叢集中的多個節點合併。您也可以使用 Web 瀏覽器，在單一節點上顯示目錄內容 `/mroot/etc/log/mlog`。如["指令參考資料ONTAP"](#)需詳細 `security audit log show`` 資訊，請參閱。

### 網頁瀏覽器

您可以使用 Web 瀏覽器，在單一節點上顯示目錄內容 `/mroot/etc/log/mlog`。["瞭解如何使用網頁瀏覽器存取節點的記錄檔，核心傾印和 MIB 檔案"](#)。

## 管理 ONTAP 稽核 Get 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  右上角的、然後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"[指令參考資料ONTAP](#)"需詳細 `security audit show` 資訊，請參閱。

## 啟用ONTAP跨叢集審核

從ONTAP 9.17.1 以及ONTAP 9.16.1 P4 和更高版本的 9.16.1 修補程式版本開始，您可以在ONTAP中啟用跨叢集稽核功能，以記錄從對等叢集發起的操作。這種遠端審計功能在多個ONTAP叢集互動的環境中尤其有用，可以提供遠端操作的可追溯性和責任追究。

跨叢集審計可以區分用戶發起的 GET（讀取）或 SET（建立/修改/刪除）操作。預設情況下，目標叢集僅會審計使用者發起的 SET 操作。任何讀取資料的請求，例如 GET 或 show CLI 中的命令，無論請求是否跨叢集，預設都不會受到審核。

### 開始之前

- 你必須有 `advanced` 等級權限
- 此叢集必須與另一個叢集對等，且兩個叢集都必須執行ONTAP 9.16.1 P4 或更高版本。



在部分節點（而非所有節點）升級到ONTAP 9.16.1 P4 或更高版本的環境中，稽核日誌記錄僅在執行升級版本的節點上進行。建議將所有節點升級到受支援的版本，以確保一致的審計行為。

### 啟用或停用跨叢集審計

#### 步驟

1. 透過設定 cluster-peer 參數 `on` 或者 `off`：

```
security audit modify -cluster-peer {on|off}
```

2. 透過檢查目前審核狀態來確認叢集對等設定是啟用還是停用：

```
security audit show
```

回覆:

```
Audit Setting State
-----
      CLI GET: off
      HTTP GET: off
      ONTAPI GET: off
      Cluster Peer: on
```

## 啟用 **GET** 稽核的效果

從ONTAP 9.17.1 開始，如果您 "[啟用 CLI、HTTP、ONTAPI GET 審計](#)"在對等叢集上，您也可以啟用對跨叢集使用者發起的 GET 請求的審核。在早期ONTAP版本中，GET 審核僅適用於本機叢集上的請求。在ONTAP 9.17.1 中，如果您使用 `cluster-peer`` 選項設定為 ``on``，本地集群和跨集群請求都將被審核。

## 管理 **ONTAP** 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](#)"。

您可以使用 ``-protocol`` 參數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。

預設連接埠為 514（用於 UDP）、6514（用於 TCP）、但您可以指定任何符合網路需求的連接埠。

您可以使用 ``-message-format`` 命令選取下列其中一種訊息格式：

### 舊版 **NetApp**

RFC-3164 Syslog 格式的變化（格式： <PRIVAL> TAIMP 主機名稱： MSG）

### **RFC-5424**

根據 RFC-5424 格式的系統記錄格式（格式： <PRIVAL> 資料處理時間戳主機名稱： MSG）

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\*。+\*通知管理方塊\*會顯示記錄目的地的計數。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  \*主機位址\* 欄、以編輯或刪除項目。

#### 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 6514 -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

Destination Host          Port  Protocol          Verify Syslog
-----
192.168.123.96           514   udp-unencrypted  false  user
192.168.123.98           6514  tcp-encrypted    true   user
2 entries were displayed.
```

#### 相關資訊

- ["叢集記錄轉送顯示"](#)
- ["建立叢集記錄轉送"](#)

## AutoSupport

## 瞭解 AutoSupport

### 瞭解 ONTAP AutoSupport

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"](#)
- ["指令參考資料ONTAP"](#)

### 瞭解數位顧問與 ONTAP AutoSupport

這個功能的元件會收集遙測資料並傳送給分析人員。AutoSupport ONTAP數位顧問會分析 AutoSupport 的資料、並提供主動式照護與最佳化。使用人工智慧、Digital Advisor 可識別潛在問題、並協助您在問題影響企業之前加以解決。

Digital Advisor可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、讓您在全球混合雲中最佳化資料基礎架構。所有擁有有效 SupportEdge 合約的 NetApp 客戶、都能從數位顧問獲得資料導向的洞見和建議（功能因產品和支援層而異）。

以下是數位顧問的一些功能：

- 規劃升級。數位顧問可識別環境中可透過升級至較新版本的 ONTAP 來解決的問題、而升級顧問元件則可協助您規劃成功的升級。
- 檢視系統健全狀況。數位顧問儀表板會回報任何健康問題、並協助您修正這些問題。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：Digital Advisor 顯示系統效能的時間比 System Manager 長。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。Digital Advisor 會顯示完整的庫存及軟體與硬體組態資訊。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：數位顧問"

"啟動 Digital Advisor"

"部門服務SupportEdge"

瞭解 **ONTAP AutoSupport** 訊息的傳送時間和位置

根據訊息類型、將訊息傳送給不同的收件者。AutoSupport瞭解 AutoSupport 傳送訊息的時間和地點、可協助您瞭解透過電子郵件收到的訊息、或是在數位顧問網站上檢視。

除非另有指定、否則下表中的設定是參數 `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 <code>-to</code> 和 <code>-noteto</code> 。（僅會傳送影響服務的重大事件。）  中指定的位址 <code>-partner-address</code>  技術支援、如果 <code>-support</code> 設為 <code>enable</code>

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 <code>-partner-address</code>  技術支援、如果 <code>-support</code> 設為 <code>enable</code>
每日（依預設、於上午12：00之間傳送和上午1：00效能訊息） <code>-perf</code> 參數設定為 <code>true</code>	合作夥伴地址中指定的地址  技術支援、如果 <code>-support</code> 設為 <code>enable</code>
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 <code>-partner-address</code>  技術支援、如果 <code>-support</code> 設為 <code>enable</code>

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
<p>您可以使用手動初始化訊息 <code>system node autosupport invoke</code> 命令</p>	<p>如果使用指定 URI <code>-uri</code> 中的參數 <code>system node autosupport invoke</code> 命令會將訊息傳送至該 URI。</p> <p>如果 <code>-uri</code> 如果省略、訊息會傳送至中指定的位址 <code>-to</code> 和 <code>-partner-address</code>。此訊息也會傳送給技術支援人員、如果有的話 <code>-support</code> 設為 <code>enable</code>。</p>
<p>您可以使用手動初始化訊息 <code>system node autosupport invoke-core-upload</code> 命令</p>	<p>如果使用指定 URI <code>-uri</code> 中的參數 <code>system node autosupport invoke-core-upload</code> 命令會將訊息傳送至該 URI、核心傾印檔案會上傳至 URI。</p> <p>如果 <code>-uri</code> 在中省略 <code>system node autosupport invoke-core-upload</code> 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。</p> <p>這兩種情況都需要這樣做 <code>-support</code> 設為 <code>enable</code> 和 <code>-transport</code> 設為 <code>https</code> 或 <code>http</code>。</p> <p>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 <code>-to</code> 和 <code>-partner-addresses</code> 參數。</p>
<p>您可以使用手動初始化訊息 <code>system node autosupport invoke-performance-archive</code> 命令</p>	<p>如果使用指定 URI <code>-uri</code> 中的參數 <code>system node autosupport invoke-performance-archive</code> 命令會將訊息傳送至該 URI、效能封存檔案會上傳至 URI。</p> <p>如果 <code>-uri</code> 在中省略 <code>system node autosupport invoke-performance-archive</code>、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。</p> <p>這兩種情況都需要這樣做 <code>-support</code> 設為 <code>enable</code> 和 <code>-transport</code> 設為 <code>https</code> 或 <code>http</code>。</p> <p>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 <code>-to</code> 和 <code>-partner-addresses</code> 參數。</p>
<p>您可以使用手動重新傳送過去的訊息 <code>system node autosupport history retransmit</code> 命令</p>	<p>僅限您在中指定的 URI <code>-uri</code> 的參數 <code>system node autosupport history retransmit</code> 命令</p>

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 <code>-partner-address</code>  技術支援、如果 <code>-support</code> 設為 <code>enable</code> 和 <code>-transport</code> 設為 <code>https</code>
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 <code>-support</code> 設為 <code>enable</code> 和 <code>-transport</code> 設為 <code>https</code>
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 <code>-support</code> 設為 <code>enable</code> 和 <code>-transport</code> 設為 <code>https</code> 。核心傾印或效能歸檔檔案會上傳至技術支援網站。

### 瞭解 ONTAP AutoSupport 事件觸發訊息

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。

## ONTAP AutoSupport 訊息類型及其內容

支援子系統的狀態資訊包含在內。AutoSupport瞭解 AutoSupport 訊息所包含的內容、可協助您解讀或回應以電子郵件或數位顧問網站檢視的訊息。

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	<p>取決於中指定的值 -type 參數：</p> <ul style="list-style-type: none"> <li>• test 傳送含有一些基本資料的使用者觸發訊息。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• performance 傳送效能資料。</li> <li>• 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。</li> </ul> <p>技術支援部門通常會要求提供此訊息。</p>
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

訊息類型	訊息所包含的資料類型
由AutoSupport NetApp按需觸發	<p>根據需求、可索取新訊息或過去訊息：AutoSupport</p> <ul style="list-style-type: none"> <li>• 視 AutoSupport 集合類型而定、可以是新訊息 <code>test`、`all`或`performance`。</code></li> <li>• 過去的訊息取決於重新傳送的訊息類型。</li> </ul> <p>AutoSupport OnDemand 可要求將下列檔案上傳至 NetApp 支援網站的新訊息 "<a href="https://mysupport.netapp.com">mysupport.netapp.com</a>"、網址為：</p> <ul style="list-style-type: none"> <li>• 核心傾印</li> <li>• 效能歸檔</li> </ul>

### 檢視 ONTAP AutoSupport 子系統

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

#### 步驟

1. 檢視有關子系統和觸發事件的資訊：

```
system node autosupport trigger show
```

### 瞭解 ONTAP AutoSupport 的規模和時間預算

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。

### 瞭解事件觸發的 ONTAP AutoSupport 訊息中所傳送的檔案

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
<ul style="list-style-type: none"><li>• 的記錄檔 <code>/mroot/etc/log/mlog/</code> 目錄</li><li>• 訊息記錄檔</li></ul>	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。)
<ul style="list-style-type: none"><li>• 的記錄檔 <code>/mroot/etc/log/shelflog/</code> 目錄</li><li>• 的記錄檔 <code>/mroot/etc/log/acp/</code> 目錄</li><li>• 事件管理系統 (EMS) 記錄資料</li></ul>	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

瞭解 **ONTAP AutoSupport** 隨選即用如何從技術支援取得交付指示

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

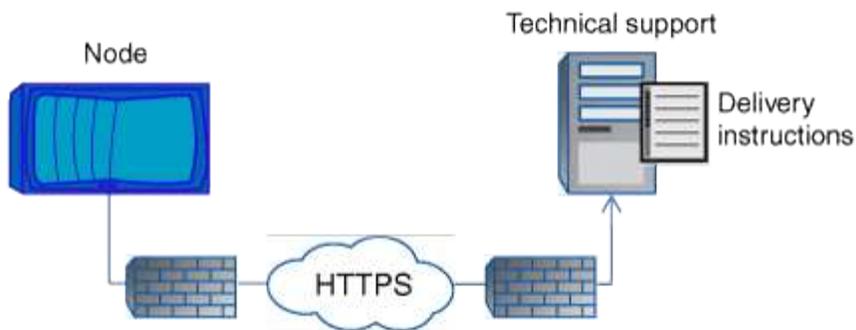
《支援不限需求的用戶端》AutoSupport 會將HTTPS要求傳送至AutoSupport 傳送該訊息的相同技術支援位置。不接受傳入連線的不適用。AutoSupport



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，但保持 AutoSupport 啟用，請使用命令 `system node autosupport modify -ondemand-state disable`。如"[指令參考資料ONTAP](#)"需詳細 `system node autosupport modify -ondemand-state disable` 資訊，請參閱。

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。

### 瞭解透過電子郵件傳送的 **ONTAP AutoSupport** 訊息結構

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。

#### 瞭解 ONTAP AutoSupport 嚴重性類型

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。

#### 取得 ONTAP AutoSupport 訊息說明

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 ONTAP AutoSupport 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	<code>system node autosupport modify</code> 使用 <code>-state</code> 參數
控制 AutoSupport 是否將不實訊息傳送至技術支援	<code>system node autosupport modify</code> 使用 <code>-support</code> 參數
設定 AutoSupport 功能不完善或修改 AutoSupport 功能不完善的組態	<code>system node autosupport modify</code>
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	<code>system node autosupport trigger modify</code>

### 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	<code>system node autosupport show</code> 使用 <code>-node</code> 參數
檢視接收 AutoSupport 到不實訊息的所有位址和 URL 摘要	<code>system node autosupport destinations show</code>
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	<code>system node autosupport trigger show</code>
顯示 AutoSupport 錶板配置狀態、以及傳送至不同目的地	<code>system node autosupport check show</code>
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	<code>system node autosupport check show-details</code>

### 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	<code>system node autosupport history show</code>
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	<code>system node autosupport history show-upload-details</code>

如果您想要...	使用此命令...
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	<code>system node autosupport manifest show</code>

傳送、重新傳送或取消AutoSupport 等字訊息

如果您想要...	使用此命令...
<p>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</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>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。</p> </div>	<pre>system node autosupport history retransmit</pre>
<p>產生AutoSupport 並傳送一個資訊不全的訊息、例如用於測試目的</p>	<pre>system node autosupport invoke</pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>使用 <code>-force</code> 即使 AutoSupport 已停用、仍可傳送訊息的參數。使用 <code>-uri</code> 將訊息傳送至指定目的地而非設定目的地的參數。</p> </div>
<p>取消AutoSupport 訊息</p>	<pre>system node autosupport history cancel</pre>

如"指令參考資料ONTAP"需詳細 `system node autosupport` 資訊，請參閱。

相關資訊

["指令參考資料ONTAP"](#)

瞭解 **ONTAP AutoSupport** 資訊清單中包含的資訊

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。

AutoSupport 資訊清單會隨附於每則 AutoSupport 訊息中、並以 XML 格式顯示、這表示您可以使用一般的 XML 檢視器來讀取資訊、或是使用數位顧問入口網站來檢視資訊。

## 規劃

### 準備使用 ONTAP AutoSupport

您可以設定 ONTAP 叢集、將 AutoSupport 訊息傳送至 NetApp。在此過程中、您也可以將訊息的複本傳送至組織內的本機電子郵件地址。您應該先檢閱可用選項、準備好設定 AutoSupport。

### 將 AutoSupport 訊息傳送至 NetApp

AutoSupport 訊息可使用 HTTPS 或 SMTP 傳輸協定傳送至 NetApp。從 ONTAP 9.15.1 開始、您也可以搭配 SMTP 使用 TLS。



請盡可能使用 HTTPS 與 AutoSupport OnDemand 通訊，並上傳大型檔案。

另請注意下列事項：

- AutoSupport 訊息只能設定一個傳送通道至 NetApp。您無法使用兩種通訊協定將 AutoSupport 訊息傳送至 NetApp。
- 此功能可限制每個傳輸協定的最大檔案大小。AutoSupport 如果 AutoSupport 訊息的大小超過設定的限制、AutoSupport 會盡可能傳送訊息、但會發生截斷。
- 您可以視需要變更檔案大小上限。如"[指令參考資料ONTAP](#)"需詳細 `system node autosupport modify` 資訊，請參閱。
- 這兩種通訊協定都可以根據名稱解析的位址系列、透過 IPv4 或 IPv6 傳輸。
- 由 ONTAP 建立的 TCP 連線 AutoSupport 是暫時性的、而且是短暫的。

## HTTPS

這提供最強大的功能。請注意下列事項：

- 支援 AutoSupport OnDemand 和大型檔案傳輸。
- 首先嘗試 HTTPS Put 要求。如果在傳輸期間要求失敗、要求會在停止處重新啟動。
- 如果伺服器不支援 Put、則改用 HTTPS POST 方法。
- HTTPS 傳輸的預設限制為 50 MB。
- HTTPS 傳輸協定使用連接埠 443。

## SMTP

一般而言，只有在不允許或不支援 HTTPS 時，才應使用 SMTP。請注意下列事項：

- 不支援 AutoSupport OnDemand 和大型檔案傳輸。

- 如果已設定 SMTP 登入認證、則會以未加密和清除的方式傳送。
- 傳輸的預設限制為 5 MB。
- 不安全的 SMTP 傳輸協定使用連接埠 25。

### 使用 TLS 改善 SMTP 安全性

使用 SMTP 時，所有流量都不會加密，而且很容易攔截和讀取。從 ONTAP 9.15.1 開始、您也可以使用 TLS 搭配 SMTP（SMTPS）。在這種情況下、會使用 *explicit tls*、在建立 TCP 連線之後啟動安全通道。

下列連接埠通常用於 SMTPS：連接埠 587

### 其他組態考量

在設定 AutoSupport 時、還有一些其他考量。

有關這些注意事項的命令的詳細資訊，請參閱["設定 AutoSupport 功能"](#)。

### 使用電子郵件傳送本機複本

無論用於將 AutoSupport 訊息傳送至 NetApp 的傳輸協定為何、您也可以將每封訊息的複本傳送至一或多個本機電子郵件地址。例如、您可能會傳送訊息給內部支援組織或合作夥伴組織。



如果您使用 SMTP（或 SMTPS）將訊息傳送至 NetApp、而且您也會傳送這些訊息的本機電子郵件複本、則會使用相同的電子郵件伺服器組態。

## HTTP Proxy

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。如果使用 HTTPS 將 AutoSupport 訊息傳送給技術支援人員、而且您有 Proxy、則必須識別 Proxy 的 URL。如果 Proxy 使用的連接埠不是預設的連接埠（連接埠 3128），您可以指定該 Proxy 的連接埠。您也可以選擇性地指定 Proxy 驗證的使用者名稱和密碼。

### 安裝伺服器憑證

透過 TLS（HTTPS 或 SMTPS），從伺服器下載的憑證會由 ONTAP 根據根 CA 憑證進行驗證。在使用 HTTPS 或 SMTPS 之前，您必須確定根憑證已安裝在 ONTAP 中，而且 ONTAP 可以驗證伺服器憑證。此驗證是根據簽署伺服器憑證的 CA 來執行。

ONTAP 包含大量預先安裝的根 CA 憑證。在許多情況下，ONTAP 會立即辨識您伺服器的憑證，無需額外設定。視伺服器憑證的簽署方式而定，您可能需要安裝根 CA 憑證和任何中繼憑證。

如有需要，請使用下列程序來安裝憑證。您應該在叢集層級安裝所有必要的憑證。

## 範例 1. 步驟

### 系統管理員

1. 在 System Manager 中，選擇 **Cluster** > \* Settings\* 。
2. 向下捲動至 \* 安全性 \* 區段。
3. 選取  \* 憑證 \* 旁的。
4. 在 \* 信任的憑證授權單位 \* 索引標籤下、按一下 \* 新增 \* 。
5. 按一下 \* 匯入 \* 並選取憑證檔案。
6. 完成環境的組態參數。
7. 按一下「\* 新增 \*」。

### CLI

1. 開始安裝：

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

如"[指令參考資料ONTAP](#)"需詳細 `security certificate install` 資訊，請參閱。

2. 查看下列主控台訊息：

```
Please enter Certificate: Press <Enter> when done
```

3. 使用文字編輯器開啟憑證檔案。
4. 複製整個憑證、包括下列幾行：

```
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----
```

5. 在命令提示字元之後、將憑證貼到終端機。
6. 按 **Enter** 鍵完成安裝。
7. 執行下列其中一個命令，確認已安裝憑證：

```
security certificate show-user-installed
```

```
security certificate show
```

如"[指令參考資料ONTAP](#)"需詳細 `security certificate show` 資訊，請參閱。

## 相關資訊

- ["設定AutoSupport 功能"](#)
- ["指令參考資料ONTAP"](#)

## 設定 ONTAP AutoSupport

您可以設定 ONTAP 叢集、將 AutoSupport 訊息傳送給 NetApp 技術支援部門、並將電子郵件複本傳送給內部支援組織。在此過程中、您也可以正式作業環境中使用組態之前、先測試組態。

### 關於這項工作

從 ONTAP 9.5 開始、您可以同時為叢集的所有節點啟用和設定 AutoSupport。當新節點加入叢集時、節點會自動繼承相同的 AutoSupport 組態。為支援此功能、請參閱 CLI 命令的範圍 `system node autosupport modify` 為叢集層級。◦ `-node` 為了回溯相容性而保留命令選項、但會忽略該選項。



在 ONTAP 9.4 及更早版本中、命令 `system node autosupport modify` 專屬於每個節點。如果叢集執行的是 ONTAP 9.4 或更早版本、則需要在叢集中的每個節點上啟用和設定 AutoSupport。

### 開始之前

將 AutoSupport 訊息傳送至 NetApp 的建議傳輸組態是 HTTPS（HTTP 搭配 TLS）。此選項提供最強大的功能和最佳安全性。

檢閱 ["準備使用 AutoSupport"](#) 如需更多資訊、請在設定 ONTAP 叢集之前先參閱。

### 步驟

1. 確保AutoSupport 啟用了功能：

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

2. 如果您想要 NetApp 技術支援人員接收 AutoSupport 訊息、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。



AutoSupport OnDemand 預設為啟用，設定為使用 HTTPS 傳輸通訊協定傳送訊息給技術支援時，功能正常。

3. 如果您啟用 NetApp 技術支援來接收 AutoSupport 訊息，請指定這些訊息要使用的傳輸通訊協定。

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 <code>system node autosupport modify</code> 命令 ...
使用預設的HTTPS傳輸協定	<ul style="list-style-type: none"> <li>a. 設定 <code>-transport</code> 至 <code>https</code>。</li> <li>b. 如果您使用 Proxy、請設定 <code>-proxy-url</code> 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。</li> </ul>
使用SMTP	<p>設定 <code>-transport</code> 至 <code>smtp</code>。</p> <p>此組態不支援AutoSupport 以「根據需求」或上傳大型檔案。</p>

4. 如果您想要內部支援組織或支援合作夥伴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...
<code>-to</code>	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
<code>-noteto</code>	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
<code>-partner-address</code>	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. 如果您在上一步中為內部支援組織設定收件者位址，或是選擇 SMTP 傳輸訊息給技術支援，請設定命令的下列參數來設定 SMTP `system node autosupport modify`：

- 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 <code>system node autosupport modify</code> 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 <code>-remove-private-data</code> 至 <code>true</code> 。如果您從變更 <code>false</code> 至 <code>true</code> ，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 <code>-perf</code> 至 <code>false</code> 。

8. 如果您使用 SMTP 將 AutoSupport 訊息傳送至 NetApp、您可以選擇性地啟用 TLS 以改善安全性。

a. 顯示新參數的可用值：

```
cluster1::> system node autosupport modify -smtp-encryption ?
```

b. 啟用 TLS 以傳輸 SMTP 訊息：

```
cluster1::> system node autosupport modify -smtp-encryption start_tls
```

c. 顯示目前的組態：

```
cluster1::> system node autosupport show -fields smtp-encryption
```

9. 使用檢查整體組態 `system node autosupport show` 命令 `-node` 參數。

10. 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。

11. 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：

```
system node autosupport history show -node local
```

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。

c. 您也可以選擇查看您為設定的任何地址的電子郵件、確認 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。

## 相關資訊

- ["準備使用 AutoSupport"](#)
- ["指令參考資料ONTAP"](#)

## 設定

### 管理 **ONTAP AutoSupport** 設定

您可以使用系統管理員來管理 AutoSupport 帳戶的設定。

如需 AutoSupport 組態選項的詳細資訊，包括系統管理員中無法使用的設定，請參閱 `system-node-autosupport-modify` 中的 ["指令參考資料ONTAP"](#)。

### 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 、然後選取 **\* 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 、然後選取 **\* 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 、然後選取 \* 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 家用電話系統，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有問題之前自動開啟。
- \* 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僅在啟用AutoSupport時才有效，例如NetApp控制台中的某些工作流程。

#### 步驟

1. 選擇\*叢集>設定\*。
2. 在 \* AutoSupport \* 區段中、選取 、然後選取 \* 停用 \*。
3. 如果您想再次啟用 AutoSupport、請在 \* AutoSupport \* 區段中選取 、然後選取 \* 啟用 \*。

#### 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 、然後選取 \* 抑制支援個案產生 \*。
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 、然後選取 \* 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 、然後選取 \* 更多選項 \*。
3. 在 \* 連線 \* 區段或 \* 電子郵件 \* 區段中、選取  Edit 以修改任一區段的設定。

#### 相關資訊

- ["準備使用 AutoSupport"](#)
- ["設定AutoSupport 功能"](#)

在排程的維護期間，禁止建立 **ONTAP AutoSupport** 個案

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

#### 步驟

1. 手動調用帶有文本字符串的 AutoSupport 消息 `MAINT=xh`，其中 `x` 是維護窗口的持續時間（以小時為單位）。將 `<node>` 替換為要從中發送 AutoSupport 消息的節點的名稱：

```
system node autosupport invoke -node <node> -message MAINT=xh
```

#### 相關資訊

- ["指令參考資料ONTAP"](#)
- ["如何在排程的維護期間、隱藏自動建立個案"](#)

## 使用 **AutoSupport** 上傳檔案

## 上傳 ONTAP AutoSupport 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

開始之前

- 您已使用下列設定來設定 AutoSupport：
  - 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
  - AutoSupport 設定為使用 HTTPS 傳輸協定。

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。

### "如何上傳 ONTAP 9 核心檔案進行分析"

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 ONTAP AutoSupport 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。

### 開始之前

- 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HTTPS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
```

## 疑難排解

當未收到訊息時，請疑難排解 **ONTAP AutoSupport**

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 <code>system node autosupport history show -detail</code> 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 <code>system node autosupport manifest show</code> 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 <code>system node autosupport history show -delivery</code> 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 <code>system node autosupport history show -delivery</code> 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 <code>system node autosupport history show</code> 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 <code>system node autosupport history show</code> 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：  " <a href="#">無法提供：狀態卡在初始化中AutoSupport</a> "
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。

## 透過 HTTPS 進行 ONTAP AutoSupport 訊息傳遞疑難排解

如果系統未傳送預期的 AutoSupport 訊息，而且您使用的是 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。

### 開始之前

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` 字段應返回 `up`  
 • 如 [link:https://docs.netapp.com/us-en/ontap-cli/up.html](https://docs.netapp.com/us-en/ontap-cli/up.html) ["  
 指令參考資料ONTAP"] 需詳細 `up` 資訊，請參閱。

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
```

如需協助疑難排解任何傳回的錯誤，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及網際網路：

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`

如果這些路由中有任何一條無法運作，請使用大多數協力廠商網路用戶端上的或 `tracert` 公用程式，從與叢集位於同一子網路上運作正常的主機嘗試相同的路由 `tracert`。然後您可以判斷問題是在您的網路組態或叢集組態中。如"[指令參考資料ONTAP](#)"需詳細 `network traceroute` 資訊，請參閱。

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。

訪問應該會成功。如果沒有，請確保所有防火牆都已正確配置以允許 HTTPS 和 DNS 流量，並且代理伺服器已正確配置。有關為 `support.netapp.com` 配置靜態名稱解析的更多信息，請參閱"[NetApp知識庫：如何在ONTAP中為 support.netapp.com 新增 HOST 項目？](#)"

8. 從 ONTAP 9.10.1 開始，如果您啟用自動更新，請確保您有 HTTPS 連線功能可連線至下列其他 URL：

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

## 疑難排解透過 SMTP 傳送 ONTAP AutoSupport 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。

### 開始之前

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` 字段應返回 `up`  
。如 [link:https://docs.netapp.com/us-en/ontap-cli/up.html](https://docs.netapp.com/us-en/ontap-cli/up.html) ["  
指令參考資料ONTAP"] 需詳細 `up` 資訊，請參閱。

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。

- 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.
```

- 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
```

- 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。

- 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。

- 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。

### ONTAP AutoSupport 子系統疑難排解

◦ 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 子系統的整體狀態，例如 AutoSupport HTTPS 目的地，AutoSupport SMTP 目的地，AutoSupport 隨選伺服器和 AutoSupport 組態的狀態
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

### 瞭解 ONTAP 系統健全狀況監控

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"

## 瞭解 ONTAP 健全狀況監控元件

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。

## 瞭解 ONTAP 系統健全狀況警示回應

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」）。

## 瞭解 ONTAP 系統健全狀況警示自訂功能

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。

相關資訊

- ["系統健康警報顯示"](#)

## 瞭解 ONTAP AutoSupport 健全狀況警示觸發程序

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、讓您的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。

## 瞭解可用的 ONTAP 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
乙太網路交換器	交換器 (交換器健全狀況)	ONTAP 乙太網路交換器健全狀況監視器 (CSHM) 可監控叢集和儲存網路交換器的狀態，同時收集記錄以供分析。根據預設，CSHM 會每 5 分鐘透過 SNMPv2c 輪詢每個交換器，以更新資源表，其中包含支援性，監控狀態，溫度感測器，CPU 使用率，介面組態和連線，叢集交換器備援，以及風扇和電源供應器作業等資訊。此外，如果已設定，CSHM 會每小時透過 SSH/SCP 收集記錄，並透過 AutoSupport 傳送以供進一步分析。CSHM 也可根據要求，使用 SSH/SCP 執行更詳細的技術支援記錄收集。  如需詳細資訊，請參閱 <a href="#">"交換器健全狀況監控"</a> 。
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 ONTAP 系統健全狀況警示

您可以使用命令手動檢視系統健全狀況警示 `system health alert show`。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.mailed` 訊息和所有 `hm.alert.Cleared` 訊息的通知。

所有 `hm.alert.mailed` 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"[指令參考資料ONTAP](#)"需詳細 `system health alert show` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `event destination create` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `event route add-destinations` 資訊，請參閱。

相關資訊

- "[使用系統管理員視覺化 ONTAP 網路](#)"
- "[如何在 DATA ONTAP 上設定 SNMP 監控](#)"

## 回應降級的 ONTAP 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。

#### 相關資訊

- ["系統健康警報修改"](#)

## 瞭解如何回應降級的 **ONTAP** 系統健全狀況

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
```

#### 相關資訊

- ["系統健康警報修改"](#)

### 用於監控 ONTAP 系統健全狀況的命令

您可以使用 `system health` 命令來顯示系統資源健全狀況的相關資訊，回應警示，以及設定未來的警示。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。如"[指令參考資料 ONTAP](#)"需詳細 `system health` 資訊，請參閱。

#### 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	<code>system health status show</code>
顯示子系統的健全狀況狀態、以便進行健全狀況監控	<code>system health subsystem show</code>

#### 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	<code>storage shelf show -connectivity</code> 使用 <code>-instance</code> 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	<code>storage disk show</code> 使用 <code>-instance</code> 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	<code>storage port show</code> 使用 <code>-instance</code> 參數以顯示每個介面卡的詳細資訊。

#### 監控叢集與儲存網路交換器

如果您想要...	使用此命令... (更新版本: <b>ONTAP</b> )	使用此命令... (更新版本: <b>9.7</b> ) <b>ONTAP</b>
顯示叢集監控的交換器	<code>system switch ethernet show</code>	<code>system cluster-switch show</code>
顯示叢集目前監控的交換器，包括您刪除的交換器 (顯示在命令輸出的「原因」欄中)  此命令可在進階權限層級使用	<code>system switch ethernet show-all</code>	<code>system cluster-switch show-all</code>
設定對未探索到的交換器的監控	<code>system switch ethernet create</code>	<code>system cluster-switch create</code>
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)	<code>system switch ethernet modify</code>	<code>system cluster-switch modify</code>
停用交換器的監控功能	<code>system switch ethernet modify -disable-monitoring</code>	<code>system cluster-switch modify -disable-monitoring</code>
從監控中刪除交換器	<code>system switch ethernet delete</code>	<code>system cluster-switch delete</code>
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)	<code>system switch ethernet delete -force</code>	<code>system cluster-switch delete -force</code>
使用交換器執行記錄收集	<code>system switch ethernet log</code>	<code>system cluster-switch log</code>



如需詳細資訊，請參閱["交換器健全狀況監控"](#)和["設定記錄收集"](#)。

## 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	<code>system health alert show</code>
顯示每個產生警示的相關資訊	<code>system health alert show -instance</code>
表示有人正在處理警示	<code>system health alert modify</code>
確認警示	<code>system health alert modify -acknowledge</code>

如果您想要...	使用此命令...
隱藏後續警示、使其不影響子系統的健全狀況	<code>system health alert modify -suppress</code>
刪除未自動清除的警示	<code>system health alert delete</code>
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	<code>system health autosupport trigger history show</code>

### 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	<code>system health policy definition modify</code>

### 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	<code>system health config show</code> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>使用 <code>-instance</code> 顯示每個健全狀況監視器的詳細資訊的參數。</p> </div>
顯示健全狀況監視器可能產生之警示的相關資訊	<code>system health alert definition show</code> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>使用 <code>-instance</code> 顯示每個警示定義的詳細資訊的參數。</p> </div>
顯示有關健全狀況監視原則的資訊、以決定何時發出警示	<code>system health policy definition show</code> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>使用 <code>-instance</code> 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。</p> </div>

### 相關資訊

- ["儲存連接埠顯示"](#)
- ["倉儲貨架展示"](#)
- ["系統健康警報刪除"](#)

## 檢視 ONTAP 環境資訊

感應器可協助您監控系統的環境元件。您可以檢視的環境感應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

### 瞭解 ONTAP 檔案系統分析

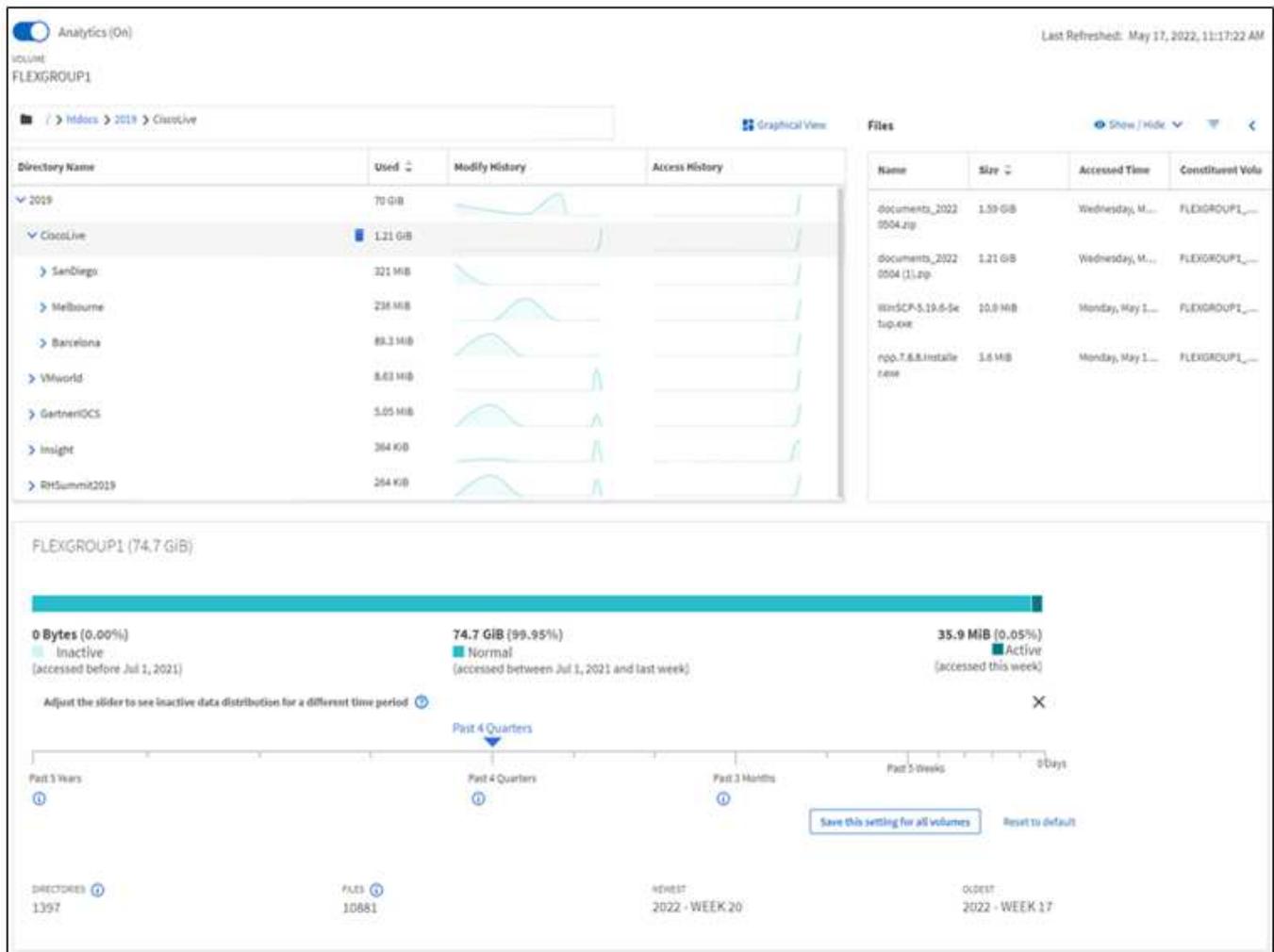
檔案系統分析 (FSA) 是 ONTAP 在更新版本 9.8 中首次推出、可即時查看 ONTAP FlexGroup 檔案使用率及內部的儲存容量趨勢、包括更新版本。FlexVol 這項原生功能不需要使用外部工具，並針對儲存設備的使用方式，以及是否有機會針對您的業務需求最佳化儲存設備，提供重要見解。

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 及更新版本	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	是的	是的	是的	是的	是的	是的	是的
容量分析	是的	是的	是的	是的	是的	是的	是的
非作用中資料資訊	是的	是的	是的	是的	是的	是的	是的
支援Data ONTAP 從VMware 7-Mode轉換的Volume	是的	是的	是的	是的	是的	是的	否

	ONTAP 9.14.1 及更新版本	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
能夠在System Manager中自訂非作用中期間	是的	是的	是的	是的	是的	是的	否
Volume層級活動追蹤	是的	是的	是的	是的	是的	否	否
將活動追蹤資料下載至CSV	是的	是的	是的	是的	是的	否	否
SVM層級的活動追蹤	是的	是的	是的	是的	否	否	否
時間表	是的	是的	是的	是的	否	否	否
使用分析	是的	是的	是的	否	否	否	否
預設啟用檔案系統分析的選項	是的	是的	否	否	否	否	否
初始化掃描進度監視器	是的	否	否	否	否	否	否

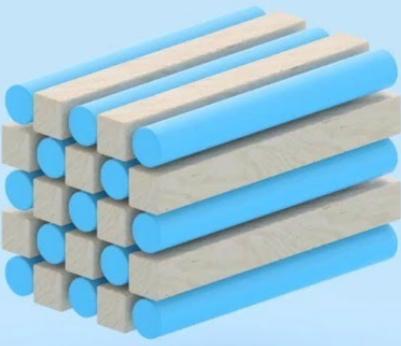
## 深入瞭解檔案系統分析

# ONTAP File System Analytics

**Daniel Tennant**  
Director of Software Engineering  
December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —



### 相關資訊

- "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 ONTAP 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。



從ONTAP 9.17.1 開始，在ONTAP叢集上新建的 SVM 上建立的磁碟區（如果已指派 NAS 協定）現在預設啟用檔案系統分析 (FSA)。FSA會在磁碟區建立後立即自動激活，無需額外配置即可提供即時分析功能。如果您不想在新磁碟區上啟用檔案系統分析，則必須 "[在新磁碟區上停用 FSA](#)" 來自 SVM。

#### 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。
- 啟用分析所需的時間取決於磁碟區的大小和內容。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掃描進度資訊、可以使用 ONTAP CLI 命令 `volume analytics show`。
  - 從 ONTAP 9.15.1 開始、您只能在節點上同時執行四次初始化掃描。您必須等待掃描完成、才能開始新的掃描。ONTAP 也會強制磁碟區上有足夠的可用空間、如果沒有、則會顯示錯誤訊息。請確定至少有 5% 至 8% 的磁碟區可用空間可用。如果磁碟區已啟用自動調整大小、請根據最大自動增加大小來計算可用大小。
  - 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。
  - 如需初始化掃描的進一步考量、請參閱 [掃描考量](#)。
  - 如"[指令參考資料ONTAP](#)"需詳細 `volume analytics show` 資訊，請參閱。

#### 在現有磁碟區上啟用檔案系統分析

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。

## 範例 2. 步驟

### 系統管理員

更新版本ONTAP	ONTAP 9.9.1 和ONTAP 9.8
<ol style="list-style-type: none"><li>1. 選擇*儲存&gt;磁碟區*。</li><li>2. 選取所需的Volume。從個別Volume功能表中、選取*檔案系統&gt;檔案總管*。</li><li>3. 選取 * 啟用分析 * 或 * 停用分析 *。</li></ol>	<ol style="list-style-type: none"><li>1. 選擇*儲存&gt;磁碟區*。</li><li>2. 選取所需的磁碟區，然後選取 * 檔案總管 *。</li><li>3. 選取 * 啟用分析 * 或 * 停用分析 *。</li></ol>

### CLI

#### 使用 CLI 啟用檔案系統分析

1. 運行以下命令：

```
volume analytics on -vserver <svm_name> -volume <volume_name> [-foreground {true|false}]
```

預設情況下，此命令在前台運行；ONTAP會在完成後顯示進度並提供分析資料。如果您需要更精確的訊息，可以使用`-foreground false`選項，然後使用`volume analytics show`指令在CLI中顯示初始化進度。

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。

如"[指令參考資料ONTAP](#)"需詳細`volume analytics on`資訊，請參閱。

### 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。

### 範例 3. 步驟

#### 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. 在系統管理員中，導航至\*集群設定\*。
2. 在「叢集設定」中，查看「檔案系統設定」標籤。若要修改設置，請選擇  圖示。
3. 在「活動追蹤」欄位中，輸入預設啟用活動追蹤的 SVM 名稱。如果將此欄位留空，則所有 SVM 上的活動追蹤功能均處於停用狀態。

取消勾選「在新儲存虛擬機器上啟用」方塊以預設在新儲存虛擬機器上停用活動追蹤。

4. 在「分析」欄位中，輸入您希望預設啟用容量分析的儲存虛擬機器的名稱。如果將此欄位留空，則所有 SVM 上的容量分析均處於停用狀態。

取消勾選「在新儲存虛擬機器上啟用」方塊以預設在新儲存虛擬機器上停用容量分析。

5. 選擇\*保存\*。

#### 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，使用切換按鈕啟用或停用儲存虛擬機器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 以在所有新建的磁碟區上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
```

如"[指令參考資料ONTAP](#)"需詳細 `vserver modify` 資訊，請參閱。

#### 相關資訊

- "[指令參考資料ONTAP](#)"

### 使用 FSA 查看 ONTAP 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：

從ONTAP 功能上開始。9.10.1	在ONTAP 9.9.1 和 9.8 中
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*。	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 *。

## 相關資訊

- ["Volume修改"](#)

## 使用 FSA 啟用 ONTAP 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 ONTAP 9.11.1 開始， System Manager 也提供活動追蹤時間表，讓您可以查看最多五分鐘的活動追蹤資料。

「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 ONTAP 9.11.1 開始，時間軸功能可讓您在 Volume 或 SVM 上保留熱點活動記錄，並持續每五秒更新一次，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。

## 使用 FSA 啟用 ONTAP 使用情況分析

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，您可以查看 [ONTAP 檔案系統活動](#)。

## 根據 FSA 中的 ONTAP 分析採取糾正措施

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。以低延遲的非同步目錄刪除功能刪除目錄。（非同步目錄刪除也可從 ONTAP 9.9.1 開始使用，但不啟用分析功能。）

從ONTAP 功能上開始。9.10.1	在ONTAP 9.9.1 中
<ol style="list-style-type: none"> <li>1. 選擇“儲存 &gt; 磁碟區”並選擇所需的磁碟區名稱。</li> <li>2. 在單一磁碟區頁面中，選擇「檔案系統」選項卡，然後選擇「資源管理器」標籤。</li> <li>3. 在*Explorer*視圖中，選擇所需的目錄。</li> <li>4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除  選項出現。</li> </ol> <p>一次只能刪除一個物件。</p>	<ol style="list-style-type: none"> <li>1. 選擇*儲存&gt;磁碟區*。</li> <li>2. 選取所需的磁碟區，然後選取 * 檔案總管 *。</li> <li>3. 在*Explorer*視圖中，選擇所需的目錄。</li> <li>4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除  選項出現。</li> </ol>
<p>刪除目錄和檔案時、新的儲存容量值不會立即顯示。</p>	

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. 若要比較某個 Volume 的目的地選項、請按一下  該 Volume 、然後按一下 \* 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\*。

### 透過 ONTAP 檔案系統分析，以角色為基礎的存取控制

從 ONTAP 9.12.1 開始，ONTAP 包含一種預先定義的角色型存取控制（RBAC）角色，稱為 `admin-no-fsa`。此 `admin-no-fsa` 角色可授予系統管理員層級的 Privileges，但可防止使用者在 ONTAP CLI，REST API 和系統管理員中執行與端點相關的作業 `\files`（例如檔案系統分析）。

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 9.12.1 開始，您可以使用系統管理員來設定檔案系統分析的 RBAC 權限。

### 步驟

1. 選擇\*叢集>設定\*。在 \* 安全 \* 下，導航至 \* 用戶和角色 \*，然後選擇 [→](#)。
2. 在 \* 角色 \* 下，選擇 [+ 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	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
SVM上的活動追蹤	/api/svm/svms	<ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul>
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 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"](#)
- ["建立安全登入"](#)

## ONTAP 檔案系統分析的考量事項

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。

如果您發現延遲明顯增加，請參閱["NetApp知識庫：開啟NetApp ONTAP檔案系統分析後延遲過高或波動"](#)。

## 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 CLI 命令來追蹤掃描進度 `volume analytics show`。如果發生節流事件、ONTAP 會提供通知。

在磁碟區上啟用檔案系統分析時、請確保至少有 5% 至 8% 的磁碟區可用空間可用。如果磁碟區已啟用自動調整大小、請根據最大自動增加大小來計算可用大小。從 ONTAP 9.15.1 開始、如果您在磁碟區上啟用檔案系統分析時沒有足夠的可用空間、ONTAP 會顯示錯誤訊息。

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。

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

## 瞭解 ONTAP EMS 組態

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"](#)。

## 使用系統管理員設定 ONTAP 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。
ONTAP 9.10.0 至 9.7	僅設定SNMP traphosts。您可以使用ONTAP CLI設定其他EMS目的地。請參閱 <a href="#">"EMS 組態概觀"</a> 。

## 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["指令參考資料ONTAP"](#)需詳細 `event notification destination create` 資訊，請參閱。

### 步驟

1. 按一下\*叢集>設定\*。
2. 在 \* 通知管理 \* 區段中、按一下  下、然後按一下 \* 檢視事件目的地 \*。
3. 在\*通知管理\*頁面上、選取\*事件目的地\*索引標籤。
4. 單擊。  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	<ul style="list-style-type: none"> <li>TrapHost名稱</li> </ul>
電子郵件 (從9.10.1開始)	<ul style="list-style-type: none"> <li>目的地電子郵件地址</li> <li>郵件伺服器</li> <li>寄件者電子郵件地址</li> </ul>
系統記錄伺服器 (從9.10.1開始)	<ul style="list-style-type: none"> <li>伺服器的主機名稱或IP位址</li> <li>系統記錄連接埠 (從9.12.1開始)</li> <li>系統記錄傳輸 (從9.12.1開始)</li> </ul> <p>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。</p>
Webhook (從9.10.1開始)	<ul style="list-style-type: none"> <li>Webhook URL</li> <li>用戶端驗證 (選取此選項以指定用戶端憑證)</li> </ul>

### 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

- 按一下\*叢集>設定\*。
- 在 \* 通知管理 \* 區段中、按一下 下、然後按一下 \* 檢視事件目的地 \*。
- 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
- 單擊。 [+ Add](#)
- 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。
- 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	<ol style="list-style-type: none"> <li>選取現有的事件篩選器。</li> <li>修改現有規則。</li> <li>如有需要、請按一下以新增其他規則 <a href="#">+ Add</a>。</li> </ol>

### 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  下、然後按一下 \* 檢視事件目的地 \* 。
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邊，按一下  ，然後按一下 \* 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  下、然後按一下 \* 檢視事件目的地 \* 。
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邊，按一下  ，然後按一下 \* 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  下、然後按一下 \* 檢視事件目的地 \* 。
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邊，按一下  ，然後按一下 \* 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  下、然後按一下 \* 檢視事件目的地 \*。
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邊，按一下 ，然後按一下 \* 刪除 \*。

### 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](#)"

## 使用CLI設定EMS事件通知

### ONTAP EMS 組態工作流程

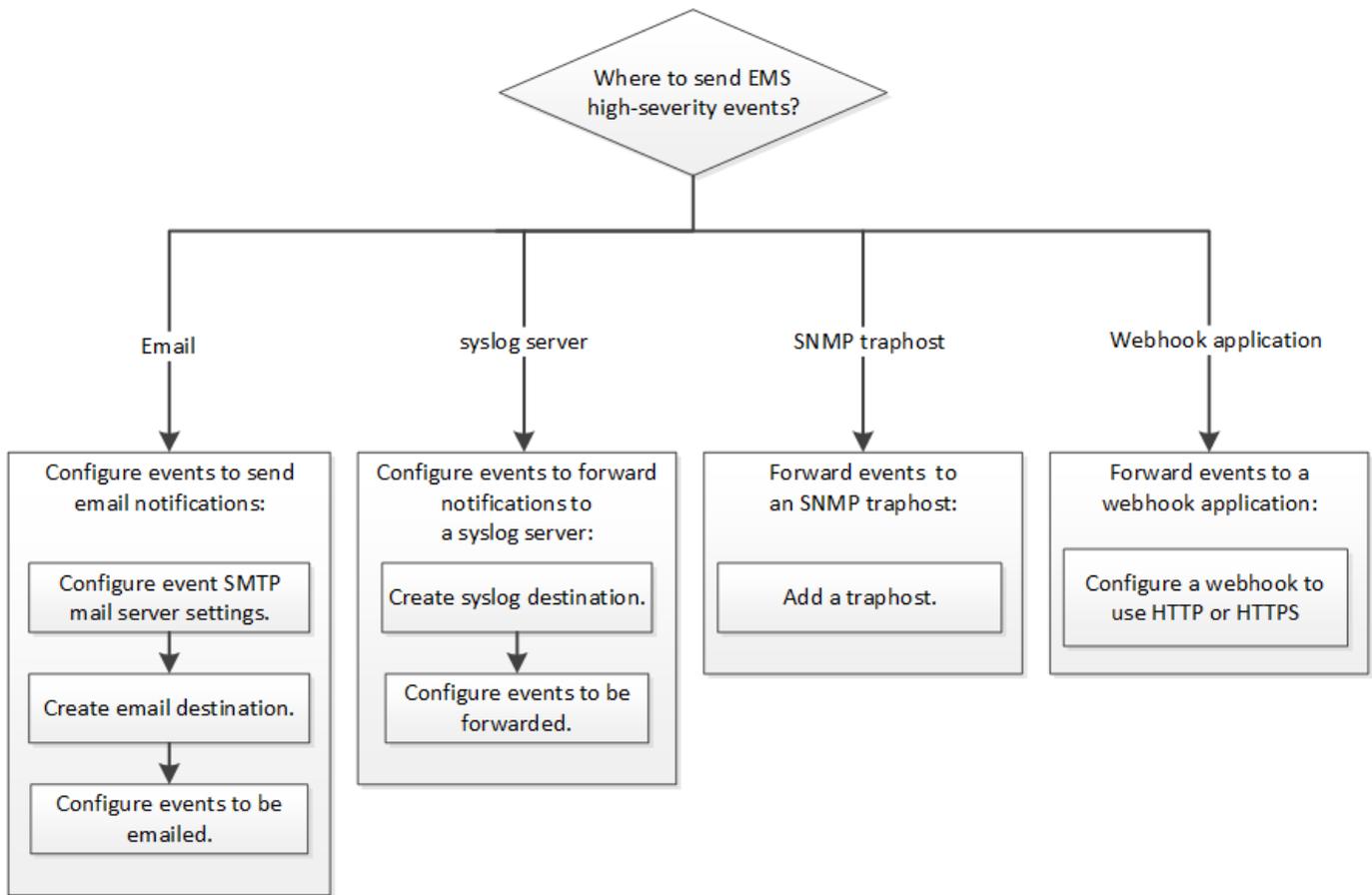
您必須將重要的EMS事件通知設定為以電子郵件傳送、轉送至syslog伺服器、轉送至SNMP traphost、或轉送至Webhook應用程式。這有助於您及時採取修正行動、避免系統中斷。

### 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（例如同服務器和應用程式）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	<a href="#">設定重要的EMS事件以傳送電子郵件通知</a>
EMS可將重要事件通知轉送至syslog伺服器	<a href="#">設定重要的EMS事件、將通知轉送到syslog伺服器</a>
如果您想要EMS將事件通知轉送到SNMP traphost	<a href="#">設定SNMP traphosts以接收事件通知</a>
如果您想要EMS將事件通知轉送到Webhook應用程式	<a href="#">設定重要的EMS事件、將通知轉送到Webhook應用程式</a>

設定重要的 **ONTAP 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。

開始之前

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
```

如"[指令參考資料ONTAP](#)"需詳細 `event config modify` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `event notification destination create` 資訊，請參閱。

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
```

如"[指令參考資料ONTAP](#)"需詳細 `event notification create` 資訊，請參閱。

設定重要的 **ONTAP EMS** 事件，將通知轉送到系統記錄伺服器

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。

#### 開始之前

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。

#### 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`。

如"[指令參考資料ONTAP](#)"需詳細 `event notification destination create` 資訊，請參閱。

## 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
```

如"[指令參考資料ONTAP](#)"需詳細 `event notification create` 資訊，請參閱。

設定 **ONTAP 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。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。



SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。

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 **ONTAP EMS** 事件，將通知轉寄至 **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Webhook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 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。

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

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
```

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

### 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
```

## 相關資訊

- ["安全性憑證安裝"](#)

## 更新過時的EMS事件對應

### 瞭解 ONTAP EMS 事件對應模式

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。如["指令參考資料ONTAP"](#)需詳細 `event` 資訊，請參閱。

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.*

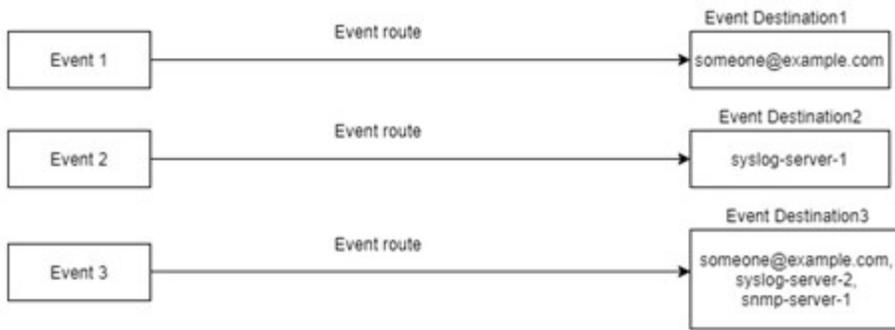
Time
Message                               Severity      Destinations  Freq
Threshd                               Threshd
-----
-----
raid.aggr.autoGrow.abort              NOTICE      test          0          0
raid.aggr.autoGrow.success            NOTICE      test          0          0
raid.aggr.lock.conflict                INFORMATIONAL test          0          0
raid.aggr.log.CP.count                DEBUG        test          0          0
4 entries were displayed.

```

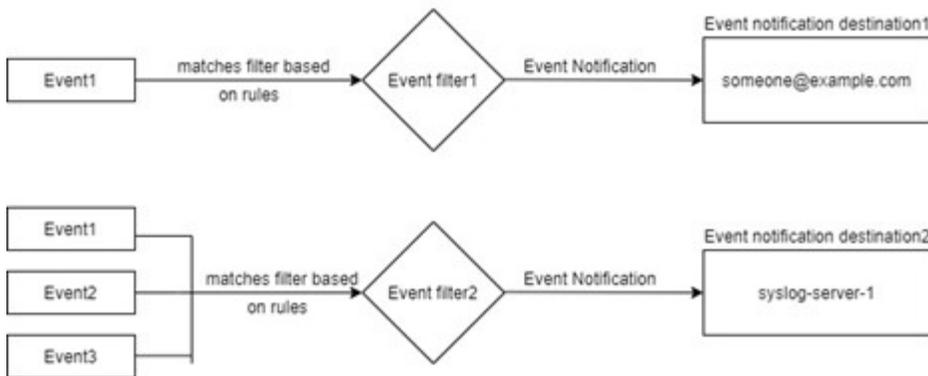
全新且可擴充的EMS事件通知機制、是以事件篩選器和事件通知目的地為基礎。如需新事件通知機制的詳細資訊、請參閱下列知識庫文章：

- ["事件管理系統概述ONTAP \(適用於\) 。9."](#)

Legacy routing based model



Event notification based model



### 使用過時的命令更新 ONTAP EMS 事件對應

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
```

```
Time
Message          Severity      Destinations    Freq
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。

如“[指令參考資料ONTAP](#)”需詳細 `event filter` 資訊，請參閱。



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.

```

深入瞭解 event notification destination 及 event destination ["指令參考資料ONTAP"](#)。

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?: -
```

## 版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。