管理事件和警報

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

管理事件和警報

管理活動

事件可協助您識別受監控叢集中的問題。

Active IQ平台事件是什麼

Unified Manager 可以顯示Active IQ平台發現的事件。這些事件是透過針對 Unified Manager 監控的所有儲存系統產生的AutoSupport訊息執行一組規則而建立的。

有關詳細信息，請參閱 "Active IQ平台事件是如何產生的"。

Unified Manager 會自動檢查新規則文件，並且僅在有更新規則時下載新文件。在沒有外部網路存取的網站中，您需要從*儲存管理* > 事件設定 > *上傳規則*手動上傳規則。

這些Active IQ事件與現有的 Unified Manager 事件不重疊，它們可以識別有關係統配置、佈線、最佳實務和可用性問題的事件或風險。

有關啟用平台事件的更多信息，請參閱"啟用Active IQ入口網站事件"。有關上傳規則文件的更多信息，請參閱"上傳新的Active IQ規則文件"。

NetApp Active IQ是一種基於雲端的服務，可提供預測分析和主動支持，以優化整個NetApp混合雲的儲存系統操作。看 "NetApp Active IQ"了解更多。

什麼是事件管理系統事件

事件管理系統 (EMS) 從ONTAP核心的不同部分收集事件資料並提供事件轉發機制。這些ONTAP事件可以在 Unified Manager 中報告為 EMS 事件。集中監控和管理簡化了關鍵 EMS 事件和基於這些 EMS 事件的警報通知的配置。

當您將叢集新增至 Unified Manager 時，Unified Manager 位址將會作為通知目標新增至叢集。一旦集群中發生事件，就會立即報告 EMS 事件。

在 Unified Manager 中接收 EMS 事件的方法有兩種：

- 一定數量的重要 EMS 事件會自動通報。
- 您可以訂閱接收單獨的 EMS 事件。

Unified Manager 產生的 EMS 事件的報告方式會根據產生事件的方法而有所不同：

功能	自動 **EMS** 訊息	訂閱的 **EMS** 訊息
可用的 EMS 事件	EMS 事件子集	所有 EMS 活動

功能	自動 **EMS** 訊息	訂閱的 **EMS** 訊息
觸發時的 EMS 訊息名稱	Unified Manager 事件名稱（由 EMS 事件名稱轉換而來）	格式不具體，為「收到錯誤 EMS」。詳細訊息提供了實際 EMS 事件的點符號格式
收到的訊息	一旦發現集群	將每個所需的 EMS 事件新增至 Unified Manager 後，以及在下一個 15 分鐘輪詢週期之後
事件生命週期	與其他 Unified Manager 事件相同：新、已確認、已解決和過時狀態	EMS 事件在叢集刷新後（即事件建立後 15 分鐘）將失效
擷取 Unified Manager 停機期間的事件	是的，當系統啟動時，它會與每個集群通訊以獲取缺失的事件	不
活動詳情	建議的糾正措施直接從ONTAP導入，以提供一致的解決方案	事件詳情頁面中未提供糾正措施

一些新的自動 EMS 事件是資訊事件，表示先前的事件已解決。例如，「FlexGroup Constituents Space Status All OK」訊息事件表示「FlexGroup Constituents Have Space Issues」錯誤事件已解決。資訊事件不能使用與其他事件嚴重性類型相同的事件生命週期進行管理，但是，如果同一磁碟區收到另一個「空間問題」錯誤事件，則該事件將自動過時。

自動新增至 **Unified Manager** 的 **EMS** 事件

以下ONTAP EMS 事件會自動新增至 Unified Manager。當 Unified Manager 監控的任何叢集觸發時，將會產生這些事件。

監控執行ONTAP 9.5 或更高版本軟體的叢集時，可取得以下 EMS 事件：

統一管理器事件名稱	**EMS** 活動名稱	受影響的資源	統一管理器嚴重性
因聚合遷移而拒絕雲層訪問	arl.netra.ca.check.失敗	總計的	錯誤
在儲存故障轉移期間，因聚合重新定位而拒絕雲層訪問	gb.netra.ca.check.失敗	總計的	錯誤
FabricPool鏡像複製重新同步已完成	wafl.ca.重新同步.完成	簇	錯誤
FabricPool空間幾乎已滿	fabricpool.幾乎.已滿	簇	錯誤
NVMe-oF 寬限期已開始	nvmf.寬限期.開始	簇	警告

統一管理器事件名稱	**EMS** 活動名稱	受影響的資源	統一管理器嚴重性
NVMe-oF 寬限期有效	nvmf.寬限期.活躍	簇	警告
NVMe-oF 寬限期已過	nvmf.寬限期.已過期	簇	警告
LUN 已損壞	lun.destroy	邏輯單元號	資訊
雲端 AWS MetaDataConnFail	cloud.aws.metadataConnFail	節點	錯誤
雲端 AWS IAMCreds已過期	cloud.aws.iamCreds已過期	節點	錯誤
雲端 AWS IAMCredsInvalid	cloud.aws.iamCreds無效	節點	錯誤
雲端 AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	節點	錯誤
雲端 AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	節點	資訊
雲端 AWS IAMRoleInvalid	cloud.aws.iamRole無效	節點	錯誤
雲端 AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	節點	錯誤
雲層主機無法解析	objstore.host.無法解析	節點	錯誤
雲層集群間網路介面關閉	objstore.interclusterlifDown	節點	錯誤
請求與雲層簽名不匹配	osc.簽章不符	節點	錯誤
其中一個 NFSv4 池已耗盡	Nblade.nfsV4PoolExhaust	節點	批判的
QoS 監視器記憶體已滿	qos.monitor.memory.maxed	節點	錯誤
QoS 監控記憶體減少	qos.monitor.memory.abated	節點	資訊
NVMeNS 銷毀	NVMeNS.destroy	命名空間	資訊

統一管理器事件名稱	**EMS** 活動名稱	受影響的資源	統一管理器嚴重性
NVMeNS 在線	NVMeNS.離線	命名空間	資訊
NVMeNS 離線	NVMeNS.online	命名空間	資訊
NVMeNS 空間不足	NVMeNS 空間不足	命名空間	警告
同步複製不同步	簡訊狀態不同步	SnapMirror關係	警告
同步複製已恢復	簡訊狀態同步	SnapMirror關係	資訊
同步複製自動重新同步失敗	簡訊重新同步嘗試失敗	SnapMirror關係	錯誤
許多 CIFS 連接	Nblade.cifsManyAuths	支援向量機	錯誤
超出最大 CIFS 連線數	Nblade.cifsMaxOpenSameFile	支援向量機	錯誤
超出每個使用者的最大 CIFS 連線數	Nblade.cifsMaxSessPerUsrConn	支援向量機	錯誤
CIFS NetBIOS 名稱衝突	Nblade.cifsNbName衝突	支援向量機	錯誤
嘗試連接不存在的 CIFS 共享	Nblade.cifs無私共享	支援向量機	批判的
CIFS 磁碟區複製作業失敗	cifs.shadowcopy.失敗	支援向量機	錯誤
AV 伺服器發現病毒	Nblade.vscan病毒檢測	支援向量機	錯誤
沒有用於病毒掃描的 AV 伺服器連接	Nblade.vscanNoScannerConn	支援向量機	批判的
未註冊 AV 伺服器	Nblade.vscanNoRegdScanner	支援向量機	錯誤
無回應的 AV 伺服器連接	Nblade.vscanConnInactive	支援向量機	資訊
AV 伺服器太忙，無法接受新的掃描請求	Nblade.vscanConnBackPressure	支援向量機	錯誤

統一管理器事件名稱	**EMS** 活動名稱	受影響的資源	統一管理器嚴重性
未經授權的使用者嘗試存取 AV 伺服器	Nblade.vscanBadUserPrivAccess	支援向量機	錯誤
FlexGroup成員有空間問題	flexgroup.constituents.有.空間.問題	體積	錯誤
FlexGroup成分空間狀態全部正常	flexgroup.constituents.space.status.all.ok	體積	資訊
FlexGroup成分存在 Inode 問題	flexgroup.constituents.有.inodes.問題	體積	錯誤
FlexGroup組成部分 Inode 狀態全部正常	flexgroup.constituents.inodes.status.all.ok	體積	資訊
磁碟區邏輯空間幾乎已滿	監視器.vol.nearFull.inc.sav	體積	警告
磁碟區邏輯空間已滿	監視器.vol.full.inc.sav	體積	錯誤
磁碟區邏輯空間正常	監視器.vol.one.ok.inc.sav	體積	資訊
WAFL卷自動調整大小失敗	wafl.vol.自動調整大小失敗	體積	錯誤
WAFL卷自動調整大小完成	wafl.vol.自動大小.完成	體積	資訊
WAFL READDIR 檔案操作逾時	wafl.readdir.expired	體積	錯誤

訂閱**ONTAP EMS** 活動

您可以訂閱接收安裝了ONTAP軟體的系統所產生的事件管理系統 (EMS) 事件。部分 EMS 事件會自動回報給 Unified Manager，但只有您訂閱了這些事件，才會回報其他 EMS 事件。

開始之前

不要訂閱已自動新增至 Unified Manager 的 EMS 事件，因為這可能會在接收相同問題的兩個事件時造成混淆。

您可以訂閱任意數量的 EMS 事件。您訂閱的所有事件都會經過驗證，並且只有經過驗證的事件才會套用到您在 Unified Manager 中監控的叢集。 _ONTAP 9 EMS 事件目錄_提供了指定版本的ONTAP 9 軟體的所有 EMS 訊息的詳細資訊。從ONTAP 9 產品文件頁面中找到對應版本的“EMS 事件目錄”，以取得適用事件的清單。

"ONTAP 9 產品庫"

您可以為訂閱的ONTAP EMS 事件設定警報，並且可以建立要為這些事件執行的自訂腳本。

如果您沒有收到您訂閱的ONTAP EMS 事件，則叢集的 DNS 設定可能有問題，導致叢集無法存取 Unified Manager 伺服器。若要解決此問題，叢集管理員必須修正叢集的 DNS 配置，然後重新啟動 Unified Manager。這樣做會將待處理的 EMS 事件刷新到 Unified Manager 伺服器。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「事件設定」。
2. 在事件設定頁面中，點選*訂閱 EMS 事件*按鈕。
3. 在「訂閱 EMS 事件」對話方塊中，輸入要訂閱的ONTAP EMS 事件的名稱。

   若要查看您可以訂閱的 EMS 事件的名稱，您可以從ONTAP叢集 Shell 中使用 `event route show`命令（ONTAP 9 之前版本）或 `event catalog show`命令（ONTAP 9 或更高版本）。

   "如何在Active IQ Unified Manager中設定和接收來自ONTAP EMS 事件訂閱的警報"

4. 按一下“新增”。

   EMS 事件已新增至「訂閱的 EMS 事件」清單中，但「適用於叢集」欄位顯示您新增的 EMS 事件的狀態為「未知」。

5. 按一下「儲存並關閉」以向叢集註冊 EMS 事件訂閱。
6. 再次點選*訂閱 EMS 事件*。

   您新增的 EMS 事件的「適用於集群」列中將顯示狀態「是」。

   如果狀態不是“是”，請檢查ONTAP EMS 事件名稱的拼字。如果名稱輸入錯誤，則必須刪除錯誤的事件，然後重新新增該事件。

當ONTAP EMS 事件發生時，該事件會顯示在「事件」頁面上。您可以選擇事件以在事件詳細資訊頁面中查看有關 EMS 事件的詳細資訊。您也可以管理事件的處置或為事件建立警報。

收到事件時會發生什麼

當 Unified Manager 收到事件時，它會顯示在「儀表板」頁面、「活動管理」庫存頁面、「叢集/效能」頁面的「摘要」和「資源管理器」標籤以及特定於物件的庫存頁面（例如，「磁碟區/運作狀況」庫存頁面）中。

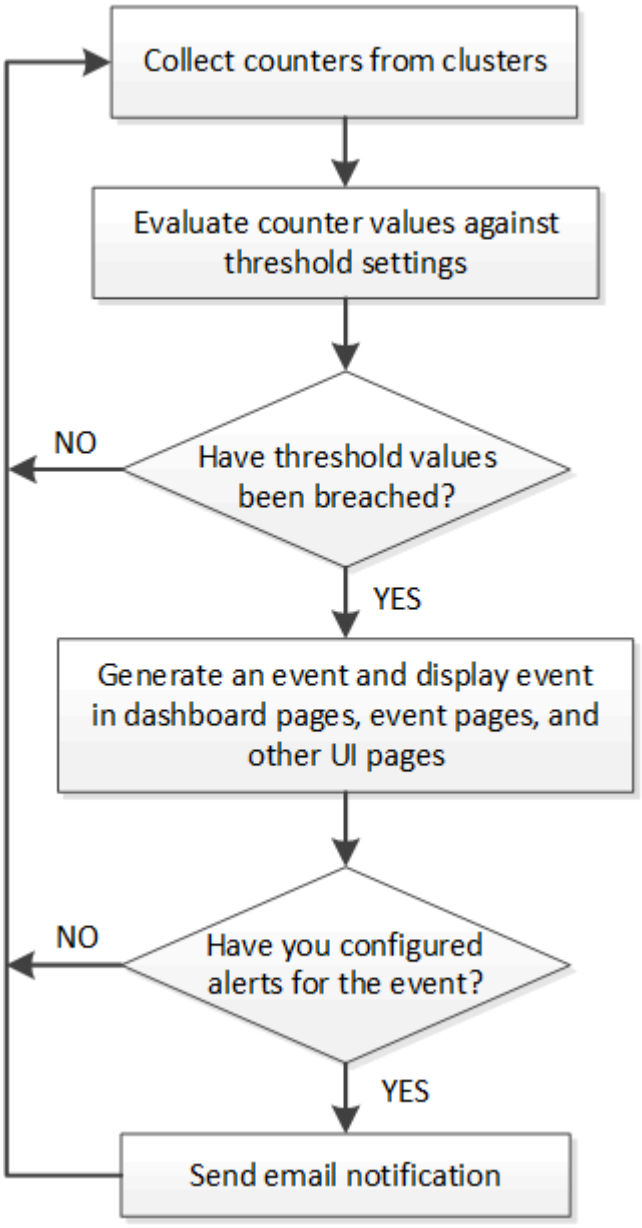
當 Unified Manager 偵測到相同叢集元件連續多次出現相同事件條件時，它會將所有出現的事件視為單一事件，而不是單獨的事件。事件的持續時間會增加，以表明事件仍然有效。

根據您在「警報設定」頁面中配置設定的方式，您可以將這些事件通知其他使用者。此警報將導致以下操作啟動：

- 可以將有關該事件的電子郵件傳送給所有 Unified Manager 管理員使用者。
- 該事件可以傳送給其他電子郵件收件者。
- SNMP 陷阱可以傳送到陷阱接收器。

- 可以執行自訂腳本來執行操作。

此工作流程如下圖所示。



查看活動和活動詳情

您可以查看由 Unified Manager 觸發的事件的詳細信息，以便採取糾正措施。例如，如果存在健康事件“卷離線”，您可以單擊該事件以查看詳細資訊並執行糾正措施。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

事件詳情包括事件來源、事件原因以及與事件相關的任何註釋等資訊。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。

預設情況下，「所有活動事件」檢視會顯示過去 7 天內產生的、影響等級為事件或風險的新事件和已確認（活動）事件。

2. 如果您想查看特定類別的事件，例如容量事件或效能事件，請按一下*查看*並從事件類型功能表中選擇。
3. 按一下您要查看其詳細資訊的事件名稱。

   事件詳情顯示在事件詳情頁面。

查看未指派的事件

您可以查看未指派的事件，然後將每個事件指派給可以解決它們的使用者。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。

   預設情況下，新事件和已確認事件顯示在事件管理庫存頁面上。

2. 從「篩選器」窗格中，選擇「指派給」區域中的「未指派」篩選器選項。

確認並解決事件

您應該在開始處理產生事件的問題之前確認該事件，這樣您就不會繼續收到重複的警報通知。對特定事件採取糾正措施後，您應該將該事件標記為已解決。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

您可以同時確認並解決多個事件。

ⓘ 您無法確認訊息事件。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。
2. 從事件清單中，執行以下操作來確認事件：

如果你想...	這樣做...
確認並將單一事件標記為已解決	a. 按一下事件名稱。 b. 從事件詳細資訊頁面確定事件的原因。 c. 點選*確認*。 d. 採取適當的糾正措施。 e. 按一下“標記為已解決”。

如果你想...	這樣做...
確認多個事件並將其標記為已解決	a. 從相應的事件詳細資訊頁面確定事件的原因。 b. 選擇事件。 c. 點選*確認*。 d. 採取適當的糾正措施。 e. 按一下“標記為已解決”。

事件被標記為已解決後，該事件將被移至已解決事件清單。

3. 可選：在*註釋和更新*區域，新增有關如何處理事件的註釋，然後按一下*發布*。

將事件指派給特定用戶

您可以將未指派的事件指派給自己或其他用戶，包括遠端用戶。如果需要，您可以將已指派的事件重新指派給另一個使用者。例如，當儲存物件頻繁出現問題時，您可以將這些問題的事件指派給管理該物件的使用者。

開始之前

- 必須正確配置使用者的姓名和電子郵件 ID。
- 您必須具有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。
2. 在*事件管理*庫存頁面中，選擇一個或多個要指派的事件。
3. 透過選擇以下選項之一來指派事件：

如果您想將事件指派給...	然後這樣做...
你自己	點選“分配給”>“我”。
另一個用戶	a. 點選*指派給*>*其他使用者*。 b. 在「分配所有者」對話方塊中，輸入使用者名，或從下拉清單中選擇使用者。 c. 點選*分配*。 電子郵件通知已發送給使用者。 如果您不輸入用戶名或從下拉清單中選擇用戶，然後按一下“分配”，則該事件仍未分配。

禁用不需要的事件

預設情況下，所有事件均啟用。您可以全域停用事件，以防止產生對您的環境不重要的事件的通知。當您想要恢復接收已停用的事件的通知時，您可以啟用這些事件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您停用事件時，系統中先前產生的事件將被標記為過時，並且不會觸發為這些事件配置的警報。當您啟用已停用的事件時，將從下一個監控週期開始產生這些事件的通知。

當您停用某個物件的某個事件時（例如，`vol offline`事件），然後您啟用該事件，則 Unified Manager 不會為在事件處於停用狀態時離線的物件產生新事件。僅當重新啟用事件後物件狀態變更時，Unified Manager 才會產生新事件。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「事件設定」。
2. 在「事件設定」頁面中，透過選擇以下選項之一來停用或啟用事件：

如果你想...	然後這樣做...
禁用事件	a. 按一下“禁用”。 b. 在「停用事件」對話方塊中，選擇事件嚴重性。 c. 在符合事件列中，根據事件嚴重性選擇要停用的事件，然後按一下向右箭頭將這些事件移至停用事件列。 d. 按一下“儲存並關閉”。 e. 驗證您停用的事件是否顯示在「事件設定」頁面的清單檢視中。
啟用事件	a. 選取要啟用的一個或多個事件的複選框。 b. 按一下“啟用”。

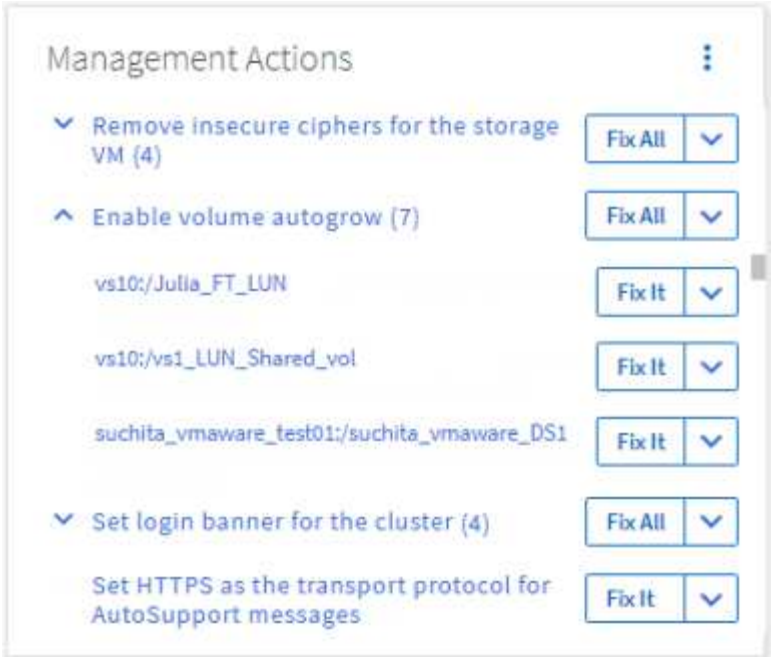
使用 **Unified Manager** 自動修復功能解決問題

對於某些事件，Unified Manager 可以徹底診斷並使用 **Fix It** 按鈕提供單一解決方案。當可用時，這些解決方案將顯示在儀表板、事件詳細資訊頁面以及左側導覽功能表上的工作負載分析選擇中。

大多數事件都有多種可能的解決方案，這些解決方案顯示在事件詳細資訊頁面中，以便您可以使用ONTAP系統管理器或ONTAP CLI 實施最佳解決方案。當 Unified Manager 確定存在一個解決方案來修復該問題、並且可以使用ONTAP CLI 命令解決該問題時，可以執行 修復 操作。

步驟

1. 若要從*儀表板*查看可修復的事件，請按一下*儀表板*。



2. 若要解決 Unified Manager 可以修復的任何問題，請按一下「修復」按鈕。若要修復多個物件上存在的問題，請按一下「修復全部」按鈕。

有關可透過自動修復修復的問題的信息，請參閱"Unified Manager 可以修復哪些問題"。

啟用並停用**Active IQ**事件報告

預設情況下， Active IQ平台事件會在 Unified Manager 使用者介面中產生並顯示。如果您發現這些事件太“吵雜”，或者您不想在 Unified Manager 中查看這些事件，那麼您可以停用這些事件的產生。如果您想恢復接收這些通知，可以稍後啟用它們。

開始之前

您必須具有應用程式管理員角色。

當您停用此功能時，Unified Manager 將立即停止接收Active IQ平台事件。

啟用此功能後，Unified Manager 會根據叢集的時區在午夜後不久開始接收Active IQ平台事件。開始時間取決於 Unified Manager 從每個叢集接收AutoSupport訊息的時間。

步驟

1. 在左側導覽窗格中，按一下「常規」>「功能設定」。
2. 在「功能設定」頁面中，透過選擇以下選項之一來停用或啟用Active IQ平台事件：

如果你想...	然後這樣做...
停用Active IQ平台事件	在* Active IQ Portal Events*面板中，將滑桿按鈕向左移動。
啟用Active IQ平台事件	在* Active IQ Portal Events*面板中，將滑桿按鈕向右移動。

上傳新的**Active IQ**規則文件

Unified Manager 會自動檢查新的Active IQ事件（規則）文件，並在有更新的規則時下載新文件。但是，在沒有外部網路存取的網站中，您需要手動上傳規則檔案。

Active IQ規則也稱為Config Advisor (CA) 安全規則。

當您在沒有網路連線的網站中安裝或升級 Unified Manager 到特定版本時，隨附的Active IQ規則將自動可供上傳。但是，建議您大約每月從 NetApp 的支援網站下載一次新規則文件，以確保產生更新的事件並且您的儲存系統繼續以最佳狀態運作。

開始之前

- 必須啟用Active IQ入口網站事件報告。此功能預設為啟用。有關信息，請參閱"啟用Active IQ入口網站事件"。
- 您必須從NetApp支援網站下載規則檔。

  規則文件位於： https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

步驟

1. 在具有網路存取權限的電腦上，導覽至NetApp支援網站並下載目前規則 `.zip`文件。

   捆綁的規則包包括規則儲存庫、資料來源和NetApp KB 文章。

   在 Windows 系統上，在沒有網路連線的網站中， NetApp KB 文章預設不會與安裝程式捆綁在一起。您可以從支援網站下載_secure_rules.zip_檔案並上傳它以查看所有規則的知識庫文章。

2. 將規則檔案傳輸到可以帶入安全區域的某些媒體，然後將其複製到安全區域中的系統上。
3. 在左側導覽窗格中，按一下「儲存管理」>「事件設定」。
4. 在*事件設定*頁面中，點選*上傳規則*按鈕。
5. 在「上傳規則」對話方塊中，導覽至並選擇規則 `.zip`下載的檔案並點擊*上傳*。

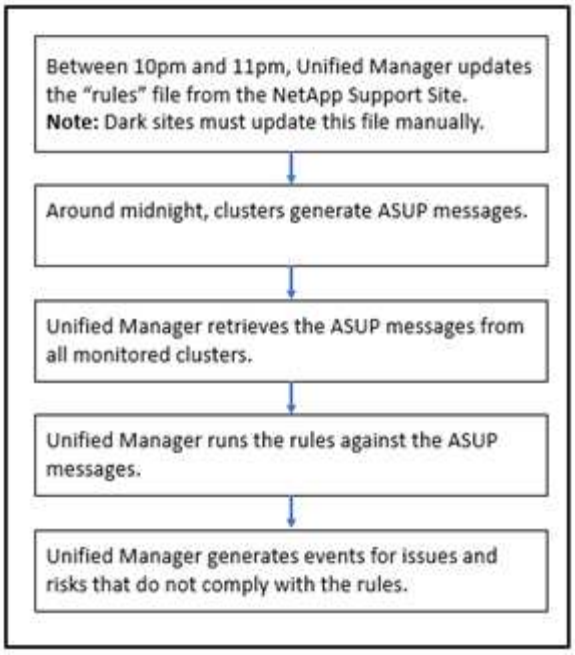
   此過程可能需要幾分鐘。

規則檔案在 Unified Manager 伺服器上解壓縮。當您管理的叢集在午夜後產生AutoSupport檔案時，Unified Manager 會根據規則檔案檢查叢集並根據需要產生新的風險和事件。

有關詳細信息，請參閱此知識庫 (KB) 文章： "如何在Active IQ Unified Manager中手動更新 AIQCASecure 規則"。

Active IQ平台事件是如何產生的

Active IQ平台事件和風險轉換為 Unified Manager 事件，如下圖所示。

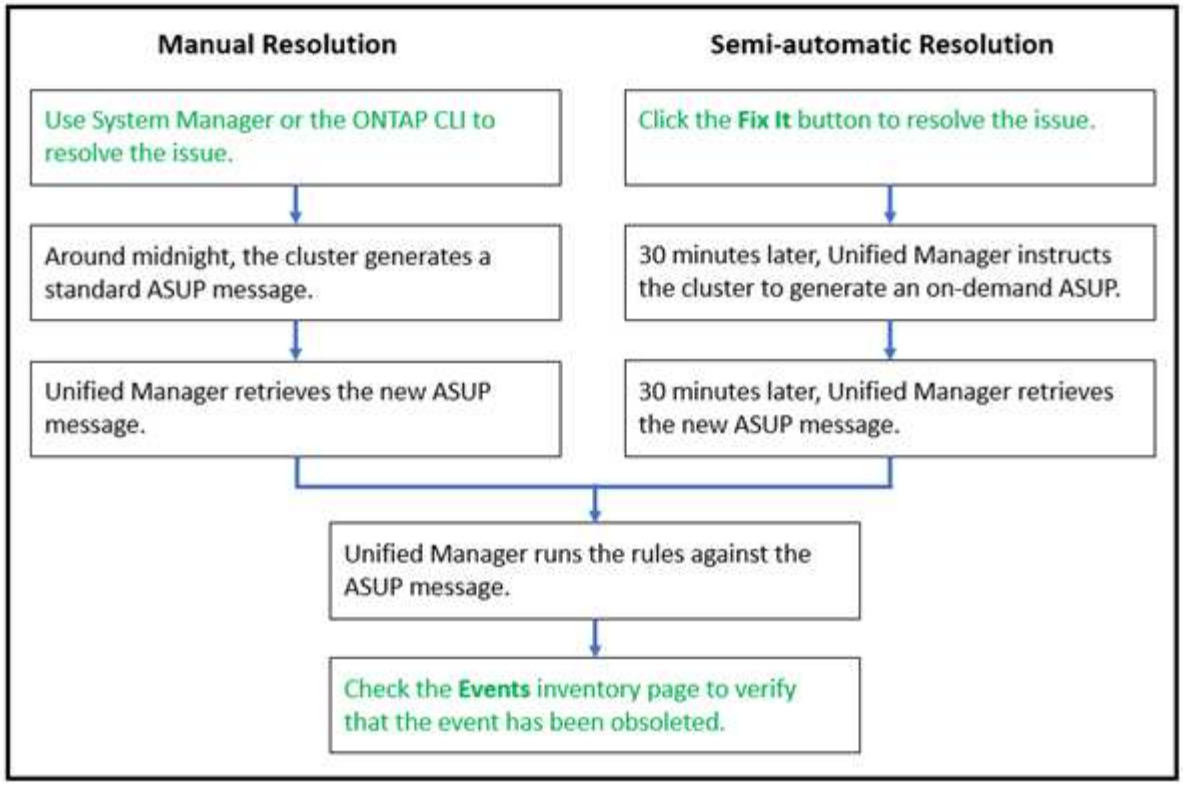


如您所見，在Active IQ平台上編譯的規則檔案保持最新，叢集AutoSupport訊息每天生成，並且 Unified Manager 每天更新事件清單。

解決**Active IQ**平台事件

Active IQ平台事件和風險與其他 Unified Manager 事件類似，因為它們可以指派給其他使用者解決，並且具有相同的可用狀態。但是，當您使用「修復」按鈕解決這些類型的事件時，您可以在數小時內驗證解決方案。

下圖顯示了在解決從Active IQ平台產生的事件時您必須採取的操作（綠色）以及 Unified Manager 採取的操作（黑色）。



執行手動解決時，您必須登入系統管理員或ONTAP命令列介面來解決問題。只有在叢集於午夜產生新的AutoSupport訊息後，您才能夠驗證該問題。

當使用「修復」按鈕執行半自動解決方案時，您可以在數小時內驗證修復是否成功。

配置事件保留設定

您可以指定事件在自動刪除之前在 Unified Manager 伺服器中保留的月份數。

開始之前

您必須具有應用程式管理員角色。

保留事件超過 6 個月可能會影響伺服器效能，因此不建議這樣做。

步驟

1. 在左側導覽窗格中，按一下「常規」>「資料保留」。
2. 在*資料保留*頁面中，選擇事件保留區域中的滑桿並將其移至應保留事件的月份數，然後按一下*儲存*。

Unified Manager 維護視窗是什麼

當您安排了叢集維護並且不想收到大量不必要的通知時，您可以定義 Unified Manager 維護視窗來抑制特定時間範圍內的事件和警報。

當維護視窗開始時，「物件維護視窗已啟動」事件將發佈到事件管理庫存頁面。維護時段結束後，此事件將自動失效。

在維護視窗期間，仍會產生與該叢集上所有物件相關的事件，但它們不會出現在任何 UI 頁面中，並且不會針對

這些事件發送任何警報或其他類型的通知。但是，您可以透過選擇「事件管理」庫存頁面上的「檢視」選項之一來查看維護時段內為所有儲存物件產生的事件。

您可以安排將來啟動的維護窗口，可以更改計劃維護窗口的開始和結束時間，也可以取消計劃維護窗口。

安排維護時段以停用叢集事件通知

如果您打算對叢集進行停機，例如，升級叢集或移動其中一個節點，則可以透過排程 Unified Manager 維護視窗來抑制通常在該時間範圍內產生的事件和警報。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

在維護時段期間，仍會產生與該叢集上所有物件相關的事件，但它們不會出現在事件頁面中，並且不會針對這些事件發送任何警報或其他類型的通知。

您輸入的維護視窗時間是基於 Unified Manager 伺服器的時間。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在叢集的*維護模式*列中，選擇滑桿按鈕並將其向右移動。

   顯示日曆視窗。

3. 選擇維護視窗的開始和結束日期和時間，然後按一下「套用」。

   滑桿按鈕旁邊會出現「已排程」訊息。

當達到開始時間時，叢集進入維護模式並產生「物件維護視窗已開始」事件。

更改或取消計劃的維護時段

如果您已設定將來發生的 Unified Manager 維護窗口，則可以變更開始時間和結束時間或取消發生維護窗口。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

如果您在規劃的維護時段結束時間之前完成了叢集維護，並且想要再次開始接收來自叢集的事件和警報，則取消目前正在執行的維護時段很有用。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在叢集的「維護模式」欄位中：

如果你想...	執行此步驟...
更改計畫維護時段的時間範圍	a. 點擊滑桿按鈕旁邊的文字“Scheduled”。 b. 變更開始和/或結束日期和時間，然後按一下*套用*。
延長活動維護視窗的長度	a. 點擊滑桿按鈕旁邊的文字“Active”。 b. 變更結束日期和時間，然後按一下「套用」。
取消計畫的維護時段	選擇滑桿按鈕並將其向左移動。
取消活動維護時段	選擇滑桿按鈕並將其向左移動。

查看維護時段內發生的事件

如有必要，您可以檢視 Unified Manager 維護時段內為所有儲存物件產生的事件。一旦維護視窗結束並且所有系統資源恢復運行，大多數事件將出現在過時狀態。

開始之前

必須至少完成一個維護窗口，然後才能獲得任何事件。

預設情況下，維護時段內發生的事件不會出現在事件管理庫存頁面上。

步驟

1. 在左側導覽窗格中，按一下「事件」。

   預設情況下，所有活動（新事件和已確認）事件都會顯示在事件管理庫存頁面上。

2. 從檢視窗格中，選擇選項*維護期間產生的所有事件*。

   顯示過去 7 天內所有維護時段會話和所有群集觸發的事件清單。

3. 如果單一叢集有多個維護窗口，您可以點擊*觸發時間*日曆圖示並選擇您感興趣的維護窗口事件的時間段。

管理主機系統資源事件

Unified Manager 包含一項服務，用於監控安裝了 Unified Manager 的主機系統上的資源問題。諸如可用磁碟空間不足或主機系統記憶體不足等問題可能會觸發管理站事件，這些事件會以橫幅訊息的形式顯示在 UI 頂部。

管理站事件表示安裝了 Unified Manager 的主機系統有問題。管理站問題的範例包括主機系統上的磁碟空間不足；Unified Manager 缺少常規資料收集週期；以及由於啟動了下一次收集輪詢而導致統計分析未完成或延遲完成。

與所有其他 Unified Manager 事件訊息不同，這些特定的管理站警告和嚴重事件顯示在橫幅訊息中。

步

1. 若要查看管理站事件訊息，請執行以下操作：

如果你想...	這樣做...
查看活動詳情	按一下事件橫幅可顯示包含該問題的建議解決方案的事件詳細資訊頁面。
查看所有管理站事件	a. 在左側導覽窗格中，按一下「事件管理」。 b. 在事件管理清單頁面的篩選器窗格中，按一下來源類型清單中的管理站方塊。

了解更多活動信息

了解有關事件的概念有助於您有效地管理叢集和叢集物件並適當地定義警報。

事件狀態定義

事件的狀態可以幫助您確定是否需要採取適當的糾正措施。事件可以是新的、已確認的、已解決的或過時的。請注意，新事件和已確認事件均被視為活動事件。

事件狀態如下：

- 新的

  新事件的狀態。

- 已確認

  您確認事件時的狀態。

- 已解決

  事件被標記為已解決時的狀態。

- 過時的

  事件被自動修正或事件原因不再有效時的狀態。

  您無法確認或解決過時的事件。

事件不同狀態的範例

以下範例說明了手動和自動事件狀態的變更。

當觸發事件「Cluster Not Reachable」時，事件狀態為「New」。當您確認事件時，事件狀態將變更為「已確認」。當您採取適當的糾正措施後，您必須將事件標記為已解決。事件狀態隨後變為「已解決」。

如果因斷電而產生「群集不可達」事件，則當電源恢復時，群集將開始運行，無需任何管理員幹預。因此，「叢

集不可達」事件不再有效，且事件狀態在下一個監控週期中變為「過時」。

當事件處於「已過時」或「已解決」狀態時，Unified Manager 會發送警報。警報的電子郵件主旨和電子郵件內容提供有關事件狀態的資訊。 SNMP 陷阱還包括有關事件狀態的資訊。

事件嚴重性類型描述

每個事件都與嚴重性類型相關聯，以幫助您確定需要立即採取糾正措施的事件的優先順序。

- 批判的

  出現問題，如果不立即採取糾正措施，可能會導致服務中斷。

  效能關鍵事件僅從使用者定義的閾值發送。

- 錯誤

  事件來源仍在運作；但是，需要採取糾正措施以避免服務中斷。

- 警告

  事件來源經歷了您應該注意的事件，或者群集物件的效能計數器超出了正常範圍，應該進行監視以確保其不會達到嚴重程度。這種嚴重程度的事件不會導致服務中斷，並且可能不需要立即採取糾正措施。

  效能警告事件由使用者定義、系統定義或動態閾值發送。

- 資訊

  當發現新物件或執行使用者操作時，就會發生該事件。例如，當刪除任何儲存物件或發生任何配置變更時，就會產生嚴重性類型為資訊的事件。

  當 ONTAP 偵測到設定變更時，會直接從ONTAP傳送訊息事件。

事件影響程度描述

每個事件都與一個影響等級（事件、風險、事件或升級）相關聯，以幫助您確定需要立即採取糾正措施的事件的優先順序。

- 事件

  事件是一組可能導致叢集停止向客戶端提供資料並耗盡儲存空間的事件。影響等級為「事故」的事件最為嚴重。應立即採取糾正措施以避免服務中斷。

- 風險

  風險是一系列可能導致叢集停止向客戶端提供資料並耗盡資料儲存空間的事件。影響等級為「風險」的事件可能會導致服務中斷。可能需要採取糾正措施。

- 事件

  事件是儲存物件及其屬性的狀態或狀況的變化。影響等級為「事件」的事件僅供參考，不需要採取糾正措

施。

- 升級

  升級事件是Active IQ平台報告的特定類型的事件。這些事件標識了需要您升級ONTAP軟體、節點韌體或作業系統軟體（以取得安全公告）才能解決的問題。您可能希望立即對其中一些問題採取糾正措施，而其他問題可能要等到下次預定的維護時再解決。

事件影響區域描述

事件分為六個影響領域（可用性、容量、配置、效能、保護和安全性），以使您能夠專注於您負責的事件類型。

- 可用性

  如果儲存物件離線、協定服務中斷、發生儲存故障轉移問題或發生硬體問題，可用性事件會通知您。

- 容量

  如果您的聚合、磁碟區、LUN 或命名空間正在接近或已達到大小閾值，或成長率對於您的環境而言異常，容量事件會通知您。

- 配置

  配置事件會通知您儲存物件的發現、刪除、新增、移除或重新命名。配置事件的影響等級為事件，嚴重性類型為資訊。

- 表現

  效能事件會通知您叢集上的資源、配置或活動狀況，這些狀況可能會對受監控的儲存物件上的資料儲存輸入或檢索速度產生不利影響。

- 保護

  保護事件會通知您涉及SnapMirror關係、目標容量問題、 SnapVault關係問題或保護作業問題的活動或風險。任何託管二級磁碟區和保護關係的ONTAP物件（尤其是聚合、磁碟區和 SVM）都歸類到保護影響區域。

- 安全

  安全事件會根據定義的參數通知您ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全性 "NetApp ONTAP 9 安全強化指南"。

  此外，該區域還包括從Active IQ平台報告的升級事件。

如何計算物件狀態

物件狀態由目前處於「新」或「已確認」狀態的最嚴重事件決定。例如，如果物件狀態為“錯誤”，則該物件事件之一的嚴重性類型為“錯誤”。採取糾正措施後，事件狀態將變為「已解決」。

對於動態效能事件，事件詳細資訊頁面的系統診斷部分列出了爭用叢集元件中延遲或使用率最高的頂級工作負載。

效能統計資料是基於偵測到效能事件的時間直到上次分析該事件的時間。圖表也顯示處於爭用的群集組件的歷史效能統計資料。

例如，您可以識別組件利用率高的工作負載，以確定將哪些工作負載移至使用率較低的組件。移動工作負載將會減少目前元件的工作量，甚至可能使該元件不再發生爭用。此部分的頂部是偵測和最後分析事件的時間和日期範圍。對於活動事件（新事件或已確認事件），最後分析的時間會更新。

當您將遊標停留在圖表上時，延遲和活動圖表會顯示主要工作負載的名稱。點擊圖表右側的“工作負載類型”選單，您可以根據工作負載在事件中的角色對其進行排序，包括“sharks”、“bullies”或“victims”，並顯示有關其延遲及其在爭用叢集元件上的使用情況的詳細資訊。您可以將實際值與預期值進行比較，以查看何時工作負載超出其預期的延遲或使用範圍。有關信息，請參閱"Unified Manager 監控的工作負載類型"。

> 當您按延遲的峰值偏差排序時，系統定義的工作負載不會顯示在表中，因為延遲僅適用於使用者定義的工作負載。具有非常低延遲值的工作負載不會顯示在表格中。

有關動態效能閾值的更多信息，請參閱"從動態效能閾值分析事件"。

有關 Unified Manager 如何對工作負載進行排名並確定排序順序的信息，請參閱"Unified Manager 如何決定事件對效能的影響"。

圖表中的數據顯示了上次分析事件之前 24 小時的效能統計。每個工作負載的實際值和預期值均基於工作負載參與事件的時間。例如，工作負載可能會在偵測到事件後才參與其中，因此其效能統計資料可能與事件偵測時的值不符。預設情況下，工作負載會依延遲的峰值（最高）偏差排序。

> 由於 Unified Manager 最多保留 30 天的 5 分鐘歷史效能和事件數據，因此如果事件超過 30 天，則不會顯示任何效能數據。

- 工作負載排序列
  - 延遲圖表

    顯示上次分析時該事件對工作負載延遲的影響。
  - 組件使用狀況列

    顯示有關爭用中的叢集元件的工作負載使用情況的詳細資訊。在圖表中，實際使用情況是一條藍線。紅色條突出顯示事件持續時間，從偵測時間到最後分析時間。有關詳細信息，請參閱 "工作負載效能測量值"。

    > 對於網路元件，由於網路效能統計資料來自群集外的活動，因此不會顯示此列。
  - 組件使用

    顯示網路處理、資料處理和聚合元件的使用率歷史記錄（以百分比表示），或顯示 QoS 策略群組元件的活動記錄（以百分比表示）。此圖表不顯示網路或互連組件。您可以指向統計資料來查看特定時間點的使用情況統計資料。

- 總寫入 **MB/s** 歷史記錄

  僅適用於MetroCluster資源元件，顯示MetroCluster配置中鏡像到配對叢集的所有磁碟區工作負載的總寫入吞吐量（以兆位元組/秒 (MBps) 為單位）。

- 事件歷史

  顯示紅色陰影線來指示爭用元件的歷史事件。對於過時的事件，圖表顯示在偵測到所選事件之前和解決之後發生的事件。

Unified Manager 偵測到的設定更改

Unified Manager 監控叢集的設定變化，以協助您確定變更是否可能導致或促成效能事件。效能資源管理器頁面顯示更改事件圖示 ( ) 來指示偵測到變化的日期和時間。

您可以查看效能資源管理器頁面和工作負載分析頁面中的效能圖表，以了解變更事件是否會影響所選叢集物件的效能。如果在效能事件發生時或大約同時偵測到變化，則該變化可能導致問題，從而觸發事件警報。

Unified Manager 可以偵測下列變更事件，這些事件被歸類為資訊事件：

- 卷在聚合體之間移動。

  Unified Manager 可以偵測移動何時進行、完成或失敗。如果 Unified Manager 在磁碟區移動期間關閉，則當它重新啟動時，它會偵測磁碟區移動並顯示其變更事件。

- 包含一個或多個受監控工作負載的 QoS 策略群組的吞吐量（MB/s 或 IOPS）限制會變更。

  更改策略群組限制可能會導致延遲（反應時間）出現間歇性峰值，這也可能會觸發策略群組的事件。延遲逐漸恢復正常，並且由峰值引起的任何事件都會消失。

- HA 對中的節點接管或歸還其配對節點的儲存。

  Unified Manager 可以偵測接管、部分接手或交還作業何時完成。如果接管是由崩潰的節點引起的，Unified Manager 將不會偵測到該事件。

- ONTAP升級或復原作業已成功完成。

  顯示先前版本和新版本。

事件和嚴重性類型列表

您可以使用事件清單來熟悉事件類別、事件名稱以及您可能在 Unified Manager 中看到的每個事件的嚴重性類型。事件按照物件類別的字母順序列出。

聚合事件

聚合事件為您提供有關聚合狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
聚合離線（ocumEvtAggregateStateOffline）	事件	總計的	批判的
聚合失敗（ocumEvtAggregateStateFailed）	事件	總計的	批判的
聚合限制（ocumEvtAggregateStateRestricted）	風險	總計的	警告
聚合重建（ocumEvtAggregateRaidStateReconstructing）	風險	總計的	警告
聚合降級（ocumEvtAggregateRaidStateDegraded）	風險	總計的	警告
雲層部分可達（ocumEventCloudTierPartiallyReachable）	風險	總計的	警告
雲層無法存取（ocumEventCloudTierUnreachable）	風險	總計的	錯誤
拒絕雲層存取以進行聚合重新定位 *(arlNetraCaCheckFailed)	風險	總計的	錯誤
在儲存故障轉移期間拒絕雲層存取以進行聚合重定位 *(gbNetraCaCheckFailed)	風險	總計的	錯誤
MetroCluster聚合滯後(ocumEvtMetroClusterAggregateLeftBehind)	風險	總計的	錯誤

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
MetroCluster聚合鏡像降級 (ocumEvtMetroClusterAggregateMirrorDegraded)	風險	總計的	錯誤

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
聚合空間幾乎已滿（ocumEvtAggregateNearlyFull）	風險	總計的	警告
聚合空間已滿（ocumEvtAggregateFull）	風險	總計的	錯誤
滿載前的總天數（ocumEvtAggregateDaysUntilFullSoon）	風險	總計的	錯誤
聚合過度提交（ocumEvtAggregateOvercommitted）	風險	總計的	錯誤
聚合幾乎過度承諾（ocumEvtAggregateAlmostOvercommitted）	風險	總計的	警告
聚合快照保留已滿（ocumEvtAggregateSnapReserveFull）	風險	總計的	警告
整體成長率異常（ocumEvtAggregateGrowthRateAbnormal）	風險	總計的	警告

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
發現的總量（不適用）	事件	總計的	資訊
聚合重命名（不適用）	事件	總計的	資訊

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已刪除的集合（不適用）	事件	節點	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
聚合 IOPS 臨界閾值被突破（ocumAggregateIopsIncident）	事件	總計的	批判的
超出聚合 IOPS 警告閾值(ocumAggregateIopsWarning)	風險	總計的	警告
總計 MB/s 臨界門檻突破（ocumAggregateMbpsIncident）	事件	總計的	批判的
超出聚合 MB/s 警告閾值(ocumAggregateMbpsWarning)	風險	總計的	警告
聚合延遲臨界閾值突破（ocumAggregateLatencyIncident）	事件	總計的	批判的
超出聚合延遲警告閾值（ocumAggregateLatencyWarning）	風險	總計的	警告
已使用的總效能容量臨界門檻已突破(ocumAggregatePerfCapacityUsedIncident)	事件	總計的	批判的
已使用總體效能容量警告閾值已突破(ocumAggregatePerfCapacityUsedWarning)	風險	總計的	警告
總體利用率臨界門檻被突破（ocumAggregateUtilizationIncident）	事件	總計的	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
超出聚合利用率警告閾值（ocumAggregateUtilizationWarning）	風險	總計的	警告
聚合磁碟過度利用閾值已突破(ocumAggregateDisksOverUtilizedWarning)	風險	總計的	警告
聚合動態閾值突破（ocumAggregateDynamicEventWarning）	風險	總計的	警告

叢集事件

叢集事件提供有關叢集狀態的信息，使您能夠監控叢集中的潛在問題。事件依影響區域分組，包括事件名稱、陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
叢集缺少備用磁碟（ocumEvtDisksNoSpares）	風險	簇	警告
叢集不可存取（ocumEvtClusterUnreachable）	風險	簇	錯誤
叢集監控失敗（ocumEvtClusterMonitoringFailed）	風險	簇	警告
叢集FabricPool許可證容量限制已超出(ocumEvtExternalCapacityTierSpaceFull)	風險	簇	警告
NVMe-oF 寬限期開始*(nvmfGracePeriodStart)	風險	簇	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVMe-oF 寬限期活動*(nvmfGracePeriodActive)	風險	簇	警告
NVMe-oF 寬限期已過期*(nvmfGracePeriodExpired)	風險	簇	警告
物件維護視窗已啟動（objectMaintenanceWindowStarted）	事件	簇	批判的
物件維護視窗結束（objectMaintenanceWindowEnded）	事件	簇	資訊
MetroCluster剩餘磁碟(ocumEvtSpareDiskLeftBehind)	風險	簇	錯誤
MetroCluster自動排程外切換已停用(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	風險	簇	警告
叢集使用者密碼已更改*(cluster.passwd.changed)	事件	簇	資訊

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
叢集容量不平衡閾值突破（ocumConformanceNodeImbalanceWarning）	風險	簇	警告
叢集雲規劃（clusterCloudTierPlanningWarning）	風險	簇	警告
FabricPool鏡像複製重新同步已完成*（waflCaResyncComplete）	事件	簇	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
FabricPool空間幾乎已滿*(fabricpoolNearlyFull)	風險	簇	錯誤

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
節點已新增（不適用）	事件	簇	資訊
節點已移除（不適用）	事件	簇	資訊
集群已移除（不適用）	事件	簇	資訊
群集新增失敗（不適用）	事件	簇	錯誤
群集名稱已更改（不適用）	事件	簇	資訊
收到緊急 EMS（不適用）	事件	簇	批判的
收到關鍵 EMS（不適用）	事件	簇	批判的
已收到警報 EMS（不適用）	事件	簇	錯誤
錯誤 EMS 已收到（不適用）	事件	簇	警告
警告 EMS 已收到（不適用）	事件	簇	警告
收到調試 EMS（不適用）	事件	簇	警告
通知 EMS 已收到（不適用）	事件	簇	警告
訊息 EMS 已收到（不適用）	事件	簇	警告

ONTAP EMS 事件分為三個 Unified Manager 事件嚴重性等級。

Unified Manager 事件嚴重性等級	ONTAP EMS 事件嚴重性級別

批判的	緊急狀況 批判的
錯誤	警報
警告	錯誤 警告 偵錯 注意 資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
叢集負載不平衡閾值突破()	風險	簇	警告
集群 IOPS 臨界閾值被突破（ocumClusterIopsIncident）	事件	簇	批判的
群集 IOPS 警告閾值超出(ocumClusterIopsWarning)	風險	簇	警告
集群 MB/s 臨界閾值突破（ocumClusterMbpsIncident）	事件	簇	批判的
群集 MB/s 警告閾值超出(ocumClusterMbpsWarning)	風險	簇	警告
集群動態閾值被突破（ocumClusterDynamicEventWarning）	風險	簇	警告

影響領域：安全

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
AutoSupport HTTPS 傳輸已停用（ocumClusterASUPHttpsConfiguredDisabled）	風險	簇	警告
日誌轉送未加密（ocumClusterAuditLogUnencrypted）	風險	簇	警告
預設本機管理員使用者已啟用（ocumClusterDefaultAdminEnabled）	風險	簇	警告
FIPS 模式已停用（ocumClusterFipsDisabled）	風險	簇	警告
登入橫幅已停用（ocumClusterLoginBannerDisabled）	風險	簇	警告
登入橫幅已更改（ocumClusterLoginBannerChanged）	風險	簇	警告
日誌轉送目的地已變更（ocumLogForwardDestinationsChanged）	風險	簇	警告
NTP 伺服器名稱已變更（ocumNtpServerNamesChanged）	風險	簇	警告
NTP 伺服器數量低（securityConfigNTPServerCountLowRisk）	風險	簇	警告
叢集對等通訊未加密（ocumClusterPeerEncryptionDisabled）	風險	簇	警告
SSH 正在使用不安全的密碼（ocumClusterSSHInsecure）	風險	簇	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已啟用 Telnet 協定（ocumClusterTelnetEnabled）	風險	簇	警告
某些ONTAP使用者帳號的密碼使用安全性較低的 MD5 雜湊函數（ocumClusterMD5PasswordHashUsed）	風險	簇	警告
叢集使用自簽名憑證（ocumClusterSelfSignedCertificate）	風險	簇	警告
叢集遠端 Shell 已啟用（ocumClusterRshDisabled）	風險	簇	警告
叢集憑證即將過期（ocumEvtClusterCertificateAboutToExpire）	風險	簇	警告
叢集憑證已過期（ocumEvtClusterCertificateExpired）	風險	簇	錯誤

磁碟事件

磁碟事件為您提供有關磁碟狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
快閃磁碟 - 備用區塊幾乎已用完（ocumEvtClusterFlashDiskFewerSpareBlockError）	風險	簇	錯誤
快閃磁碟 - 無備用區塊（ocumEvtClusterFlashDiskNoSpareBlockCritical）	事件	簇	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
一些未指派的磁碟（ocumEvtClusterUnassignedDisksSome）	風險	簇	警告
部分故障磁碟（ocumEvtDisksSomeFailed）	事件	簇	批判的

圍欄事件

機箱事件為您提供有關資料中心磁碟架機箱狀態的信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
磁碟架風扇故障（ocumEvtShelfFanFailed）	事件	置物架	批判的
磁碟架電源故障（ocumEvtShelfPowerSupplyFailed）	事件	置物架	批判的
未配置磁碟架多路徑(ocumDiskShelfConnectivityNotInMultiPath) 此活動不適用於： • MetroCluster配置中的集群 • 以下平台：FAS2554、FAS2552、FAS2520 和 FAS2240	風險	節點	警告
磁碟架路徑故障（ocumDiskShelfConnectivityPathFailure）	風險	置物架	警告

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已發現磁碟架（不適用）	事件	節點	資訊
磁碟架已移除（不適用）	事件	節點	資訊

粉絲活動

風扇事件為您提供有關資料中心節點上風扇狀態的信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
一個或多個風扇發生故障（ocumEvtFansOneOrMoreFailed）	事件	節點	批判的

抽認卡活動

閃存卡事件為您提供有關資料中心節點上安裝的閃存卡的狀態信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
離線抽認卡（ocumEvtFlashCardOffline）	事件	節點	批判的

Inode 事件

當 inode 已滿或接近已滿時，inode 事件會提供信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
Inode 幾乎已滿（ocumEvtInodesAlmostFull）	風險	體積	警告
Inode 已滿（ocumEvtInodesFull）	風險	體積	錯誤

網路介面 **(LIF)** 事件

網路介面事件提供有關網路介面 (LIF) 狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
網路介面狀態關閉（ocumEvtLifStatusDown）	風險	介面	錯誤
FC/FCoE 網路介面狀態關閉（ocumEvtFCLifStatusDown）	風險	介面	錯誤
網路介面故障轉移不可能（ocumEvtLifFailoverNotPossible）	風險	介面	警告
網路介面不在主連接埠（ocumEvtLifNotAtHomePort）	風險	介面	警告

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
網路介面路由未設定（不適用）	事件	介面	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
網路介面 MB/s 臨界閾值突破（ocumNetworkLifMbpsIncident）	事件	介面	批判的
網路介面 MB/s 警告閾值已超出(ocumNetworkLifMbpsWarning)	風險	介面	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
FC 網路介面 MB/s 臨界閾值突破（ocumFcpLifMbpsIncident）	事件	介面	批判的
FC 網路介面 MB/s 警告閾值超出(ocumFcpLifMbpsWarning)	風險	介面	警告
NVMf FC 網路介面 MB/s 臨界閾值突破（ocumNvmfFcLifMbpsIncident）	事件	介面	批判的
NVMf FC 網路介面 MB/s 警告閾值超出(ocumNvmfFcLifMbpsWarning)	風險	介面	警告

LUN 事件

LUN 事件為您提供有關 LUN 狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN 離線(ocumEvtLunOffline)	事件	邏輯單元號	批判的
LUN 已銷毀*(lunDestroy)	事件	邏輯單元號	資訊
LUN 對應了 igroup 中不支援的作業系統（igroupUnsupportedOsType）	事件	邏輯單元號	警告
造訪 LUN 的單一活動路徑(ocumEvtLunSingleActivePath)	風險	邏輯單元號	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
沒有存取 LUN 的活動路徑（ocumEvtLunNotReachable）	事件	邏輯單元號	批判的
沒有存取 LUN 的最佳化路徑（ocumEvtLunOptimizedPathInactive）	風險	邏輯單元號	警告
沒有從 HA 合作夥伴訪問 LUN 的路徑（ocumEvtLunHaPathInactive）	風險	邏輯單元號	警告
沒有從 HA 對中的一個節點存取 LUN 的路徑（ocumEvtLunNodePathStatusDown）	風險	邏輯單元號	錯誤

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN 快照複製空間不足（ocumEvtLunSnapshotNotPossible）	風險	體積	警告

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN 對應了 igroup 中不支援的作業系統（igroupUnsupportedOsType）	風險	邏輯單元號	警告

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN IOPS 臨界閾值被突破（ocumLunIopsIncident）	事件	邏輯單元號	批判的
LUN IOPS 警告閾值超出(ocumLunIopsWarning)	風險	邏輯單元號	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN MB/s 臨界閾值超出（ocumLunMbpsIncident）	事件	邏輯單元號	批判的
超出 LUN MB/s 警告閾值 (ocumLunMbpsWarning)	風險	邏輯單元號	警告
LUN 延遲 ms/op 臨界閾值超出 (ocumLunLatencyIncident)	事件	邏輯單元號	批判的
LUN 延遲 ms/op 警告閾值已超出 (ocumLunLatencyWarning)	風險	邏輯單元號	警告
LUN 延遲和 IOPS 臨界閾值被突破 (ocumLunLatencyIopsIncident)	事件	邏輯單元號	批判的
LUN 延遲和 IOPS 警告閾值超出 (ocumLunLatencyIopsWarning)	風險	邏輯單元號	警告
LUN 延遲和 MB/s 臨界閾值被突破（ocumLunLatencyMbpsIncident）	事件	邏輯單元號	批判的
超出 LUN 延遲和 MB/s 警告閾值 (ocumLunLatencyMbpsWarning)	風險	邏輯單元號	警告
LUN 延遲和聚合效能容量使用臨界閾值被突破 (ocumLunLatencyAggregatePerfCapacityUsedIncident)	事件	邏輯單元號	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN 延遲和聚合效能容量使用警告閾值已突破 (ocumLunLatencyAggregatePerfCapacityUsedWarning)	風險	邏輯單元號	警告
LUN 延遲和聚合利用率臨界閾值被突破 (ocumLunLatencyAggregateUtilizationIncident)	事件	邏輯單元號	批判的
LUN 延遲和聚合利用率警告閾值超出 (ocumLunLatencyAggregateUtilizationWarning)	風險	邏輯單元號	警告
LUN 延遲和節點效能容量使用臨界閾值被突破 (ocumLunLatencyNodePerfCapacityUsedIncident)	事件	邏輯單元號	批判的
LUN 延遲和節點效能容量使用警告閾值已突破 (ocumLunLatencyNodePerfCapacityUsedWarning)	風險	邏輯單元號	警告
LUN 延遲和已使用節點效能容量 - 超出接管臨界閾值 (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	事件	邏輯單元號	批判的
LUN 延遲和已使用節點效能容量 - 超出接管警告閾值 (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	風險	邏輯單元號	警告
LUN 延遲和節點利用率臨界閾值被突破 (ocumLunLatencyNodeUtilizationIncident)	事件	邏輯單元號	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
LUN 延遲和節點利用率警告閾值超出 (ocumLunLatencyNodeUtilizationWarning)	風險	邏輯單元號	警告
QoS LUN 最大 IOPS 警告閾值超出 (ocumQosLunMaxIopsWarning)	風險	邏輯單元號	警告
QoS LUN 最大 MB/s 警告閾值超出 (ocumQosLunMaxMbpsWarning)	風險	邏輯單元號	警告
工作負載 LUN 延遲閾值超出效能服務等級策略所定義的範圍 (ocumConformanceLatencyWarning)	風險	邏輯單元號	警告

管理站事件

管理站事件為您提供有關安裝 Unified Manager 的伺服器狀態的信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
管理伺服器磁碟空間幾乎已滿（ocumEvtUnifiedManagerDiskSpaceNearlyFull）	風險	管理站	警告
管理伺服器磁碟空間已滿（ocumEvtUnifiedManagerDiskSpaceFull）	事件	管理站	批判的
管理伺服器記憶體不足（ocumEvtUnifiedManagerMemoryLow）	風險	管理站	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
管理伺服器記憶體即將耗盡（ocumEvtUnifiedManagerMemoryAlmostOut）	事件	管理站	批判的
MySQL 日誌檔案大小增加；需要重新啟動（ocumEvtMysqlLogFileSizeWarning）	事件	管理站	警告
總審計日誌大小分配即將滿	風險	管理站	警告
Syslog 伺服器憑證即將過期	風險	管理站	警告
Syslog 伺服器憑證已過期	風險	管理站	錯誤
審計日誌檔案被篡改	風險	管理站	警告
審計日誌檔已刪除	風險	管理站	警告
Syslog 伺服器連線錯誤	風險	管理站	錯誤
Syslog 伺服器設定已更改	事件	管理站	警告

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
效能資料分析受到影響（ocumEvtUnifiedManagerDataMissingAnalyze）	風險	管理站	警告
效能資料收集受到影響（ocumEvtUnifiedManagerDataMissingCollection）	事件	管理站	批判的

最後兩個效能事件僅適用於 Unified Manager 7.2。如果其中任何一個事件處於「新」狀態，然後您升級到較新版本的 Unified Manager 軟體，則不會自動清除這些事件。您需要手動將事件移至「已解決」狀態。

MetroCluster Bridge 事件

MetroCluster Bridge 事件為您提供有關網橋狀態的信息，以便您可以監控 FC 配置上

的MetroCluster中的潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
橋不可達（ocumEvtBridgeUnreachable）	事件	MetroCluster橋接器	批判的
橋溫異常(ocumEvtBridgeTemperatureAbnormal)	事件	MetroCluster橋接器	批判的

MetroCluster連線事件

連接事件為您提供有關叢集元件之間以及MetroCluster over FC 和MetroCluster over IP 配置中的叢集之間的連接的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

兩種配置中常見的事件

這些連線事件對於MetroCluster over FC 和MetroCluster over IP 配置都很常見。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
MetroCluster合作夥伴之間的所有連結均已關閉(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	事件	MetroCluster關係	批判的
MetroCluster合作夥伴無法透過對等網路存取 (MetroCluster)	事件	MetroCluster關係	批判的
MetroCluster災難復原能力受到影響（ocumEvtMetroClusterDRStatusImpacted）	風險	MetroCluster關係	批判的
MetroCluster配置已切換（ocumEvtMetroClusterDRStatusImpacted）	風險	MetroCluster關係	警告

基於 **FC** 的**MetroCluster**配置

這些事件與 FC 配置上的MetroCluster有關。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
所有交換器間連結均斷開（ocumEvtMetroClusterAllISLBetweenSwitchesDown）	事件	MetroCluster交換器間連接	批判的
FC-SAS 橋接至儲存堆疊連結關閉(ocumEvtBridgeSasPortDown)	事件	MetroCluster橋接堆疊連接	批判的
MetroCluster配置部分切換(ocumEvtMetroClusterDRStatusPartiallyImpacted)	風險	MetroCluster關係	錯誤
節點到 FC 交換器所有 FC-VI 互連鏈路關閉(ocumEvtMccNodeSwitchFcviLinksDown)	事件	MetroCluster節點交換器連接	批判的
節點到 FC 交換器一個或多個 FC 發起方鏈路斷開(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	風險	MetroCluster節點交換器連接	警告
節點到 FC 切換所有 FC 發起方鏈路關閉(ocumEvtMccNodeSwitchFcLinksDown)	事件	MetroCluster節點交換器連接	批判的
切換到 FC-SAS 橋接器 FC 連結關閉（ocumEvtMccSwitchBridgeFcLinksDown）	事件	MetroCluster交換器橋接連接	批判的
節點間所有 FC VI 互連連結均已關閉(ocumEvtMccInterNodeLinksDown)	事件	節點間連接	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
節點間一個或多個 FC VI 互連連結斷開 (ocumEvtMccInterNodeLinksOneOrMoreDown)	風險	節點間連接	警告
節點到橋接連結斷開（ocumEvtMccNodeBridgeLinksDown）	事件	節點橋接	批判的
節點到儲存堆疊所有 SAS 連結均關閉 (ocumEvtMccNodeStackLinksDown)	事件	節點堆疊連接	批判的
節點到儲存堆疊一個或多個 SAS 連結斷開 (ocumEvtMccNodeStackLinksOneOrMoreDown)	風險	節點堆疊連接	警告

MetroCluster over IP 配置

這些事件與MetroCluster over IP 配置有關。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
MetroCluster IP 站點間連線狀態已關閉 (mccIntersiteconnectivityStatusDown)	風險	MetroCluster關係	批判的
MetroCluster-IP 節點到交換器的連線離線 (mccIpPortStatusOffline)	風險	節點	錯誤

MetroCluster交換器事件

MetroCluster over FC 配置的MetroCluster交換器事件為您提供有關MetroCluster交換器狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
開關溫度異常(ocumEvtSwitchTemperatureAbnormal)	事件	MetroCluster交換機	批判的
交換器不可達（ocumEvtSwitchUnreachable）	事件	MetroCluster交換機	批判的
交換器風扇故障（ocumEvtSwitchFansOneOrMoreFailed）	事件	MetroCluster交換機	批判的
開關電源故障（ocumEvtSwitchPowerSuppliesOneOrMoreFailed）	事件	MetroCluster交換機	批判的
開關溫度感測器故障（ocumEvtSwitchTemperatureSensorFailed） 此事件僅適用於Cisco交換器。	事件	MetroCluster交換機	批判的

NVMe 命名空間事件

NVMe 命名空間事件為您提供有關命名空間狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVMeNS 離線 *(nvmeNamespaceStatusOffline)	事件	命名空間	資訊
NVMeNS 線上 *(nvmeNamespaceStatusOnline)	事件	命名空間	資訊

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVMeNS 空間不足 *(nvmeNamespaceSpaceOutOfSpace)	風險	命名空間	警告
NVMeNS 銷毀 *(nvmeNamespaceDestroy)	事件	命名空間	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVMe 命名空間 IOPS 臨界閾值被突破（ocumNvmeNamespaceIopsIncident）	事件	命名空間	批判的
NVMe 命名空間 IOPS 警告閾值已超出 (ocumNvmeNamespaceIopsWarning)	風險	命名空間	警告
NVMe 命名空間 MB/s 臨界閾值被突破（ocumNvmeNamespaceMbpsIncident）	事件	命名空間	批判的
超出 NVMe 命名空間 MB/s 警告閾值 (ocumNvmeNamespaceMbpsWarning)	風險	命名空間	警告
NVMe 命名空間延遲 ms/op 臨界閾值突破（ocumNvmeNamespaceLatencyIncident）	事件	命名空間	批判的
NVMe 命名空間延遲 ms/op 警告閾值已超出 (ocumNvmeNamespaceLatencyWarning)	風險	命名空間	警告
NVMe 命名空間延遲和 IOPS 臨界閾值被突破（ocumNvmeNamespaceLatencyIopsIncident）	事件	命名空間	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVMe 命名空間延遲和 IOPS 警告閾值已超出 (ocumNvmeNamespaceLatencyIopsWarning)	風險	命名空間	警告
NVMe 命名空間延遲和 MB/s 臨界閾值被突破（ocumNvmeNamespaceLatencyMbpsIncident）	事件	命名空間	批判的
NVMe 命名空間延遲和 MB/s 警告閾值超出 (ocumNvmeNamespaceLatencyMbpsWarning)	風險	命名空間	警告

節點事件

節點事件為您提供有關節點狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
節點根捲空間幾乎已滿（ocumEvtClusterNodeRootVolumeSpaceNearlyFull）	風險	節點	警告
雲端 AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	風險	節點	錯誤
雲 AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	風險	節點	錯誤
雲 AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	風險	節點	錯誤

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
雲端 AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	風險	節點	錯誤
雲 AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	事件	節點	資訊
雲端 AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	風險	節點	錯誤
雲端 AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	風險	節點	錯誤
雲層主機無法解析 *(ocumObjstoreHostUnresolvable)	風險	節點	錯誤
雲層叢集間網路介面關閉*(ocumObjstoreInterClusterLifDown)	風險	節點	錯誤
其中一個 NFSv4 池已耗盡 *(nbladeNfsv4PoolEXhaust)	事件	節點	批判的
請求不符雲層簽名*（oscSignatureMismatch）	風險	節點	錯誤

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
QoS 監視器記憶體最大值 *(ocumQosMonitorMemoryMaxed)	風險	節點	錯誤
QoS 監視器記憶體減少 *(ocumQosMonitorMemoryAbated)	事件	節點	資訊

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
節點重命名（不適用）	事件	節點	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
節點 IOPS 臨界閾值被突破（ocumNodeIopsIncident）	事件	節點	批判的
節點 IOPS 警告閾值超出 (ocumNodeIopsWarning)	風險	節點	警告
節點 MB/s 臨界閾值突破（ocumNodeMbpsIncident）	事件	節點	批判的
節點 MB/s 警告閾值超出 (ocumNodeMbpsWarning)	風險	節點	警告
節點延遲 ms/op 臨界閾值突破（ocumNodeLatencyIncident）	事件	節點	批判的
節點延遲 ms/op 警告閾值超出 (ocumNodeLatencyWarning)	風險	節點	警告
節點效能容量使用臨界閾值已突破 (ocumNodePerfCapacityUsedIncident)	事件	節點	批判的
節點效能容量使用警告閾值超出 (ocumNodePerfCapacityUsedWarning)	風險	節點	警告
已使用節點效能容量 - 超出接管臨界閾值 (ocumNodePerfCapacityUsedTakeoverIncident)	事件	節點	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已使用節點效能容量 - 超出接管警告閾值 (ocumNodePerfCapacityUsedTakeoverWarning)	風險	節點	警告
節點利用率臨界閾值被突破 (ocumNodeUtilizationIncident)	事件	節點	批判的
節點利用率警告閾值超出 (ocumNodeUtilizationWarning)	風險	節點	警告
節點 HA 對過度利用閾值被突破 (ocumNodeHaPairOverUtilizedInformation)	事件	節點	資訊
節點磁碟碎片閾值超出（ocumNodeDiskFragmentationWarning）	風險	節點	警告
效能容量使用閾值超出 (ocumNodeOverUtilizedWarning)	風險	節點	警告
節點動態閾值被突破（ocumNodeDynamicEventWarning）	風險	節點	警告

影響領域：安全

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
諮詢 ID：NTAP-<*advisory ID*>(ocumx)	風險	節點	批判的

NVRAM電池事件

NVRAM電池事件為您提供有關電池狀態的信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
NVRAM電池電量低（ocumEvtNvramBatteryLow）	風險	節點	警告
NVRAM電池放電(ocumEvtNvramBatteryDischarged)	風險	節點	錯誤
NVRAM電池過度充電（ocumEvtNvramBatteryOverCharged）	事件	節點	批判的

港口事件

連接埠事件為您提供有關叢集連接埠的狀態，以便您可以監控連接埠上的變更或問題，例如連接埠是否已關閉。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
連接埠狀態關閉（ocumEvtPortStatusDown）	事件	節點	批判的

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
網路連接埠 MB/s 臨界閾值突破（ocumNetworkPortMbpsIncident）	事件	港口	批判的
網路連接埠 MB/s 警告閾值超出(ocumNetworkPortMbpsWarning)	風險	港口	警告
FCP 連接埠 MB/s 臨界閾值突破（ocumFcpPortMbpsIncident）	事件	港口	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
FCP 連接埠 MB/s 警告閾值超出(ocumFcpPortMbpsWarning)	風險	港口	警告
網路連接埠利用率臨界閾值被突破（ocumNetworkPortUtilizationIncident）	事件	港口	批判的
網路連接埠利用率警告閾值超出(ocumNetworkPortUtilizationWarning)	風險	港口	警告
FCP 連接埠利用率臨界閾值被突破（ocumFcpPortUtilizationIncident）	事件	港口	批判的
FCP 連接埠利用率警告閾值超出(ocumFcpPortUtilizationWarning)	風險	港口	警告

電源事件

電源事件為您提供有關硬體狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
一個或多個電源故障(ocumEvtPowerSupplyOneOrMoreFailed)	事件	節點	批判的

保護事件

保護事件會告訴您作業是否失敗或中止，以便您可以監控問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：保護

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
保護作業失敗（ocumEvtProtectionJobTaskFailed）	事件	磁碟區或儲存服務	批判的
保護作業已中止（ocumEvtProtectionJobAborted）	風險	磁碟區或儲存服務	警告

Qtree 事件

Qtree 事件為您提供有關 qtree 容量以及檔案和磁碟限制的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
Qtree 空間幾乎已滿(ocumEvtQtreeSpaceNearlyFull)	風險	qtree	警告
Qtree 空間已滿(ocumEvtQtreeSpaceFull)	風險	qtree	錯誤
Qtree 空間正常(ocumEvtQtreeSpaceThresholdOk)	事件	qtree	資訊
已達到 Qtree 檔案硬限制(ocumEvtQtreeFilesHardLimitReached)	事件	qtree	批判的
超出 Qtree 檔案軟體限制(ocumEvtQtreeFilesSoftLimitBreached)	風險	qtree	警告
已達到 Qtree 空間硬限制(ocumEvtQtreeSpaceHardLimitReached)	事件	qtree	批判的
超出 Qtree 空間軟限制(ocumEvtQtreeSpaceSoftLimitBreached)	風險	qtree	警告

服務處理器事件

服務處理器事件為您提供有關處理器狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
服務處理器未配置（ocumEvtServiceProcessorNotConfigured）	風險	節點	警告
服務處理器離線（ocumEvtServiceProcessorOffline）	風險	節點	錯誤

SnapMirror關係事件

SnapMirror關係事件為您提供有關非同步和同步SnapMirror關係狀態的信息，以便您可以監控潛在問題。儲存虛擬機器和磁碟區都會產生非同步SnapMirror關係事件，但僅為磁碟區關係產生同步SnapMirror關係事件。對於作為儲存虛擬機器災難復原關係一部分的組成捲，不會產生任何事件。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：保護

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

SnapMirror關係事件是針對受儲存虛擬機器災難復原保護的儲存虛擬機器產生的，但不針對任何組成物件關係產生。

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
鏡像複製不健康（ocumEvtSnapmirrorRelationshipUnhealthy）	風險	SnapMirror關係	警告
鏡像複製中斷（ocumEvtSnapmirrorRelationshipStateBrokenoff）	風險	SnapMirror關係	錯誤
鏡像複製初始化失敗（ocumEvtSnapmirrorRelationshipInitializeFailed）	風險	SnapMirror關係	錯誤

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
鏡像複製更新失敗（ocumEvtSnapmirrorRelationshipUpdateFailed）	風險	SnapMirror關係	錯誤
鏡像複製延遲錯誤（ocumEvtSnapMirrorRelationshipLagError）	風險	SnapMirror關係	錯誤
鏡像複製滯後警告（ocumEvtSnapMirrorRelationshipLagWarning）	風險	SnapMirror關係	警告
鏡像複製重新同步失敗（ocumEvtSnapmirrorRelationshipResyncFailed）	風險	SnapMirror關係	錯誤
同步複製不同步*(syncSnapmirrorRelationshipOutofsync)	風險	SnapMirror關係	警告
同步複製已恢復*（syncSnapmirrorRelationshipInSync）	事件	SnapMirror關係	資訊
同步複製自動重新同步失敗*（syncSnapmirrorRelationshipAutoSyncRetryFailed）	風險	SnapMirror關係	錯誤
在叢集上新增了 ONTAP 調解器(SnapmirrorMediatorAdded)	事件	簇	資訊
ONTAP 調解器已從叢集中刪除（snapmirrorMediatorRemoved）	事件	簇	資訊
無法從叢集存取 ONTAP 調解器(SnapmirrorMediatorUnreachable)	風險	調解員	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
無法從叢集存取 ONTAP 調解器（SnapmirrorMediatorMisconfigured）	風險	調解員	錯誤
ONTAP 調解器連線已重新建立、重新同步並準備好進行SnapMirror主動同步（snapmirrorMediatorInQuorum）	事件	調解員	資訊

非同步鏡像和 **Vault** 關係事件

非同步鏡像和 Vault 關係事件為您提供有關非同步SnapMirror和 Vault 關係狀態的信息，以便您可以監控潛在問題。捲和儲存虛擬機器保護關係均支援非同步鏡像和保險庫關係事件。但儲存虛擬機器災難復原僅不支援 Vault 關係。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：保護

也會為受儲存虛擬機器災難復原保護的儲存虛擬機器產生SnapMirror和 Vault 關係事件，但不會為任何組成物件關係產生事件。

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
非同步鏡像和保險庫不健康（ocumEvtMirrorVaultRelationshipUnhealthy）	風險	SnapMirror關係	警告
非同步鏡像和保險庫斷開（ocumEvtMirrorVaultRelationshipStateBrokenoff）	風險	SnapMirror關係	錯誤
非同步鏡像和 Vault 初始化失敗（ocumEvtMirrorVaultRelationshipInitializeFailed）	風險	SnapMirror關係	錯誤
非同步鏡像和 Vault 更新失敗（ocumEvtMirrorVaultRelationshipUpdateFailed）	風險	SnapMirror關係	錯誤

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
非同步鏡像和 Vault 滯後錯誤（ocumEvtMirrorVaultRelationshipLagError）	風險	SnapMirror關係	錯誤
非同步鏡像和 Vault 滯後警告（ocumEvtMirrorVaultRelationshipLagWarning）	風險	SnapMirror關係	警告
非同步鏡像和 Vault 重新同步失敗（ocumEvtMirrorVaultRelationshipResyncFailed）	風險	SnapMirror關係	錯誤

Active IQ網站（Config Advisor ）引發「 SnapMirror更新失敗」事件。

快照事件

快照事件提供有關快照狀態的信息，使您能夠監視快照中是否存在潛在問題。事件依影響區域分組，包括事件名稱、陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
快照自動刪除已停用（不適用）	事件	體積	資訊
已啟用快照自動刪除（不適用）	事件	體積	資訊
快照自動刪除配置已修改（不適用）	事件	體積	資訊

SnapVault關係事件

SnapVault關係事件為您提供有關SnapVault關係狀態的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：保護

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
非同步 Vault 不健康（ocumEvtSnapVaultRelationshipUnhealthy）	風險	SnapMirror關係	警告
非同步保險庫斷開（ocumEvtSnapVaultRelationshipStateBrokenoff）	風險	SnapMirror關係	錯誤
非同步 Vault 初始化失敗（ocumEvtSnapVaultRelationshipInitializeFailed）	風險	SnapMirror關係	錯誤
非同步 Vault 更新失敗（ocumEvtSnapVaultRelationshipUpdateFailed）	風險	SnapMirror關係	錯誤
非同步 Vault 滯後錯誤（ocumEvtSnapVaultRelationshipLagError）	風險	SnapMirror關係	錯誤
非同步 Vault 滯後警告（ocumEvtSnapVaultRelationshipLagWarning）	風險	SnapMirror關係	警告
非同步 Vault 重新同步失敗（ocumEvtSnapvaultRelationshipResyncFailed）	風險	SnapMirror關係	錯誤

儲存故障轉移設定事件

儲存故障轉移 (SFO) 設定事件為您提供有關儲存故障轉移是否已停用或未配置的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
儲存故障轉移互連一個或多個連結斷開(ocumEvtSfoInterconnectOneOrMoreLinksDown)	風險	節點	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
儲存故障轉移已停用（ocumEvtSfoSettingsDisabled）	風險	節點	錯誤
未配置儲存故障轉移（ocumEvtSfoSettingsNotConfigured）	風險	節點	錯誤
儲存故障轉移狀態 - 接管（ocumEvtSfoStateTakeover）	風險	節點	警告
儲存故障轉移狀態 - 部分交還(ocumEvtSfoStatePartialGiveback)	風險	節點	錯誤
儲存故障轉移節點狀態關閉（ocumEvtSfoNodeStatusDown）	風險	節點	錯誤
儲存故障轉移接管不可能（ocumEvtSfoTakeoverNotPossible）	風險	節點	錯誤

儲存服務事件

儲存服務事件為您提供有關儲存服務的建立和訂閱的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已建立儲存服務（不適用）	事件	儲存服務	資訊
已訂購儲存服務（不適用）	事件	儲存服務	資訊
儲存服務已取消（不適用）	事件	儲存服務	資訊

影響區域：保護

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
意外刪除託管SnapMirror關係 ocumEvtStorageServiceUnsupportedRelationshipDeletion	風險	儲存服務	警告
儲存服務成員磁碟區意外刪除（ocumEvtStorageServiceUnexpectedVolumeDeletion）	事件	儲存服務	批判的

倉儲貨架活動

儲存架事件會告訴您儲存架是否有異常，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
異常電壓範圍(ocumEvtShelfVoltageAbnormal)	風險	置物架	警告
異常電流範圍(ocumEvtShelfCurrentAbnormal)	風險	置物架	警告
溫度異常（ocumEvtShelfTemperatureAbnormal）	風險	置物架	警告

儲存虛擬機器事件

儲存虛擬機器 (SVM) 事件為您提供有關儲存虛擬機器 (SVM) 狀態的信息，以便您監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
儲存虛擬機器 CIFS 服務關閉（ocumEvtVserverCifsServiceStatusDown）	事件	支援向量機	批判的
SVM CIFS 服務未配置（不適用）	事件	支援向量機	資訊
嘗試連接不存在的 CIFS 共用 *(nbladeCifsNoPrivShare)	事件	支援向量機	批判的
CIFS NetBIOS 名稱衝突*(nbladeCifsNbNameConflict)	風險	支援向量機	錯誤
CIFS 磁碟區複製作業失敗*(cifsShadowCopyFailure)	風險	支援向量機	錯誤
許多 CIFS 連接*(nbladeCifsManyAuths)	風險	支援向量機	錯誤
超出最大 CIFS 連線數 *(nbladeCifsMaxOpenSameFile)	風險	支援向量機	錯誤
超出每個使用者的最大 CIFS 連線數 *(nbladeCifsMaxSessPerUsrConn)	風險	支援向量機	錯誤
SVM FC/FCoE 服務關閉(ocumEvtVserverFcServiceStatusDown)	事件	支援向量機	批判的
SVM iSCSI 服務關閉（ocumEvtVserverIscsiServiceStatusDown）	事件	支援向量機	批判的
儲存虛擬機器 NFS 服務關閉（ocumEvtVserverNfsServiceStatusDown）	事件	支援向量機	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
SVM FC/FCoE 服務未配置（不適用）	事件	支援向量機	資訊
SVM iSCSI 服務未配置（不適用）	事件	支援向量機	資訊
SVM NFS 服務未配置（不適用）	事件	支援向量機	資訊
儲存虛擬機器已停止（ocumEvtVserverDown）	風險	支援向量機	警告
AV 伺服器太忙，無法接受新的掃描請求*(nbladeVscanConnBackPressure)	風險	支援向量機	錯誤
沒有用於病毒掃描的 AV 伺服器連線*(nbladeVscanNoScannerConn)	事件	支援向量機	批判的
未註冊 AV 伺服器*(nbladeVscanNoRegdScanner)	風險	支援向量機	錯誤
無回應的 AV 伺服器連線*(nbladeVscanConnInactive)	事件	支援向量機	資訊
未經授權的使用者嘗試存取 AV 伺服器*(nbladeVscanBadUserPrivAccess)	風險	支援向量機	錯誤
AV 伺服器發現病毒*(nbladeVscanVirusDetected)	風險	支援向量機	錯誤

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
發現 SVM（不適用）	事件	支援向量機	資訊

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
SVM 已刪除（不適用）	事件	簇	資訊
SVM 已重新命名（不適用）	事件	支援向量機	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
SVM IOPS 臨界閾值被突破（ocumSvmIopsIncident）	事件	支援向量機	批判的
超出 SVM IOPS 警告閾值 (ocumSvmIopsWarning)	風險	支援向量機	警告
超出 SVM MB/s 臨界閾值（ocumSvmMbpsIncident）	事件	支援向量機	批判的
超出 SVM MB/s 警告閾值 (ocumSvmMbpsWarning)	風險	支援向量機	警告
SVM 延遲臨界閾值超出 (ocumSvmLatencyIncident)	事件	支援向量機	批判的
超出 SVM 延遲警告閾值 (ocumSvmLatencyWarning)	風險	支援向量機	警告

影響領域：安全

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
稽核日誌已停用（ocumVserverAuditLogDisabled）	風險	支援向量機	警告
登入橫幅已停用（ocumVserverLoginBannerDisabled）	風險	支援向量機	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
SSH 使用不安全的密碼（ocumVserverSSHInsecure）	風險	支援向量機	警告
登入橫幅已更改（ocumVserverLoginBannerChanged）	風險	支援向量機	警告
儲存虛擬機器反勒索軟體監控已停用（antiRansomwareSvmStateDisabled）	風險	支援向量機	警告
儲存虛擬機器反勒索軟體監控已啟用（學習模式）（antiRansomwareSvmStateDryrun）	事件	支援向量機	資訊
適用於反勒索軟體監控的儲存虛擬機器（學習模式）（ocumEvtSvmArwCandidate）	事件	支援向量機	資訊

使用者和群組配額事件

使用者和群組配額事件為您提供有關使用者和使用者群組配額容量以及文件和磁碟限制的信息，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
超出使用者或群組配額磁碟空間軟體限制(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	風險	使用者或群組配額	警告
達到使用者或群組配額磁碟空間硬限制(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	事件	使用者或群組配額	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
違反使用者或群組配額檔案計數軟體限制 (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	風險	使用者或群組配額	警告
達到使用者或群組配額檔案數硬限制 (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	事件	使用者或群組配額	批判的

成交量事件

卷事件提供有關磁碟區狀態的信息，使您能夠監控潛在問題。事件依影響區域分組，包括事件名稱、陷阱名稱、影響等級、來源類型和嚴重性。

星號 (*) 標識已轉換為 Unified Manager 事件的 EMS 事件。

影響領域：可用性

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
音量限制（ocumEvtVolumeRestricted）	風險	體積	警告
卷線離線（ocumEvtVolumeOffline）	事件	體積	批判的
卷部分可用（ocumEvtVolumePartiallyAvailable）	風險	體積	錯誤
卷已卸載（不適用）	事件	體積	資訊
已安裝磁碟區（不適用）	事件	體積	資訊
磁碟區已重新安裝（不適用）	事件	體積	資訊
磁碟區連接路徑非活動狀態（ocumEvtVolumeJunctionPathInactive）	風險	體積	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
已啟用磁碟區自動調整大小（不適用）	事件	體積	資訊
磁碟區自動調整大小 - 已停用（不適用）	事件	體積	資訊
磁碟區自動調整最大容量已修改（不適用）	事件	體積	資訊
磁碟區自動調整增量大小已修改（不適用）	事件	體積	資訊

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
精簡配置磁碟區空間風險（ocumThinProvisionVolumeSpaceAtRisk）	風險	體積	警告
體積效率操作錯誤（ocumEvtVolumeEfficiencyOperationError）	風險	體積	錯誤
卷空間已滿（ocumEvtVolumeFull）	風險	體積	錯誤
卷空間幾乎已滿（ocumEvtVolumeNearlyFull）	風險	體積	警告
捲邏輯空間已滿*(volumeLogicalSpaceFull)	風險	體積	錯誤
捲邏輯空間幾乎已滿*(volumeLogicalSpaceNearlyFull)	風險	體積	警告
卷邏輯空間正常*(volumeLogicalSpaceAllOK)	事件	體積	資訊

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
卷快照保留空間已滿（ocumEvtSnapshotFull）	風險	體積	警告
快照副本過多（ocumEvtSnapshotTooMany）	風險	體積	錯誤
卷 Qtree 配額過載(ocumEvtVolumeQtreeQuotaOvercommitted)	風險	體積	錯誤
卷 Qtree 配額幾乎過量使用（ocumEvtVolumeQtreeQuotaAlmostOvercommitted）	風險	體積	警告
成交量成長率異常（ocumEvtVolumeGrowthRateAbnormal）	風險	體積	警告
交易量滿前的天數（ocumEvtVolumeDaysUntilFullSoon）	風險	體積	錯誤
磁碟區空間保證已停用（不適用）	事件	體積	資訊
磁碟區空間保證已啟用（不適用）	事件	體積	資訊
磁碟區空間保證已修改（不適用）	事件	體積	資訊
卷快照預留天數至滿（ocumEvtVolumeSnapshotReserveDaysUntilFullSoon）	風險	體積	錯誤
FlexGroup組成部分存在空間問題*(flexGroupConstituentsHaveSpaceIssues)	風險	體積	錯誤

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
FlexGroup組成部分空間狀態全部正常 *(flexGroupConstituentsSpaceStatusAllOK)	事件	體積	資訊
FlexGroup組成部分存在 Inode 問題 *(flexGroupConstituentsHaveInodesIssues)	風險	體積	錯誤
FlexGroup組成部分 Inode 狀態全部正常 *(flexGroupConstituentsInodesStatusAllOK)	事件	體積	資訊
WAFL磁碟區自動調整大小失敗 *(waflVolAutoSizeFail)	風險	體積	錯誤
WAFL磁碟區自動調整大小完成 *(waflVolAutoSizeDone)	事件	體積	資訊
FlexGroup捲利用率超過 80%*	事件	體積	錯誤
FlexGroup捲利用率超過 90%*	事件	體積	批判的
磁碟區儲存效率異常（ocumVolumeAbnormalStorageEfficiencyWarning）	風險	體積	警告
磁碟區快照預留未充分利用（volumeSnaphotReserveUnderutilizedWarning）	事件	體積	警告
卷快照預留未充分利用（volumeSnaphotReserveUnderutilizedCleared）	事件	體積	警告

影響區域：配置

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
磁碟區已重新命名（不適用）	事件	體積	資訊
已發現卷（不適用）	事件	體積	資訊
卷已刪除（不適用）	事件	體積	資訊

影響領域：性能

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
QoS 磁碟區最大 IOPS 警告閾值超出 (ocumQosVolumeMaxIopsWarning)	風險	體積	警告
QoS 磁碟區最大 MB/s 警告閾值超出 (ocumQosVolumeMaxMbpsWarning)	風險	體積	警告
QoS 磁碟區最大 IOPS/TB 警告閾值已超出 (ocumQosVolumeMaxIopsPerTbWarning)	風險	體積	警告
工作負載卷延遲閾值超出效能服務等級策略所定義的範圍（ocumConformanceLatencyWarning）	風險	體積	警告
卷 IOPS 臨界閾值被突破（ocumVolumeIopsIncident）	事件	體積	批判的
卷 IOPS 警告閾值超出 (ocumVolumeIopsWarning)	風險	體積	警告
卷 MB/s 臨界閾值突破（ocumVolumeMbpsIncident）	事件	體積	批判的

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
超出磁碟區 MB/s 警告閾值（ocumVolumeMbpsWarning）	風險	體積	警告
突破磁碟區延遲臨界閾值(ocumVolumeLatencyIncident)	事件	體積	批判的
超出磁碟區延遲警告閾值(ocumVolumeLatencyWarning)	風險	體積	警告
卷緩存未命中率臨界閾值被突破（ocumVolumeCacheMissRatioIncident）	事件	體積	批判的
卷緩存未命中率警告閾值已超出(ocumVolumeCacheMissRatioWarning)	風險	體積	警告
卷延遲和 IOPS 臨界閾值被突破（ocumVolumeLatencyIopsIncident）	事件	體積	批判的
卷延遲和 IOPS 警告閾值超出(ocumVolumeLatencyIopsWarning)	風險	體積	警告
卷延遲和 MB/s 臨界閾值被突破（ocumVolumeLatencyMbpsIncident）	事件	體積	批判的
超出磁碟區延遲和 MB/s 警告閾值(ocumVolumeLatencyMbpsWarning)	風險	體積	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
卷延遲和聚合效能容量使用臨界閾值被突破（ocumVolumeLatencyAggregatePerfCapacityUsedIncident）	事件	體積	批判的
磁碟區延遲和聚合效能容量使用警告閾值已突破(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	風險	體積	警告
卷延遲和聚合利用率臨界閾值被突破（ocumVolumeLatencyAggregateUtilizationIncident）	事件	體積	批判的
卷延遲和聚合利用率警告閾值超出(ocumVolumeLatencyAggregateUtilizationWarning)	風險	體積	警告
卷延遲和節點效能容量使用臨界閾值突破（ocumVolumeLatencyNodePerfCapacityUsedIncident）	事件	體積	批判的
磁碟區延遲和節點效能容量使用警告閾值已突破(ocumVolumeLatencyNodePerfCapacityUsedWarning)	風險	體積	警告
已使用的磁碟區延遲和節點效能容量 - 超出接管臨界閾值(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	事件	體積	批判的
磁碟區延遲和節點效能容量使用情況 - 超出接管警告閾值(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	風險	體積	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
卷延遲和節點利用率臨界閾值被突破（ocumVolumeLatencyNodeUtilizationIncident）	事件	體積	批判的
磁碟區延遲和節點利用率警告閾值超出(ocumVolumeLatencyNodeUtilizationWarning)	風險	體積	警告

影響領域：安全

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
容量反勒索軟體監控已啟用（主動模式）（antiRansomwareVolumeStateEnabled）	事件	體積	資訊
大量反勒索軟體監控已停用（antiRansomwareVolumeStateDisabled）	風險	體積	警告
容量反勒索軟體監控已啟用（學習模式）（antiRansomwareVolumeStateDryrun）	事件	體積	資訊
大量反勒索軟體監控已暫停（學習模式）（antiRansomwareVolumeStateDryrunPaused）	風險	體積	警告
大量反勒索軟體監控已暫停（活動模式）（antiRansomwareVolumeStateEnablePaused）	風險	體積	警告
大量反勒索軟體監控正在停用（antiRansomwareVolumeStateDisableInProgress）	風險	體積	警告

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
發現勒索軟體活動（callHomeRansomwareActivitySeen）	事件	體積	批判的
適合反勒索軟體監控的磁碟區（學習模式）（ocumEvtVolumeArwCandidate）	事件	體積	資訊
適合反勒索軟體監控的磁碟區（主動模式）（ocumVolumeSuitedForActiveAntiRansomwareDetection）	風險	體積	警告
音量顯示吵雜的反勒索軟體警報（antiRansomwareFeatureNoisyVolume）	風險	體積	警告

影響領域：資料保護

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
磁碟區的本地快照保護不足（volumeLacksLocalProtectionWarning）	風險	體積	警告
卷的本地快照保護不足（volumeLacksLocalProtectionCleared）	風險	體積	警告

磁碟區移動狀態事件

磁碟區移動狀態事件會告訴您磁碟區移動的狀態，以便您可以監控潛在問題。事件按影響區域分組，包括事件和陷阱名稱、影響等級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
磁碟區移動狀態：正在進行中（不適用）	事件	體積	資訊

事件名稱（陷阱名稱）	影響等級	來源類型	嚴重程度
磁碟區移動狀態 - 失敗（ocumEvtVolumeMoveFailed）	風險	體積	錯誤
磁碟區移動狀態：已完成（不適用）	事件	體積	資訊
磁碟區移動 - 切換延遲（ocumEvtVolumeMoveCutoverDeferred）	風險	體積	警告

事件視窗和對話框的描述

事件會通知您環境中的任何問題。您可以使用活動管理庫存頁面和事件詳細資訊頁面來監控所有事件。您可以使用通知設定選項對話方塊來設定通知。您可以使用事件設定頁面來停用或啟用事件。

通知頁面

您可以設定 Unified Manager 伺服器，使其在產生事件或將事件指派給使用者時傳送通知。您也可以配置通知機制。例如，通知可以作為電子郵件或 SNMP 陷阱發送。

您必須具有應用程式管理員或儲存管理員角色。

電子郵件

此區域使您能夠配置以下警報通知的電子郵件設定：

- 寄件者地址

  指定發送警報通知的電子郵件地址。共用時，此值也可用作報告的寄件者地址。如果寄件者地址預先填寫了“ActiveIQUnifiedManager@localhost.com”，您應該將其變更為真實有效的電子郵件地址，以確保所有電子郵件通知都成功送達。

SMTP 伺服器

此區域可讓您設定下列 SMTP 伺服器設定：

- 主機名稱或 **IP** 位址

  指定 SMTP 主機伺服器的主機名，用於將警報通知傳送給指定的收件者。

- 使用者名稱

  指定 SMTP 使用者名稱。僅當 SMTP 伺服器中啟用 SMTPAUTH 時才需要 SMTP 使用者名稱。

- 密碼

指定 SMTP 密碼。僅當 SMTP 伺服器中啟用 SMTPAUTH 時才需要 SMTP 使用者名稱。

- 港口

  指定 SMTP 主機伺服器用於發送警報通知的連接埠。

  預設值為 25。

- 使用 **START/TLS**

  勾選此方塊可使用 TLS/SSL 協定（也稱為 start_tls 和 StartTLS）在 SMTP 伺服器和管理伺服器之間提供安全通訊。

- 使用 **SSL**

  勾選此方塊可使用 SSL 協定在 SMTP 伺服器和管理伺服器之間提供安全通訊。

SNMP

此區域可讓您設定以下 SNMP 陷阱設定：

- 版本

  根據您所需的安全性類型指定要使用的 SNMP 版本。選項包括版本 1、版本 3、帶有身份驗證的版本 3 和帶有身份驗證和加密的版本 3。預設值為版本 1。

- 陷阱目標主機

  指定接收管理伺服器傳送的 SNMP 陷阱的主機名稱或 IP 位址（IPv4 或 IPv6）。若要指定多個陷阱目標，請用逗號分隔每個主機。

  清單中所有主機的所有其他 SNMP 設定（例如「版本」和「出站連接埠」）必須相同。

- 出站陷阱端口

  指定 SNMP 伺服器透過其接收管理伺服器傳送的陷阱的連接埠。

  預設值為 162。

- 社區

  存取主機的社群字串。

- 引擎**ID**

  指定 SNMP 代理程式的唯一標識符，由管理伺服器自動產生。引擎 ID 適用於 SNMP 版本 3、具有身份驗證的 SNMP 版本 3 以及具有身份驗證和加密的 SNMP 版本 3。

- 使用者名稱

  指定 SNMP 使用者名稱。使用者名稱適用於 SNMP 版本 3、具有身份驗證的 SNMP 版本 3 以及具有身份驗證和加密的 SNMP 版本 3。

- 身份驗證協定

  指定用於驗證使用者的協定。協定選項包括 MD5 和 SHA。 MD5 是預設值。身份驗證協定適用於具有身份驗證的 SNMP 版本 3 和具有身份驗證和加密的 SNMP 版本 3。

- 認證密碼

  指定驗證使用者時使用的密碼。帶有身份驗證的 SNMP 版本 3 和帶有身份驗證和加密的 SNMP 版本 3 均提供身份驗證密碼。

- 隱私協議

  指定用於加密 SNMP 訊息的隱私協定。協定選項包括 AES 128 和 DES。預設值為 AES 128。具有身份驗證和加密功能的 SNMP 版本 3 提供隱私協定。

- 隱私密碼

  指定使用隱私協定時的密碼。具有身份驗證和加密功能的 SNMP 版本 3 提供隱私密碼。

有關 SNMP 物件和陷阱的更多信息，您可以下載"Active IQ Unified ManagerMIB"來自NetApp支援站點。

活動管理庫存頁面

事件管理庫存頁面可讓您查看目前事件及其屬性的清單。您可以執行確認、解決和指派事件等任務。您也可以為特定事件新增警報。

此頁面上的資訊每 5 分鐘自動刷新一次，以確保顯示最新的新事件。

過濾器組件

使您能夠自訂事件清單中顯示的資訊。您可以使用以下元件來最佳化顯示的事件清單：

- 查看選單以從預先定義的篩選器選擇清單中進行選擇。

  這包括所有活動（新的和已確認的）事件、活動效能事件、分配給我（登入使用者）的事件以及所有維護時段內產生的所有事件。

- 搜尋窗格可透過輸入完整或部分術語來最佳化事件清單。
- 篩選按鈕可啟動篩選器窗格，以便您可以從每個可用欄位和欄位屬性中進行選擇，以最佳化事件清單。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 分配給

  使您能夠選擇分配事件的使用者。當您將事件指派給使用者時，使用者名稱和指派事件的時間將會新增至所選事件的事件清單中。

  - 我

將事件指派給目前登入的使用者。

- 另一個用戶

  顯示「指派所有者」對話框，您可以透過該對話框將事件指派或重新指派給其他使用者。您也可以透過將所有權欄位留空來取消分配事件。

- 承認

  確認選定的事件。

  當您確認某個事件時，您的使用者名稱和確認該事件的時間將會加入到所選事件的事件清單中。當您確認某個事件時，您有責任管理該事件。

  您無法確認訊息事件。

- 標記為已解決

  使您能夠將事件狀態變更為已解決。

  當您解決某個事件時，您的使用者名稱和解決該事件的時間將會新增到所選事件的事件清單中。對事件採取糾正措施後，您必須將該事件標記為已解決。

- 新增警報

  顯示「新增警報」對話框，您可以在此為選定事件新增警報。

- 報告

  使您能夠將目前事件視圖的詳細資訊匯出到逗號分隔值 (.csv) 檔案或 PDF 文件。

- 顯示/隱藏列選擇器

  使您能夠選擇頁面上顯示的列並選擇它們的顯示順序。

事件列表

按觸發時間排序顯示所有事件的詳細資訊。

預設情況下，顯示所有活動事件視圖，以顯示前七天具有事件或風險影響等級的新事件和已確認事件。

- 觸發時間

  事件產生的時間。

- 嚴重性

  事件嚴重性：嚴重（ ），錯誤（ ），警告（ ）和資訊（ ）。

- 狀態

  事件狀態：新的、已確認的、已解決的或過時的。

- 影響程度

  事件影響等級：事件、風險、事件或升級。

- 影響區域

  事件影響區域：可用性、容量、效能、保護、配置或安全性。

- 姓名

  事件名稱。您可以選擇一個名稱來顯示該事件的事件詳細資訊頁面。

- 來源

  發生事件的物件的名稱。您可以選擇名稱來顯示該物件的健康狀況或效能詳細資訊頁面。

  當發生共享 QoS 政策違規時，此欄位中僅顯示消耗最多 IOPS 或 MB/s 的工作負載物件。使用此策略的其他工作負載顯示在事件詳細資訊頁面中。

- 來源類型

  與事件關聯的物件類型（例如，儲存虛擬機器、磁碟區或 Qtree）。

- 分配給

  分配了事件的用戶的姓名。

- 事件起源

  事件是否源自「Active IQ網站」或直接源自「Active IQ Unified Manager」。

- 註解名稱

  指派給儲存物件的註解的名稱。

- 筆記

  為事件新增的註釋數。

- 未結清天數

  自事件最初生成以來的天數。

- 指定時間

  自事件分配給用戶以來已經過去的時間。如果時間超過一周，則會顯示將事件指派給使用者的時間戳記。

- 致謝

  確認該事件的用戶的姓名。如果事件未被確認，則該欄位為空白。

- 確認時間

自事件被確認以來已經過去的時間。如果時間超過一周，則會顯示確認事件的時間戳記。

- 已解決

  解決該事件的用戶的姓名。如果事件尚未解決，則該欄位為空白。

- 解決時間

  自事件解決以來已經過去的時間。如果時間超過一周，則會顯示事件解決的時間戳記。

- 過時的時間

  事件狀態變為過時的時間。

活動詳情頁面

在事件詳情頁面中，您可以查看所選事件的詳細信息，例如事件嚴重性、影響程度、影響區域和事件來源。您也可以查看有關解決問題的可能補救措施的其他資訊。

- 活動名稱

  事件的名稱以及最後看到事件的時間。

  對於非績效事件，當事件處於「新」或「已確認」狀態時，最後看到的資訊是未知的，因此是隱藏的。

- 活動描述

  事件的簡要描述。

  在某些情況下，事件描述中會提供觸發事件的原因。

- 有爭議的組件

  對於動態效能事件，此部分顯示代表叢集的邏輯和實體元件的圖示。如果某個組件存在爭用，其圖示將被圈出並以紅色突出顯示。

  有關此處顯示的組件的描述，請參閱_集群組件以及它們為何會發生爭用_。

事件資訊、系統診斷和建議的操作部分在其他主題中描述。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 註釋圖示

  使您能夠新增或更新有關事件的註釋，並查看其他使用者留下的所有註釋。

操作選單

- 分配給我

將事件分配給您。

- 分配給其他人

  開啟「指派所有者」對話框，您可以將事件指派或重新指派給其他使用者。

  當您將事件指派給使用者時，使用者的姓名和指派事件的時間將會新增至所選事件的事件清單中。

  您也可以透過將所有權欄位留空來取消分配事件。

- 承認

  確認選定的事件，以便您不會繼續收到重複的警報通知。

  當您確認某個事件時，您的使用者名稱和確認該事件的時間將會加入所選事件的事件清單（確認人）中。當您確認某個事件時，您就承擔起管理該事件的責任。

- 標記為已解決

  使您能夠將事件狀態變更為"已解決"。

  當您解決某個事件時，您的使用者名稱和解決該事件的時間將會新增到所選事件的事件清單（解決者）中。對事件採取糾正措施後，您必須將該事件標記為已解決。

- 新增警報

  顯示「新增警報」對話框，您可以在此為選定事件新增警報。

活動資訊部分顯示的內容

您可以使用「事件詳細資料」頁面上的「事件資訊」部分查看有關選定事件的詳細信息，例如事件嚴重性、影響等級、影響區域和事件來源。

不適用於事件類型的欄位將被隱藏。您可以查看以下事件詳細資訊：

- 事件觸發時間

  事件產生的時間。

- 狀態

  事件狀態：新的、已確認的、已解決的或過時的。

- 過時的原因

  導致事件過時的操作，例如問題已修復。

- 活動時長

  對於活動（新的和已確認的）事件，這是偵測與上次分析事件之間的時間。對於過時的事件，這是偵測到事件和解決事件之間的時間。

所有效能事件都會顯示此字段，其他事件類型只有在解決或淘汰後才會顯示。

- 最後露面

  事件最後處於活躍狀態的日期和時間。

  對於效能事件，此值可能會比事件觸發時間更新，因為只要事件處於活動狀態，此欄位就會在每次新的效能資料收集後更新。對於其他類型的事件，當處於「新建」或「已確認」狀態時，此內容不會更新，因此該欄位被隱藏。

- 嚴重性

  事件嚴重性：嚴重（ ），錯誤（ ），警告（ ）和資訊（ ）。

- 影響程度

  事件影響等級：事件、風險、事件或升級。

- 影響區域

  事件影響區域：可用性、容量、效能、保護、配置或安全性。

- 來源

  發生事件的物件的名稱。

  在查看共享 QoS 策略事件的詳細資訊時，此欄位中最多列出三個消耗最多 IOPS 或 MBps 的工作負載物件。

  您可以按一下來源名稱連結來顯示該物件的健康狀況或效能詳細資訊頁面。

- 來源註解

  顯示與事件關聯的物件的註解名稱和值。

  僅針對叢集、SVM 和磁碟區上的執行狀況事件顯示此欄位。

- 來源組

  顯示受影響物件所屬的所有群組的名稱。

  僅針對叢集、SVM 和磁碟區上的執行狀況事件顯示此欄位。

- 來源類型

  與事件關聯的物件類型（例如，SVM、磁碟區或 Qtree）。

- 在集群上

  發生事件的叢集的名稱。

  您可以點擊群集名稱連結來顯示該群集的健康狀況或效能詳細資料頁面。

- 受影響對象數量

  受事件影響的物件的數量。

  您可以按一下物件連結來顯示庫存頁面，其中填入了目前受此事件影響的物件。

  僅針對效能事件顯示此欄位。

- 受影響的捲

  受此事件影響的捲的數量。

  僅針對節點或聚合上的效能事件顯示此欄位。

- 觸發策略

  發出事件的閾值策略的名稱。

  您可以將遊標懸停在策略名稱上以查看閾值策略的詳細資訊。對於自適應 QoS 策略，也會顯示定義的策略、區塊大小和分配類型（分配空間或使用空間）。

  僅針對效能事件顯示此欄位。

- 規則 **ID**

  對於Active IQ平台事件，這是觸發產生事件的規則的編號。

- 感謝

  確認事件的人員的姓名以及確認事件的時間。

- 已解決

  解決事件的人員的姓名以及解決事件的時間。

- 分配給

  被指派負責該活動的人員的姓名。

- 警報設定

  顯示有關警報的以下資訊：

  - 如果沒有與所選事件相關的警報，則會顯示*新增警報*連結。

    您可以透過點擊連結來開啟「新增警報」對話框。

  - 如果有一個警報與選定事件關聯，則會顯示警報名稱。

    您可以透過點擊連結開啟「編輯警報」對話框。

  - 如果有多個警報與選定事件關聯，則會顯示警報的數量。

您可以透過點擊連結開啟「警報設定」頁面來查看有關這些警報的更多詳細資訊。

已禁用的警報不會顯示。

- 最後通知已發送

  發送最新警報通知的日期和時間。

- 發送者

  用於傳送警報通知的機制：電子郵件或 SNMP 陷阱。

- 上一個腳本運行

  產生警報時執行的腳本的名稱。

“建議的操作”部分顯示的內容

事件詳細資訊頁面的建議操作部分提供了事件的可能原因並建議了一些操作，以便您可以嘗試自行解決該事件。建議的操作是根據事件類型或已突破的閾值類型自訂的。

此區域僅針對某些類型的事件顯示。

在某些情況下，頁面上會提供*幫助*鏈接，其中引用了許多建議操作的附加信息，包括執行特定操作的說明。某些操作可能涉及使用 Unified Manager、 ONTAP System Manager、 OnCommand Workflow Automation、 ONTAP CLI 指令或這些工具的組合。

您應該將此處建議的操作視為解決此事件的唯一指導。您為解決此事件所採取的措施應基於您的環境背景。

如果要更詳細地分析物件和事件，請按一下「分析工作負載」按鈕以顯示「工作負載分析」頁面。

Unified Manager 可以徹底診斷某些事件並提供單一解決方案。當可用時，這些解析度將顯示一個「修復」按鈕。按一下此按鈕可讓 Unified Manager 修復導致該事件的問題。

對於Active IQ平台事件，本部分可能包含指向NetApp知識庫文章（如果有）的鏈接，其中描述了問題和可能的解決方案。在沒有外部網路存取權限的網站中，知識庫文章的 PDF 會在本機開啟；該 PDF 是您手動下載至 Unified Manager 實例的規則檔案的一部分。

系統診斷部分顯示的內容

事件詳細資訊頁面的系統診斷部分提供的資訊可以幫助您診斷可能導致該事件的問題。

此區域僅針對某些事件顯示。

一些效能事件提供與已觸發的特定事件相關的圖表。通常這包括 IOPS 或 MBps 圖表和前十天的延遲圖表。透過這種方式排列，您可以看到當事件處於活動狀態時，哪些儲存元件對延遲的影響最大，或受到延遲的影響。

對於動態效能事件，顯示以下圖表：

- 工作負荷延遲 - 顯示爭用組件中排名靠前的受害者、霸凌者或鯊魚工作負荷的延遲歷史記錄。
- 工作負載活動 - 顯示有關爭用中的叢集元件的工作負載使用情況的詳細資訊。

- 資源活動 - 顯示爭用的叢集元件的歷史效能統計資料。

當某些群集組件存在爭用時，會顯示其他圖表。

其他事件簡要描述了系統對儲存物件執行的分析類型。在某些情況下，將會有一行或多行；每個已分析的元件都有一行，用於分析多個效能計數器的系統定義的效能策略。在這種情況下，診斷旁邊會顯示綠色或紅色圖標，以指示在該特定診斷中是否發現問題。

活動設定頁面

事件設定頁面顯示已停用的事件列表，並提供相關物件類型和事件嚴重性等資訊。您也可以執行全域停用或啟用事件等任務。

只有具有應用程式管理員或儲存管理員角色才可以存取此頁面。

命令按鈕

命令按鈕可讓您針對選定的事件執行下列任務：

- 禁用

  啟動「停用事件」對話框，您可以使用該對話框來停用事件。

- 使能夠

  啟用您先前選擇已停用的選定事件。

- 上傳規則

  啟動「上傳規則」對話框，使沒有外部網路存取權限的網站能夠手動將Active IQ規則檔案上傳到 Unified Manager。這些規則針對叢集AutoSupport訊息運行，以產生Active IQ平台定義的系統配置、佈線、最佳實踐和可用性事件。

- 訂閱 **EMS** 活動

  啟動「訂閱 EMS 事件」對話框，該對話框使您能夠訂閱從您正在監控的叢集接收特定的事件管理系統 (EMS) 事件。 EMS 收集有關在集群上發生的事件的資訊。當收到訂閱的 EMS 事件的通知時，將產生具有適當嚴重程度的 Unified Manager 事件。

清單視圖

清單檢視顯示（以表格形式）有關已停用事件的資訊。您可以使用列過濾器來自訂顯示的資料。

- 事件

  顯示已禁用事件的名稱。

- 嚴重性

  顯示事件的嚴重性。嚴重性可以是「嚴重」、「錯誤」、「警告」或「訊息」。

- 來源類型

顯示產生事件的來源類型。

停用事件對話框

「停用事件」對話方塊顯示您可以停用事件的事件類型清單。您可以根據特定的嚴重性或一組事件停用某種事件類型的事件。

您必須具有應用程式管理員或儲存管理員角色。

事件屬性區域

事件屬性區域指定下列事件屬性：

- 事件嚴重性

  使您能夠根據嚴重性類型選擇事件，嚴重性類型可以是「嚴重」、「錯誤」、「警告」或「訊息」。

- 事件名稱包含

  使您能夠過濾名稱包含指定字元的事件。

- 匹配事件

  顯示與您指定的事件嚴重性類型和文字字串相符的事件清單。

- 禁用事件

  顯示您選擇已停用的事件清單。

  事件的嚴重性也會與事件名稱一起顯示。

命令按鈕

命令按鈕可讓您針對選定的事件執行下列任務：

- 儲存並關閉

  停用事件類型並關閉對話方塊。

- 取消

  放棄更改並關閉對話框。

管理警報

您可以設定警報，以便在發生特定事件或特定嚴重性類型的事件時自動發送通知。您也可以將警報與觸發警報時執行的腳本關聯。

什麼是警報

雖然事件會持續發生，但只有當事件滿足指定的過濾條件時，Unified Manager 才會產生警報。您可以選擇應產生警報的事件 - 例如，當超過空間閾值或物件離線時。您也可以將警報與觸發警報時執行的腳本關聯。

篩選條件包括物件類別、名稱或事件嚴重性。

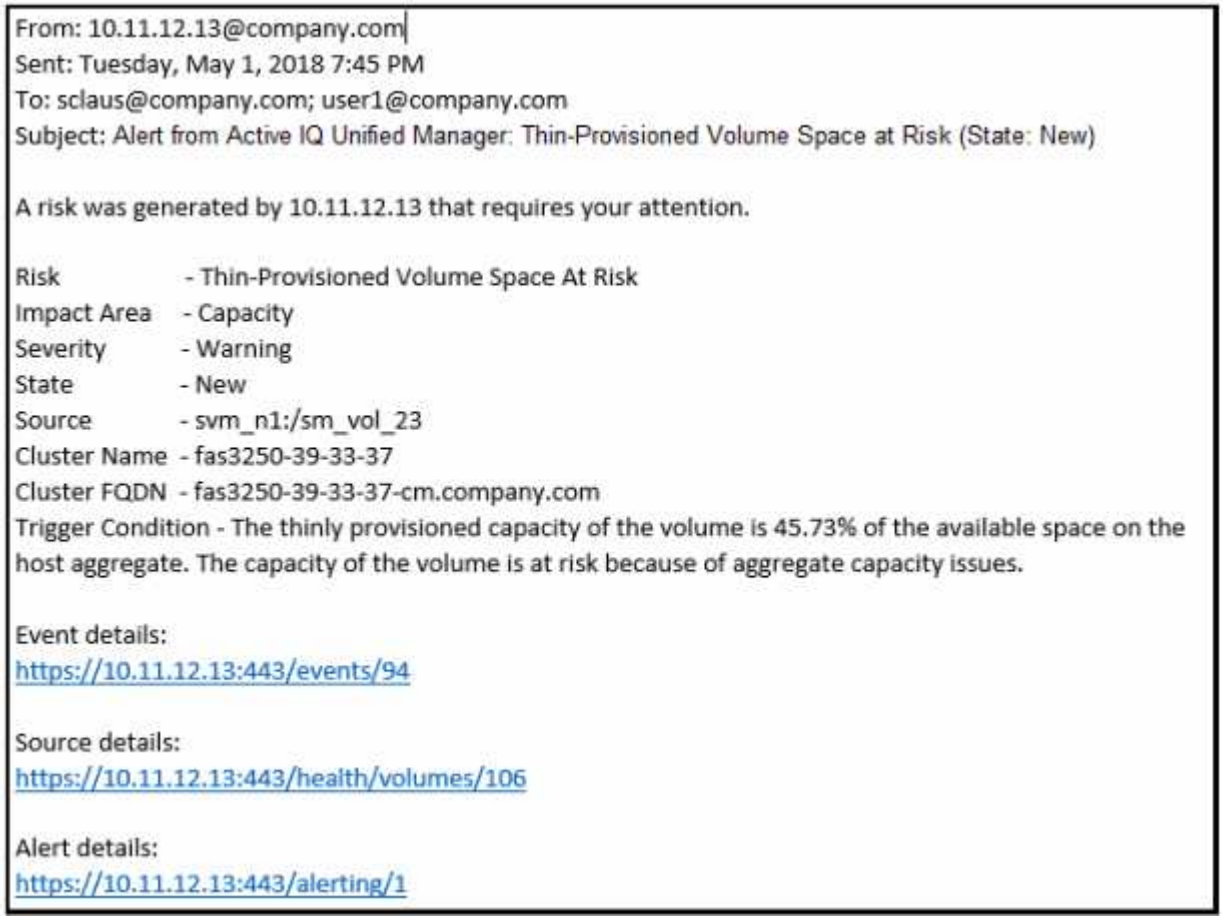
警報電子郵件包含哪些訊息

Unified Manager 警報電子郵件提供事件類型、事件嚴重性、導致事件發生的策略或閾值的名稱以及事件描述。電子郵件還為每個事件提供了超鏈接，使您可以在 UI 中查看該事件的詳細資訊頁面。

警報電子郵件將發送給所有已訂閱接收警報的使用者。

如果效能計數器或容量值在收集期間發生較大變化，則可能導致針對相同閾值策略同時觸發嚴重事件和警告事件。在這種情況下，您可能會收到一封針對警告事件的電子郵件和一封針對嚴重事件的電子郵件。這是因為 Unified Manager 允許您單獨訂閱以接收警告和嚴重閾值違規的警報。

警報電子郵件範例如下所示：


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

添加警報

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。您可以指定接收通知的頻率並將腳本與警報關聯。

開始之前

- 您必須設定通知設置，例如使用者電子郵件地址、SMTP 伺服器和 SNMP 陷阱主機，以便Active IQ Unified Manager伺服器能夠在產生事件時使用這些設定向使用者傳送通知。
- 您必須知道要觸發警報的資源和事件，以及要通知的使用者的使用者名稱或電子郵件地址。
- 如果您希望根據事件執行腳本，則必須使用腳本頁面將腳本新增至 Unified Manager。
- 您必須具有應用程式管理員或儲存管理員角色。

除了從警報設定頁面建立警報之外，您還可以在收到事件後直接從事件詳細資訊頁面建立警報，如此處所述。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在*警報設定*頁面中，按一下*新增*。
3. 在“新增警報”對話方塊中，按一下“名稱”，然後輸入警報的名稱和描述。
4. 按一下“資源”，然後選擇要包含在警報中或從警報中排除的資源。

   您可以透過在*名稱包含*欄位中指定文字字串來設定過濾器，以選擇一組資源。根據您指定的文字字串，可用資源清單僅顯示符合過濾規則的資源。您指定的文字字串區分大小寫。

   如果資源同時符合您指定的包含規則和排除規則，則排除規則優先於包含規則，並且不會針對與排除的資源相關的事件產生警報。

5. 按一下“事件”，然後根據事件名稱或事件嚴重性類型選擇要觸發警報的事件。

   若要選擇多個事件，請在選擇時按住 Ctrl 鍵。

6. 點選*操作*，選擇要通知的用戶，選擇通知頻率，選擇是否將 SNMP 陷阱傳送至陷阱接收器，並指派在產生警報時執行的腳本。

   如果您修改為使用者指定的電子郵件地址並重新開啟警報進行編輯，則「名稱」欄位將顯示為空白，因為修改後的電子郵件地址不再對應到先前選取的使用者。此外，如果您從「使用者」頁面修改了所選使用者的電子郵件地址，則所選使用者的修改後的電子郵件地址不會更新。

   您也可以選擇透過 SNMP 陷阱通知使用者。

7. 點選“儲存”。

新增警報的範例

此範例顯示如何建立滿足以下要求的警報：

- 警示名稱：HealthTest

- 資源：包括名稱包含“abc”的所有捲，並排除名稱包含“xyz”的所有捲
- 事件：包括所有重大健康事件
- 操作：包括“sample@domain.com”和“測試”腳本，並且每 15 分鐘通知一次用戶

在「新增警報」對話方塊中執行以下步驟：

1. 點選*姓名*，然後輸入*`HealthTest`* 在 警報名稱 欄位中。
2. 按一下“資源”，然後在“包含”標籤中，從下拉清單中選擇“磁碟區”。
   a. 進入*`abc`* 在「名稱包含」欄位中顯示名稱中包含「abc」的磁碟區。
   b. 選擇 **+[All Volumes whose name contains 'abc']** + 從可用資源區域，並將其移至選定資源區域。
   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”欄位中選擇“嚴重”。
4. 從符合事件區域選擇“所有關鍵事件”，並將其移至選定事件區域。
5. 點擊“操作”，然後輸入*`sample@domain.com`* 在「提醒這些使用者」欄位中。
6. 選擇*每 15 分鐘提醒一次*，每 15 分鐘通知一次使用者。

   您可以設定警報以在指定時間內重複向收件人發送通知。您應該確定事件通知對於警報生效的時間。
7. 在選擇要執行的腳本選單中，選擇*測試*腳本。
8. 點選“儲存”。

新增警報的指南

您可以根據資源（例如叢集、節點、聚合或磁碟區）以及特定嚴重性類型的事件新增警報。作為最佳實踐，您可以在新增物件所屬的叢集後為任何關鍵物件新增警報。

您可以根據以下指南和注意事項來建立警報，以有效管理您的系統：

- 警報描述

  您應該提供警報的描述，以便幫助您有效地追蹤警報。

- 資源

  您應該決定哪些實體或邏輯資源需要警報。您可以根據需要包含或排除資源。例如，如果您想要透過設定警報來密切監視您的聚合，則必須從資源清單中選擇所需的聚合。

  如果您選擇一個資源類別，例如 **+[All User or Group Quotas]** +，那麼您將收到該類別中所有物件的警報。

  > ⓘ 選擇叢集作為資源並不會自動選擇該叢集內的儲存物件。例如，如果您為所有叢集的所有關鍵事件建立警報，那麼您將只收到叢集關鍵事件的警報。您將不會收到有關節點、聚合等的關鍵事件的警報。

- 事件嚴重性

您應該決定指定嚴重性類型（嚴重、錯誤、警告）的事件是否應觸發警報，如果是，則應決定觸發哪種嚴重性類型。

- 精選活動

  如果您根據產生的事件類型新增警報，則應該決定哪些事件需要警報。

  如果您選擇事件嚴重性，但不選擇任何單一事件（如果您將「選定事件」列留空），那麼您將收到該類別中所有事件的警報。

- 行動

  您必須提供接收通知的使用者的使用者名稱和電子郵件地址。您也可以指定 SNMP 陷阱作為通知模式。您可以將腳本與警報關聯，以便在產生警報時執行它們。

- 通知頻率

  您可以設定警報以在指定時間內重複向收件人發送通知。您應該確定事件通知對於警報生效的時間。如果您希望重複發送事件通知直到事件已確認，則應確定重複發送通知的頻率。

- 執行腳本

  您可以將腳本與警報關聯起來。當警報產生時，您的腳本就會執行。

新增性能事件警報

您可以為單一效能事件設定警報，就像 Unified Manager 收到的任何其他事件一樣。此外，如果您希望平等對待所有效能事件並將電子郵件發送給同一個人，您可以建立警報，以便在觸發任何關鍵或警告效能事件時通知您。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

下面的範例展示如何為所有關鍵延遲、IOPS 和 MBps 事件建立事件。您可以使用相同的方法從所有效能計數器中選擇事件，以及所有警告事件。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在*警報設定*頁面中，按一下*新增*。
3. 在“新增警報”對話方塊中，按一下“名稱”，然後輸入警報的名稱和描述。
4. 不要在「資源」頁面上選擇任何資源。

   由於未選擇任何資源，因此警報將應用於收到這些事件的所有叢集、聚合、磁碟區等。

5. 按一下“事件”並執行以下操作：
   a. 在事件嚴重性清單中，選擇*嚴重*。
   b. 在事件名稱包含欄位中，輸入*`latency`* 然後按一下箭頭選擇所有符合的事件。

c. 在事件名稱包含欄位中，輸入*iops* 然後按一下箭頭選擇所有符合的事件。

d. 在事件名稱包含欄位中，輸入*mbps* 然後按一下箭頭選擇所有符合的事件。

6. 按一下“操作”，然後在“警告這些使用者”欄位中選擇將接收警報電子郵件的使用者的姓名。
7. 配置此頁面上的任何其他選項以發出 SNMP 陷阱和執行腳本。
8. 點選“儲存”。

測試警報

您可以測試警報以驗證您是否已正確配置它。當觸發事件時，會產生警報，並向配置的收件者發送警報電子郵件。您可以使用測試警報來驗證通知是否已發送以及您的腳本是否已執行。

開始之前

- 您必須設定通知設置，例如收件者的電子郵件地址、SMTP 伺服器和 SNMP 陷阱。

  當產生事件時，Unified Manager 伺服器可以使用這些設定向使用者傳送通知。

- 您必須指派一個腳本並將該腳本配置為在產生警報時執行。
- 您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在*警報設定*頁面中，選擇要測試的警報，然後按一下*測試*。

   測試警報電子郵件將會傳送到您在建立警報時指定的電子郵件地址。

啟用和停用已解決和已過時事件的警報

對於您已配置為發送警報的所有事件，當這些事件轉變至所有可用狀態時都會發送警報訊息：新建、已確認、已解決和過時。如果您不想在事件進入「已解決」和「過時」狀態時收到警報，您可以設定全域設定來抑制這些警報。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

預設情況下，當事件進入「已解決」和「過時」狀態時，不會發送警報。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在「警報設定」頁面中，使用「已解決和過時事件的警報」項目旁的滑桿控制執行下列其中一項操作：

到...	這樣做...
當事件解決或過時時停止發送警報	將滑桿控制項向左移動

到...	這樣做...
當事件解決或過時時開始發送警報	將滑桿控制項向右移動

排除災難復原目標磁碟區產生警報

配置磁碟區警報時，您可以在「警報」對話方塊中指定字串來識別一個磁碟區或一組磁碟區。但是，如果您已為 SVM 配置了災難恢復，則來源磁碟區和目標磁碟區具有相同的名稱，因此您將收到這兩個磁碟區的警報。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您可以透過排除具有目標 SVM 名稱的磁碟區來停用災難復原目標磁碟區的警報。這是可能的，因為磁碟區事件的識別碼包含 SVM 名稱和磁碟區名稱，格式為「<svm_name>:/<volume_name>」。

下面的範例顯示如何在主 SVM「vs1」上為磁碟區「vol1」建立警報，但排除在 SVM「vs1-dr」上同名磁碟區上產生警報。

在「新增警報」對話方塊中執行以下步驟：

步驟

1. 點擊“名稱”並輸入警報的名稱和描述。
2. 按一下“資源”，然後選擇“包括”標籤。
   a. 從下拉清單中選擇*Volume*，然後輸入*`vol1`* 在「名稱包含」欄位中顯示名稱中包含「vol1」的磁碟區。
   b. 選擇 **+[All Volumes whose name contains 'vol1']** + 從*可用資源*區域，並將其移至*選定資源*區域。
3. 選擇*Exclude*選項卡，選擇*Volume*，輸入*`vs1-dr`* 在 名稱包含 欄位中，然後按一下 新增。

   這將排除針對 SVM“vs1-dr”上的磁碟區“vol1”所產生的警報。
4. 按一下「事件」並選擇要套用於磁碟區的一個或多個事件。
5. 按一下“操作”，然後在“警告這些使用者”欄位中選擇將接收警報電子郵件的使用者的姓名。
6. 配置此頁面上的任何其他選項以發出 SNMP 陷阱和執行腳本，然後按一下*儲存*。

查看警報

您可以從警報設定頁面查看為各種事件建立的警報清單。您還可以查看警報屬性，例如警報描述、通知方法和頻率、觸發警報的事件、警報的電子郵件收件人以及受影響的資源，例如叢集、聚合和磁碟區。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

步

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。

   警報清單顯示在警報設定頁面中。

編輯警報

您可以編輯警報屬性，例如與警報關聯的資源、事件、收件者、通知選項、通知頻率和關聯腳本。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在*警報設定*頁面中，選擇要編輯的警報，然後按一下*編輯*。
3. 在「編輯警報」對話方塊中，根據需要編輯名稱、資源、事件和操作部分。

   您可以變更或刪除與警報相關的腳本。

4. 點選“儲存”。

刪除警報

當不再需要警報時，您可以刪除它。例如，當某個資源不再受 Unified Manager 監控時，您可以刪除為該資源建立的警報。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
2. 在*警報設定*頁面上，選擇要刪除的警報，然後按一下*刪除*。
3. 按一下“是”確認刪除請求。

警報視窗和對話框的描述

您應該使用「新增警報」對話方塊來設定警報以接收有關事件的通知。您也可以從警報設定頁面查看警報清單。

警報設定頁面

警報設定頁面顯示警報清單並提供有關警報名稱、狀態、通知方法和通知頻率的資訊。您也可以從此頁面新增、編輯、刪除、啟用或停用警報。

您必須具有應用程式管理員或儲存管理員角色。

命令按鈕

- 添加

  顯示「新增警報」對話框，您可以在此新增警報。

- 編輯

  顯示「編輯警報」對話框，您可以在此編輯選定的警報。

- 刪除

  刪除選定的警報。

- 使能夠

  啟用選定的警報來發送通知。

- 禁用

  當您想要暫時停止發送通知時，請停用所選警報。

- 測試

  測試選定的警報以驗證其新增或編輯後的配置。

- 已解決和過時事件的警報

  允許您在事件移至「已解決」或「過時」狀態時啟用或停用發送警報。這可以幫助用戶避免接收不必要的通知。

清單視圖

清單檢視以表格形式顯示有關所建立的警報的資訊。您可以使用列過濾器來自訂顯示的資料。您還可以選擇一個警報以在詳細資訊區域中查看有關它的更多資訊。

- 地位

  指定是否啟用警報（  ）或禁用（  ）。

- 警報

  顯示警報的名稱。

- 描述

  顯示警報的描述。

- 通知方式

  顯示為警報選擇的通知方法。您可以透過電子郵件或 SNMP 陷阱通知使用者。

- 通知頻率

指定管理伺服器持續發送通知的頻率（以分鐘為單位），直到事件被確認、解決或移至過時狀態。

詳細資訊區域

詳細資訊區域提供有關所選警報的更多資訊。

- 警報名稱

  顯示警報的名稱。

- 警報描述

  顯示警報的描述。

- 活動

  顯示您想要觸發警報的事件。

- 資源

  顯示您想要觸發警報的資源。

- 包括

  顯示您想要觸發警報的資源群組。

- 不包括

  顯示您不想觸發警報的資源群組。

- 通知方式

  顯示警報的通知方法。

- 通知頻率

  顯示管理伺服器繼續發送警報通知的頻率，直到事件被確認、解決或移至過時狀態。

- 腳本名稱

  顯示與所選警報關聯的腳本的名稱。當產生警報時執行此腳本。

- 電子郵件收件者

  顯示接收警報通知的使用者的電子郵件地址。

新增警報對話框

您可以建立警報，在產生特定事件時通知您，以便您可以快速解決問題並最大限度地減少對環境的影響。您可以為單一資源或一組資源以及特定嚴重性類型的事件建立警報。您也可以指定警報的通知方法和頻率。

您必須具有應用程式管理員或儲存管理員角色。

Name

此區域使您能夠指定警報的名稱和描述：

- 警報名稱

  使您能夠指定警報名稱。

- 警報描述

  使您能夠指定警報的描述。

資源

該區域可讓您選擇單一資源或根據要觸發警報的動態規則對資源進行分組。 _動態規則_是根據您指定的文字字串過濾的資源集。您可以從下拉清單中選擇資源類型來搜尋資源，也可以指定確切的資源名稱來顯示特定資源。

如果您從任何儲存物件詳細資料頁面建立警報，則該儲存物件將自動包含在警報中。

- 包括

  使您能夠包含想要觸發警報的資源。您可以指定一個文字字串來將與該字串相符的資源進行分組，並選擇該群組包含在警報中。例如，您可以將名稱包含“abc”字串的所有磁碟區分組。

- 排除

  使您能夠排除不想觸發警報的資源。例如，您可以排除名稱包含“xyz”字串的所有磁碟區。

  僅當您選擇特定資源類型的所有資源時才會顯示「排除」標籤：例如，<<All Volumes>>或者<<All Volumes whose name contains 'xyz'>>。

  如果資源同時符合您指定的包含規則和排除規則，則排除規則優先於包含規則，並且不會為事件產生警報。

活動

此區域使您能夠選擇要為其建立警報的事件。您可以根據特定嚴重性或一組事件建立事件警報。

若要選擇多個事件，您應該在選擇時按住 Ctrl 鍵。

- 事件嚴重性

  使您能夠根據嚴重性類型選擇事件，嚴重性類型可以是「嚴重」、「錯誤」或「警告」。

- 事件名稱包含

  使您能夠選擇名稱包含指定字元的事件。

行動

此區域使您能夠指定在觸發警報時要通知的使用者。您也可以指定通知方法和通知頻率。

- 提醒這些使用者

  使您能夠指定接收通知的使用者的電子郵件地址或使用者名稱。

  如果您修改為使用者指定的電子郵件地址並重新開啟警報進行編輯，則「名稱」欄位將顯示為空白，因為修改後的電子郵件地址不再對應到先前選取的使用者。此外，如果您從「使用者」頁面修改了所選使用者的電子郵件地址，則所選使用者的修改後的電子郵件地址不會更新。

- 通知頻率

  使您能夠指定管理伺服器發送通知的頻率，直到事件被確認、解決或移至過時狀態。

  您可以選擇以下通知方式：

  - 僅通知一次
  - 按指定頻率通知
  - 在指定時間範圍內以指定頻率通知

- 發出 **SNMP** 陷阱

  選擇此方塊可讓您指定是否應將 SNMP 陷阱傳送至全域設定的 SNMP 主機。

- 執行腳本

  使您能夠將自訂腳本新增至警報中。當產生警報時執行此腳本。

  > 如果您在使用者介面中沒有看到此功能，那是因為您的管理員已停用該功能。如果需要，您可以從*儲存管理* > *功能設定*啟用此功能。

命令按鈕

- 節省

  建立警報並關閉對話框。

- 取消

  放棄更改並關閉對話框。

編輯警報對話框

您可以編輯警報屬性，例如與警報關聯的資源、事件、腳本和通知選項。

Name

此區域使您能夠編輯警報的名稱和描述。

- 警報名稱

  使您能夠編輯警報名稱。

- 警報描述

  使您能夠指定警報的描述。

- 警戒狀態

  使您能夠啟用或停用警報。

資源

該區域可讓您選擇單一資源或根據要觸發警報的動態規則對資源進行分組。您可以從下拉清單中選擇資源類型來搜尋資源，也可以指定確切的資源名稱來顯示特定資源。

- 包括

  使您能夠包含想要觸發警報的資源。您可以指定一個文字字串來將與該字串相符的資源進行分組，並選擇該群組包含在警報中。例如，您可以將名稱包含「`vol0`」字串的所有磁碟區進行分組。

- 排除

  使您能夠排除不想觸發警報的資源。例如，您可以排除名稱包含「`xyz`」字串的所有磁碟區。

  僅當您選擇特定資源類型的所有資源時才會顯示「排除」標籤 - 例如，+[All Volumes] + 或 +[All Volumes whose name contains 'xyz'] +。

活動

此區域使您能夠選擇想要觸發警報的事件。您可以根據特定嚴重性或一組事件觸發事件警報。

- 事件嚴重性

  使您能夠根據嚴重性類型選擇事件，嚴重性類型可以是「嚴重」、「錯誤」或「警告」。

- 事件名稱包含

  使您能夠選擇名稱包含指定字元的事件。

行動

此區域使您能夠指定通知方法和通知頻率。

- 提醒這些使用者

  使您能夠編輯電子郵件地址或使用者名，或指定新的電子郵件地址或使用者名稱來接收通知。

- 通知頻率

使您能夠編輯管理伺服器發送通知的頻率，直到事件被確認、解決或移至過時狀態。

您可以選擇以下通知方式：

- 僅通知一次
- 按指定頻率通知
- 在指定時間範圍內以指定頻率通知

- 發出 **SNMP** 陷阱

  使您能夠指定是否應將 SNMP 陷阱傳送至全域設定的 SNMP 主機。

- 執行腳本

  使您能夠將腳本與警報關聯。當產生警報時執行此腳本。

命令按鈕

- 節省

  儲存變更並關閉對話框。

- 取消

  放棄更改並關閉對話框。

管理腳本

您可以使用腳本自動修改或更新 Unified Manager 中的多個儲存物件。該腳本與警報相關。當事件觸發警報時，腳本就會執行。您可以上傳自訂腳本並在產生警報時測試其執行情況。

預設情況下，將腳本上傳到 Unified Manager 並執行它們的功能是啟用的。如果您的組織因為安全原因不想允許此功能，您可以從*儲存管理*>*功能設定*停用此功能。

相關資訊

"啟用和停用上傳腳本的功能"

腳本如何與警報配合使用

您可以將警報與腳本關聯，以便在 Unified Manager 中針對某個事件發出警報時執行該腳本。您可以使用腳本來解決儲存物件的問題或識別哪些儲存物件正在產生事件。

當 Unified Manager 中某個事件產生警報時，會傳送警報電子郵件給指定的收件者。如果您已將警報與腳本關聯，則會執行該腳本。您可以從警報電子郵件中取得傳遞給腳本的參數的詳細資訊。

如果您建立了自訂腳本並將其與特定事件類型的警報關聯，則會根據該事件類型的自訂腳本採取行動，且「管理操作」頁面或 Unified Manager 儀表板上預設不提供「修正」操作。

該腳本使用以下參數來執行：

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

您可以在腳本中使用參數並收集相關事件資訊或修改儲存物件。

從腳本取得參數的範例

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

當產生警報時，將執行此腳本並顯示以下輸出：

```
-`eventID : 290`
-`eventSourceID : 4138`
```

新增腳本

您可以在 Unified Manager 中新增腳本，並將腳本與警報關聯。這些腳本在產生警報時會自動執行，並使您能夠取得有關產生事件的儲存物件的資訊。

開始之前

- 您必須已建立並儲存要新增至 Unified Manager 伺服器的腳本。
- 腳本支援的檔案格式包括 Perl、Shell、PowerShell、Python 和 `.bat`文件。

安裝 **Unified Manager** 的平台	支援的語言
VMware	Perl 和 Shell 腳本
Linux	Perl、Python 和 Shell 腳本
視窗	PowerShell、Perl、Python 和 .bat 腳本

  - 對於 Perl 腳本，必須在 Unified Manager 伺服器上安裝 Perl。對於 VMware 安裝，預設安裝 Perl 5，且

腳本僅支援 Perl 5 支援的內容。如果在 Unified Manager 之後安裝了 Perl，則必須重新啟動 Unified Manager 伺服器。

- 對於 PowerShell 腳本，必須在 Windows 伺服器上設定適當的 PowerShell 執行策略，以便執行腳本。

> 如果您的腳本建立日誌檔案來追蹤警報腳本進度，則必須確保日誌檔案不會在 Unified Manager 安裝資料夾內的任何位置建立。

- 您必須具有應用程式管理員或儲存管理員角色。

您可以上傳自訂腳本並收集有關警報的事件詳細資訊。

> 如果您在使用者介面中沒有看到此功能，那是因為您的管理員已停用該功能。如果需要，您可以從*儲存管理* > *功能設定*啟用此功能。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「腳本」。
2. 在*腳本*頁面中，按一下*新增*。
3. 在「新增腳本」對話方塊中，按一下「瀏覽」以選擇您的腳本檔案。
4. 輸入您選擇的腳本的描述。
5. 按一下“新增”。

相關資訊

"啟用和停用上傳腳本的功能"

刪除腳本

當腳本不再需要或有效時，您可以從 Unified Manager 中刪除該腳本。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 該腳本不得與警報關聯。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「腳本」。
2. 在「腳本」頁面中，選擇要刪除的腳本，然後按一下「刪除」。
3. 在「警告」對話方塊中，按一下「是」確認刪除。

測試腳本執行

當儲存物件產生警報時，您可以驗證腳本是否正確執行。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已將支援的文件格式的腳本上傳至 Unified Manager。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「腳本」。
2. 在*Scripts*頁面中，新增您的測試腳本。
3. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
4. 在「警報設定」頁面中，執行下列其中一項操作：

到...	這樣做...
添加警報	a. 按一下“新增”。 b. 在「操作」部分，將警報與您的測試腳本關聯。
編輯警報	a. 選擇一個警報，然後按一下“編輯”。 b. 在「操作」部分，將警報與您的測試腳本關聯。

5. 點選“儲存”。
6. 在*警報設定*頁面中，選擇您新增或修改的警報，然後按一下*測試*。

   該腳本使用“-test”參數執行，並將通知警報發送到建立警報時指定的電子郵件地址。

支援的 **Unified Manager CLI** 命令

身為儲存管理員，您可以使用 CLI 指令對儲存物件執行查詢；例如，對叢集、聚合、磁碟區、qtree 和 LUN 執行查詢。您可以使用 CLI 指令查詢 Unified Manager 內部資料庫和ONTAP資料庫。您也可以在操作開始或結束時執行的腳本中使用 CLI 命令，或在觸發警報時執行的腳本。

所有命令必須以命令開頭 `um cli login`以及用於身份驗證的有效使用者名稱和密碼。

若要執行 *um run* 命令，請確保您的帳戶具有 *console* 應用程式存取權限。

CLI 命令	描述	輸出
`um cli login -u <username> [-p <password>]`	登入 CLI。出於安全考慮，您應該只在“-u”選項後輸入使用者名稱。以這種方式使用時，系統將提示您輸入密碼，並且密碼不會被捕獲在歷史記錄或進程表中。會話登入後三小時過期，之後使用者必須再次登入。	顯示相應的訊息。
`um cli logout`	退出 CLI。	顯示相應的訊息。
`um help`	顯示所有第一級子命令。	顯示所有第一級子命令。

CLI 命令	描述	輸出
`um run cmd [ -t <timeout> ] <cluster> <command>`	在一個或多個主機上運行命令的最簡單方法。主要用於警報腳本以取得或執行對ONTAP 的操作。可選的超時參數設定在客戶端完成命令的最大時間限制（以秒為單位）。預設值為 0（永遠等待）。	從ONTAP收到。
`um run query <sql command>`	執行 SQL 查詢。只允許從資料庫讀取的查詢。不支援任何更新、插入或刪除操作。	結果以表格顯示。如果傳回空集，或有任何語法錯誤或錯誤要求，則會顯示對應的錯誤訊息。
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	將資料來源新增至託管儲存系統清單。資料來源描述如何建立與儲存系統的連線。新增資料來源時必須指定選項 -u（使用者名稱）和 -P（密碼）。選項 -t（協定）指定用於與叢集通訊的協定（http 或 https ）。如果未指定協議，則將嘗試兩種協議。選項 -p（連接埠）指定用於與叢集通訊的連接埠。如果未指定端口，則將嘗試相應協定的預設值。此命令只能由儲存管理員執行。	提示使用者接受證書並列印相應的訊息。
`um datasource list [ <datasource-id>]`	顯示託管儲存系統的資料來源。	以表格形式顯示以下值： `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message` 。
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	修改一個或多個資料來源選項。只能由儲存管理員執行。	顯示相應的訊息。
`um datasource remove <datasource-id>`	從 Unified Manager 中刪除資料來源（叢集）。	顯示相應的訊息。
`um option list [ <option> .. ]`	列出可以使用 set 指令配置的所有選項。	以表格形式顯示以下值： `Name, Value, Default Value, and Requires Restart.`

CLI 命令	描述	輸出
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	設定一個或多個選項。此命令只能由儲存管理員執行。	顯示相應的訊息。
`um version`	顯示 Unified Manager 軟體版本。	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	列出按指定物件篩選後的 LUN。 -q 適用於所有指令，不顯示標題。 ObjectType 可以是 lun、qtree 、cluster、volume、quota 或 svm。 例如： **`um lun list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。此指令列出了叢集內 ID 為 1 的所有 LUN。	以表格形式顯示以下值： `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	依指定物件過濾後列出儲存虛擬機器。 ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。 例如： **`um svm list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。此指令列出了叢集內 ID 為 1 的所有儲存虛擬機器。	以表格形式顯示以下值： `Name and Cluster ID.`

CLI 命令	描述	輸出
`um qtree list [-q] [ -ObjectType <object-id>]`	列出按指定物件過濾後的 qtree。 -q 適用於所有指令，不顯示標題。 ObjectType 可以是 lun、qtree 、cluster、volume、quota 或 svm。 例如： **`um qtree list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。該指令列出了叢集內 ID 為 1 的所有 qtree。	以表格形式顯示以下值： `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	列出按指定物件過濾後的磁碟。 ObjectType 可以是磁碟、聚合、節點或叢集。 例如： **`um disk list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。該指令列出了叢集內 ID 為 1 的所有磁碟。	以表格形式顯示以下值 `ObjectType and object-id`。
`um cluster list [-q] [-ObjectType <object-id>]`	列出根據指定物件進行過濾後的集群。 ObjectType 可以是磁碟、aggr、節點、叢集、lun、qtree、磁碟區、配額或 svm。 例如： **`um cluster list -aggr 1`** 在此範例中，「-aggr」是 objectType，「1」是 objectId。此指令列出了 ID 為 1 的聚合所屬的群集。	以表格形式顯示以下值： `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key` 。

CLI 命令	描述	輸出
`um cluster node list [-q] [-ObjectType <object-id>]`	根據指定物件進行過濾後列出叢集節點。 ObjectType 可以是磁碟、聚合、節點或叢集。 例如： **`um cluster node list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。該指令列出了叢集內 ID 為 1 的所有節點。	以表格形式顯示以下值 `Name and Cluster ID`。
`um volume list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的磁碟區。 ObjectType 可以是 lun、qtree、cluster、volume、quota、svm 或 aggregate。 例如： **`um volume list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。此指令列出了集群內 ID 為 1 的所有磁碟區。	以表格形式顯示以下值 `Volume ID and Volume Name`。
`um quota user list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的配額使用者。 ObjectType 可以是 qtree、cluster、volume、quota 或 svm。 例如： **`um quota user list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。此指令列出了叢集內 ID 為 1 的所有配額使用者。	以表格形式顯示以下值 `ID, Name, SID and Email`。

CLI 命令	描述	輸出
`um aggr list [-q] [-ObjectType <object-id>]`	列出按指定物件過濾後的聚合。ObjectType 可以是磁碟、聚合、節點、叢集或磁碟區。 例如： **`um aggr list -cluster 1`** 在這個範例中，「-cluster」是 objectType，「1」是 objectId。該指令列出了叢集中 ID 為 1 的所有聚合。	以表格形式顯示以下值 `Aggr ID, and Aggr Name`。
`um event ack <event-ids>`	確認一個或多個事件。	顯示相應的訊息。
`um event resolve <event-ids>`	解決一個或多個事件。	顯示相應的訊息。
`um event assign -u <username> <event-id>`	將事件分配給使用者。	顯示相應的訊息。
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	列出系統或使用者產生的事件。根據來源、狀態和 ID 過濾事件。	以表格形式顯示以下值 `Source, Source type, Name, Severity, State, User and Timestamp`。
`um backup restore -f <backup_file_path_and_name>`	使用 .7z 檔案還原 MySQL 資料庫備份。	顯示相應的訊息。

腳本視窗和對話框的描述

腳本頁面可讓您將腳本新增至 Unified Manager。

腳本頁面

透過「腳本」頁面，您可以將自訂腳本新增至 Unified Manager。您可以將這些腳本與警報關聯起來，以實現儲存物件的自動重新配置。

腳本頁面可讓您從 Unified Manager 新增或刪除腳本。

命令按鈕

- 添加

  顯示「新增腳本」對話框，您可以在其中新增腳本。

- 刪除

  刪除選定的腳本。

清單視圖

清單檢視以表格形式顯示您新增至 Unified Manager 的腳本。

- 姓名

  顯示腳本的名稱。

- 描述

  顯示腳本的描述。

新增腳本對話框

透過「新增腳本」對話框，您可以將腳本新增至 Unified Manager。您可以使用腳本配置警報，以自動解決為儲存物件產生的事件。

您必須具有應用程式管理員或儲存管理員角色。

- 選擇腳本檔案

  使您能夠選擇警報的腳本。

- 描述

  使您能夠指定腳本的描述。