



Active IQ Unified Manager 文檔

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

Active IQ Unified Manager文檔	1
發行說明	2
開始	3
VMware 安裝快速入門說明	3
系統需求	3
安裝Active IQ Unified Manager	3
Linux 安裝的快速入門說明	4
系統需求	4
安裝Active IQ Unified Manager	4
Windows 安裝快速入門說明	5
系統需求	5
安裝Active IQ Unified Manager	5
在 VMware vSphere 系統上安裝 Unified Manager	7
Active IQ Unified Manager簡介	7
Unified Manager 伺服器的功能	7
安裝順序概述	7
安裝 Unified Manager 的要求	8
虛擬基礎架構和硬體系統需求	8
VMware 軟體和安裝要求	9
支援的瀏覽器	10
協定和連接埠要求	10
完成工作表	13
安裝、升級和刪除 Unified Manager 軟體	14
部署流程概述	15
部署 Unified Manager	15
升級 Unified Manager	19
重新啟動 Unified Manager 虛擬機	21
刪除 Unified Manager	21
在 Linux 系統上安裝 Unified Manager	23
Active IQ Unified Manager簡介	23
Unified Manager 伺服器的功能	23
安裝順序概述	23
安裝 Unified Manager 的要求	24
虛擬基礎架構和硬體系統需求	24
Linux 軟體和安裝需求	25
支援的瀏覽器	27
協定和連接埠要求	28
完成工作表	30
安裝、升級和刪除 Unified Manager 軟體	32

安裝過程概述	32
設定所需的軟體儲存庫	33
NFS 和 CIFS 共享上的 SELinux 要求	35
在 Linux 系統上安裝 Unified Manager	37
在 Red Hat Enterprise Linux 上升級 Union Manager	43
安裝 Unified Manager 後升級第三方產品	48
重新啟動 Unified Manager	49
刪除 Unified Manager	49
刪除自訂 umadmin 使用者和維護群組	50
在 Windows 系統上安裝 Unified Manager	51
Active IQ Unified Manager 簡介	51
Unified Manager 伺服器的功能	51
安裝順序概述	51
安裝 Unified Manager 的要求	52
虛擬基礎架構和硬體系統需求	52
Windows 軟體和安裝要求	53
支援的瀏覽器	55
協定和連接埠要求	55
完成工作表	57
安裝、升級和刪除 Unified Manager 軟體	59
安裝過程概述	59
在 Windows 上安裝 Unified Manager	60
更改 JBoss 密碼	63
Unified Manager 版本支援的升級路徑	64
升級 Unified Manager	64
升級第三方產品	66
卸載第三方產品	66
重新啟動 Unified Manager	67
解除安裝 Unified Manager	68
執行配置和管理任務	69
配置 Active IQ Unified Manager	69
配置序列概述	69
存取 Unified Manager Web UI	69
執行 Unified Manager Web UI 的初始設置	70
新增集群	72
配置 Unified Manager 以發送警報通知	74
更改本機用戶密碼	81
設定會話不活動逾時	82
透過 CLI 設定會話逾時	82
更改 Unified Manager 主機名	83
啟用和停用基於策略的儲存管理	87

設定 Unified Manager 備份	88
管理功能設定	88
啟用基於策略的儲存管理	88
啟用 API 網關	89
指定不活動逾時	89
啟用Active IQ入口網站事件	89
啟用和停用安全設定以實現合規性	90
啟用和停用腳本上傳	90
新增登入橫幅	91
使用維護控制台	91
維護控制台提供哪些功能	91
維護用戶做什麼	91
診斷使用者功能	92
存取維護控制台	92
使用 vSphere VM 控制台存取維護控制台	93
維護控制台選單	93
在 Windows 上變更維護使用者密碼	98
在 Linux 系統上變更 umadmin 密碼	98
更改 Unified Manager 用於 HTTP 和 HTTPS 協定的端口	99
新增網路介面	99
向 Unified Manager 資料庫目錄新增磁碟空間	100
管理用戶訪問	103
新增用戶	103
編輯用戶設定	105
查看用戶	105
刪除使用者或群組	105
什麼是 RBAC	106
基於角色的存取控制的作用	106
使用者類型的定義	106
使用者角色的定義	107
Unified Manager 使用者角色和功能	108
管理 SAML 身份驗證設定	109
身份提供者要求	109
啟用 SAML 身份驗證	110
更改用於 SAML 身份驗證的身份提供者	111
Unified Manager 安全性憑證變更後更新 SAML 驗證設定	112
禁用 SAML 身份驗證	113
從維護控制台停用 SAML 驗證	114
SAML 身份驗證頁面	114
管理身份驗證	115
編輯身份驗證伺服器	115

刪除身份驗證伺服器	115
使用 Active Directory 或 OpenLDAP 進行驗證	116
審計日誌	116
遠端身份驗證頁面	118
管理安全證書	122
查看HTTPS安全證書	122
下載 HTTPS 憑證簽署請求	122
安裝 CA 簽署並傳回的 HTTPS 憑證	122
安裝使用外部工具產生的 HTTPS 憑證	123
證書管理的頁面描述	125
監視和管理存儲	128
Active IQ Unified Manager簡介	128
Active IQ Unified Manager健康監控簡介	128
Active IQ Unified Manager效能監控簡介	129
使用 Unified Manager REST API	130
Unified Manager 伺服器的功能	130
了解使用者介面	131
典型的視窗佈局	131
視窗佈局自訂	132
使用 Unified Manager 協助	133
為您最喜歡的幫助主題添加書籤	133
搜尋儲存對象	133
將儲存資料匯出為報告	135
過濾庫存頁面內容	136
從通知鈴查看活動事件	137
從儀表板監控和管理集群	137
儀表板頁面	138
直接從 Unified Manager 管理ONTAP問題或功能	141
管理集群	146
集群發現過程的工作原理	146
查看監控叢集列表	147
新增集群	147
編輯集群	149
刪除叢集	150
重新發現集群	151
監控 VMware 虛擬基礎架構	151
不支援的內容	153
檢視並新增 vCenter Server	154
移除 vCenter Server	155
監控虛擬機	156
查看災難復原設定中的虛擬基礎架構	157

預配和管理工作負載	159
工作負載概述	160
性能服務水平	165
管理儲存效率策略	170
管理和監控MetroCluster配置	172
切換和切回期間的捲行為	172
透過 FC 配置的MetroCluster的叢集連線狀態定義	174
MetroCluster over FC 的資料鏡像狀態定義	175
監控MetroCluster配置	176
監控MetroCluster複製	178
管理配額	179
什麼是配額限制	179
查看使用者和使用者群組配額	179
建立規則以產生電子郵件地址	180
為使用者和使用者群組配額建立電子郵件通知格式	180
編輯使用者和群組配額電子郵件地址	181
詳細了解配額	181
配額對話框的說明	182
故障排除	185
向 Unified Manager 資料庫目錄新增磁碟空間	185
修改效能統計收集間隔	188
更改 Unified Manager 保留事件和效能資料的時間長度	189
未知的身份驗證錯誤	190
未找到用戶	190
使用其他驗證服務新增 LDAP 的問題	190
Windows 系統上的NetApp可管理性 SDK 日誌輪替問題	191
管理事件和警報	192
管理活動	192
Active IQ平台事件是什麼	192
什麼是事件管理系統事件	192
收到事件時會發生什麼	197
查看活動和活動詳情	198
查看未指派的事件	199
確認並解決事件	199
將事件指派給特定用戶	200
禁用不需要的事件	201
使用 Unified Manager 自動修復功能解決問題	201
啟用並停用Active IQ事件報告	202
上傳新的Active IQ規則文件	203
Active IQ平台事件是如何產生的	203
解決Active IQ平台事件	204

配置事件保留設定	205
Unified Manager 維護視窗是什麼	205
管理主機系統資源事件	207
了解更多活動信息	208
事件和嚴重性類型列表	212
事件視窗和對話框的描述	263
管理警報	274
什麼是警報	275
警報電子郵件包含哪些訊息	275
添加警報	276
新增性能事件警報	278
測試警報	279
啟用和停用已解決和已過時事件的警報	279
排除災難復原目標磁碟區產生警報	280
查看警報	280
編輯警報	281
刪除警報	281
警報視窗和對話框的描述	281
管理腳本	287
腳本如何與警報配合使用	287
新增腳本	288
刪除腳本	289
測試腳本執行	289
支援的 Unified Manager CLI 命令	290
腳本視窗和對話框的描述	295
監控和管理叢集效能	297
Active IQ Unified Manager效能監控簡介	297
Unified Manager 效能監控功能	297
用於管理儲存系統效能的 Unified Manager 介面	298
叢集配置和效能資料收集活動	298
什麼是資料連續性收集週期	299
時間戳在收集的資料和事件中意味著什麼	300
在 Unified Manager GUI 中導覽效能工作流程	300
登入使用者介面	300
圖形介面和導航路徑	301
搜尋儲存對象	306
過濾庫存頁面內容	307
從儀表板監控叢集效能	308
了解儀表板上的性能面板	309
效能橫幅訊息和說明	309
修改效能統計收集間隔	310

使用工作負載分析器排除工作負載故障	310
工作負載分析器顯示哪些數據	311
我什麼時候應該使用工作負載分析器	312
使用工作負載分析器	312
從效能叢集登入頁面監控叢集效能	313
了解性能集群登陸頁面	313
性能集群登陸頁面	314
使用「效能清單」頁面監控效能	317
查看所有儲存物件的效能清單頁面	318
優化績效清單頁面內容	323
了解 Unified Manager 將資料分層到雲端的建議	325
使用效能資源管理器頁面監視效能	326
了解根對象	326
應用篩選來減少網格中相關物件的列表	326
指定相關對象的時間範圍	326
定義用於比較圖表的相關物件列表	328
了解計數器圖表	329
效能計數器圖表的類型	330
選擇要顯示的效能圖表	331
展開計數器圖表窗格	332
將計數器圖表焦點變更為較短的時間段	332
在事件時間軸中查看事件詳細信息	333
計數器圖表縮放視圖	333
按集群組件查看卷延遲	335
按協定查看 SVM IOPS 流量	336
查看捲和 LUN 延遲圖表以驗證效能保證	336
查看所有 SAN 陣列叢集的效能	337
根據僅駐留在本機節點上的工作負載查看節點 IOPS	337
物件登陸頁的元件	338
使用 QoS 策略群組資訊管理效能	343
儲存 QoS 如何控制工作負載吞吐量	343
查看所有叢集上可用的所有 QoS 策略群組	344
查看同一 QoS 策略群組中的磁碟區或 LUN	344
查看應用於特定磁碟區或 LUN 的 QoS 原則群組設置	345
查看效能圖表以比較同一 QoS 策略群組中的磁碟區或 LUN	345
不同類型的 QoS 策略如何在吞吐量圖表中顯示	346
在效能資源管理器中查看工作負載 QoS 最小和最大設置	347
使用效能容量和可用 IOPS 資訊管理效能	348
所用性能容量	348
性能容量使用值的意義	349
可用的 IOPS 是什麼	350

查看節點和聚合效能容量使用值	351
查看節點並聚合可用 IOPS 值	352
查看效能容量計數器圖表以識別問題	353
效能容量使用效能閾值條件	354
使用效能容量使用計數器來管理效能	355
了解並使用節點故障轉移規劃頁面	355
使用節點故障轉移計劃頁面確定糾正措施	355
節點故障轉移計劃頁面的元件	356
將閾值策略與節點故障轉移計劃頁面結合使用	357
使用效能容量使用明細圖表進行故障轉移規劃	357
收集數據並監控工作負載效能	359
Unified Manager 監控的工作負載類型	359
工作負載效能測量值	360
預期的表現範圍是多少	361
延遲預測如何用於效能分析	362
Unified Manager 如何使用工作負載延遲來識別效能問題	363
叢集操作如何影響工作負載延遲	363
MetroCluster配置的效能監控	364
了解性能事件和警報	365
性能事件的來源	365
效能事件嚴重性類型	366
Unified Manager 偵測到的設定更改	366
系統定義的效能閾值策略的類型	367
效能事件分析和通知	369
Unified Manager 如何決定事件對效能的影響	371
集群組件及其爭用的原因	371
效能事件中涉及的工作負載的角色	373
管理績效閾值	373
使用者定義的效能閾值策略如何運作	374
當違反績效閾值策略時會發生什麼	376
可以使用閾值追蹤哪些效能計數器	376
哪些物件和計數器可以組合使用閾值策略	378
建立使用者定義的效能閾值策略	378
為儲存物件指派效能閾值策略	379
查看效能閾值策略	380
編輯使用者定義的效能閾值策略	381
從儲存物件中刪除效能閾值策略	381
當效能閾值策略改變時會發生什麼	382
當物件移動時效能閾值策略會發生什麼變化	382
分析效能事件	383
顯示有關性能事件的信息	383

根據使用者定義的效能閾值分析事件	384
根據系統定義的效能閾值分析事件	385
根據動態效能閾值分析事件	390
解決效能事件	396
確認延遲在預期範圍內	396
審查配置變更對工作負載效能的影響	396
從客戶端提高工作負載效能的選項	396
檢查客戶端或網路問題	397
驗證 QoS 策略群組中的其他磁碟區是否具有異常高的活動	397
行動邏輯介面 (LIF)	397
在不太繁忙的時間運行儲存效率操作	398
新增磁碟並重新分配數據	399
在節點上啟用快閃記憶體如何提高工作負載效能	399
在儲存聚合上啟用 Flash Pool 可以如何提高工作負載效能	399
MetroCluster配置健康檢查	400
MetroCluster配置驗證	400
將工作負載移至不同的聚合	400
將工作負載移至其他節點	402
將工作負載移動到不同節點上的聚合	403
將工作負載移至不同 HA 對中的節點	404
將工作負載移至不同 HA 對中的另一個節點	406
使用 QoS 策略設定來優先處理此節點上的工作	407
刪除非活動捲和 LUN	408
新增磁碟並執行聚合佈局重建	408
在 Unified Manager 伺服器 and 外部資料提供者之間建立連接	409
可以傳送到外部伺服器的效能數據	409
設定 Graphite 以從 Unified Manager 接收效能數據	410
設定從 Unified Manager 伺服器到外部資料提供者的連接	410
監視和管理集群健康狀況	413
Active IQ Unified Manager健康監控簡介	413
物理和邏輯容量	413
容量測量單位	413
Unified Manager 健康監控功能	414
用於管理儲存系統健康狀況的 Unified Manager 介面	415
管理和監控叢集和叢集物件健康狀況	415
了解集群監控	415
查看集群清單及詳情	417
檢查MetroCluster配置中叢集的運作狀況	417
查看所有 SAN 陣列叢集的健康和容量狀態	419
查看節點列表及詳情	420
產生合約續約的硬體清單報告	420

查看儲存虛擬機器列表和詳細信息	421
查看匯總列表和詳細信息	421
查看FabricPool容量資訊	422
查看儲存池詳細信息	423
查看卷冊列表和詳細信息	424
查看有關 NFS 共享的詳細信息	424
查看有關 SMB/CIFS 共享的詳細信息	425
查看 Snapshot 副本列表	426
刪除 Snapshot 副本	426
計算 Snapshot 副本的可回收空間	427
集群物件視窗和對話框的描述	428
常見的 Unified Manager 運作狀況工作流程與任務	428
監控和排除數據可用性故障	429
解決容量問題	435
管理健康閾值	436
管理叢集安全目標	440
管理備份和復原作業	450
管理腳本	464
管理和監控群組	467
使用註釋確定儲存物件事件的優先權	475
透過 Web UI 和維護控制台發送支援包	483
與多個工作流程相關的任務和訊息	489
保護和恢復數據	542
建立、監控和排除保護關係故障	542
SnapMirror保護類型	542
在 Unified Manager 中設定保護關係	543
執行保護關係故障轉移和故障回復	546
解決保護作業失敗	549
解決滯後問題	552
管理和監控保護關係	553
查看卷宗保護狀態	554
查看卷宗保護關係	555
監控一致性組關係中的 LUN	556
從「Health: All Volumes」檢視建立SnapVault保護關係	557
從磁碟區/運作狀況詳細資料頁面建立SnapVault保護關係	558
從「Health: All Volumes」檢視建立SnapMirror保護關係	558
從磁碟區/運行狀況詳細資料頁面建立SnapMirror保護關係	559
創建具有版本靈活複製的SnapMirror關係	561
使用備份選項建立具有版本靈活複製的SnapMirror關係	561
配置目標效率設定	562
創建SnapMirror和SnapVault計劃	563

建立級聯或扇出關係，以擴展現有保護關係的保護	563
從卷關係頁面編輯保護關係	564
從卷/健康詳情頁面編輯保護關係	565
創建SnapMirror策略以最大程度提高傳輸效率	565
創建SnapVault策略以最大程度提高傳輸效率	566
從卷宗關係頁面中止活動資料保護傳輸	566
從卷/健康詳情頁面中止活動資料保護傳輸	567
從卷關係頁面停止保護關係	568
從卷/健康詳情頁暫停保護關係	568
從卷關係頁面斷開SnapMirror關係	569
從卷關係頁面中刪除保護關係	569
從卷關係頁面恢復靜止關係上的計劃傳輸	570
從卷/健康詳情頁面恢復已暫停關係的預定傳輸	570
從磁碟區關係頁面初始化或更新保護關係	571
從卷/健康詳情頁面初始化或更新保護關係	572
從磁碟區關係頁面重新同步保護關係	573
從「卷關係」頁面反向保護關係	574
使用捲和卷/健康詳細資料頁面恢復數據	574
什麼是資源池	575
建立資源池	576
編輯資源池	576
查看資源池清單	577
新增資源池成員	577
從資源池移除聚合	577
刪除資源池	578
監控儲存虛擬機器災難復原保護關係	578
了解儲存虛擬機器關聯	580
支援儲存服務的 SVM 和資源池需求	582
哪些工作	583
監控作業	583
查看職位詳情	583
中止作業	583
重試失敗的保護作業	584
保護關係視窗和對話框的描述	584
產生自訂報告	624
統一管理器報告	624
產生報告的存取點	624
了解報告	626
了解視圖和報表關係	626
報告類型	627
報告限制	628

使用報告	629
報告工作流程	629
報告快速入門	629
搜尋計劃報告	632
自訂報告	633
下載報告	636
計劃報告	636
安排報告	636
管理報告時間表	638
自訂報告範例	640
自訂叢集儲存報告	641
自訂聚合容量報告	643
自訂磁碟區容量報告	645
自訂 Qtree 容量報告	648
自訂 NFS 共享報告	649
自訂儲存虛擬機器報告	650
自訂數量關係報告	651
自訂磁碟區效能報告	655
Microsoft Excel 報表範例	655
建立報表以顯示聚合容量表和圖表	656
建立報表以顯示總計與可用容量圖表	658
建立報表以查看可用磁碟區容量圖表	662
建立報表以查看具有最多可用 IOPS 的聚合	664
使用 REST API 管理存儲	666
開始使用Active IQ Unified Manager REST API	666
此內容的受眾	666
Active IQ Unified Manager API 存取權和類別	666
Active IQ Unified Manager中提供的 REST 服務	667
Active IQ Unified Manager中的 API 版本	668
ONTAP中的儲存資源	668
Active IQ Unified Manager中的 REST API 存取權和身分驗證	669
驗證	672
Active IQ Unified Manager中使用的 HTTP 狀態碼	672
使用Active IQ Unified Manager API 的建議	673
故障排除日誌	673
Job物件異步進程	674
你好 API 伺服器	675
Unified Manager REST API	679
使用 API 管理資料中心內的儲存對象	679
透過代理存取存取ONTAP API	683
使用 API 執行管理任務	686

使用 API 管理用戶	687
使用 API 查看效能指標	687
查看作業和系統詳細信息	695
使用 API 管理事件和警報	696
使用 API 管理工作負載	698
儲存管理的常見 API 工作流程	706
了解工作流程中使用的 API 呼叫	706
使用 API 確定聚合中的空間問題	706
使用事件 API 確定儲存物件中的問題	708
使用網關 API 對ONTAP磁碟區進行故障排除	709
用於工作負載管理的 API 工作流程	712
法律聲明	737
版權	737
商標	737
專利	737
隱私權政策	737
開源	737

Active IQ Unified Manager 文檔

發行說明

提供Active IQ Unified Manager 9.16 的新功能、限制和已知問題的摘要。

欲了解更多信息，請參閱 "[Active IQ Unified Manager發行說明](#)"。

開始

VMware 安裝快速入門說明

您可以下載 `.tar` 包含根證書的文件 `README` 文件，以及 `OVA` 文件，並將 Unified Manager 部署為虛擬設備。

系統需求

- 作業系統：VMware ESXi 8.0
- 記憶體：12 GB
- CPU：總計 9572 MHz
- 可用磁碟空間：5 GB（精簡配置），152 GB（厚配置）

有關詳細的系統需求，請參閱["安裝 Unified Manager 的要求"](#)和["互通性矩陣"](#)。

安裝 Active IQ Unified Manager

下載安裝程式

1. 下載 `.tar` 包含根證書的文件 `README` 文件，以及 `OVA` 文件。
2. 將檔案儲存到 vSphere Client 可以存取的本機目錄或網路目錄。
3. 在下载的目錄中 `.tar` 文件，輸入 `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` 命令。+ 必需的 `OVA` 文件、根證書和 `README` 檔案解壓縮到目標目錄。

驗證完整性

您可以驗證 `OVA` 依照提供的步驟 `README` 文件。

安裝 Unified Manager

1. 在 vSphere Client 中，按一下「檔案」>「部署 OVF 範本」。
2. 找到 OVA 檔案並使用精靈在 ESXi 伺服器上部署虛擬設備。
3. 在「評論詳情」頁面的「發布者」部分中，訊息 `Entrust Code Signing - OVCS2 (Trusted certificate)` 確認下载的完整性 `OVA` 文件。對於訊息 `Entrust Code Signing - OVCS2 (Invalid certificate)`，將 VMware vCenter Server 升級至 7.0U3E 或更高版本。
4. 在「自訂範本」頁面的「屬性」標籤中，根據要執行的安裝類型填入所需的欄位：
 - 對於靜態配置，請在所有欄位中輸入所需的資訊。不需要新增「輔助 **DNS**」欄位的資訊。
 - 對於使用 IPv4 的 DHCP，請勿在任何欄位中新增任何資訊。
 - 對於使用 IPv6 的 DHCP，請勾選「啟用自動 IPv6 尋址」方塊。不要在任何其他欄位中添加任何資訊。
5. 啟動虛擬機器。
6. 按一下「控制台」標籤以查看初始啟動程序。

7. 配置時區。
8. 輸入 Unified Manager 維護使用者名稱和密碼。

安裝結束時，將顯示連接到 Unified Manager Web UI 的資訊。

Linux 安裝的快速入門說明

您可以下載安裝套件並在實體或虛擬 Red Hat Enterprise Linux 平台上安裝 Unified Manager。

系統需求

- 作業系統：Red Hat Enterprise Linux 8.x 和 9.4 版本，基於 x86_64 架構，使用作業系統安裝程式的「軟體選擇」選項中的「帶有 GUI 的伺服器」基礎環境進行安裝
- RAM：12 GB，CPU：總計 9572 MHz
- 可用磁碟空間：100 GB 磁碟空間 `/opt/netapp/data` 目錄，根分割區中 50 GB。對於單獨安裝 `/opt` 和 `/var/log` 目錄，確保 `/opt` 有 15 GB，`/var/log` 有 16 GB，並且 `/tmp` 有 10 GB 的可用空間。

有關詳細的系統要求以及在安全站點安裝產品的信息，請參閱["安裝 Unified Manager 的要求"](#)以及["互通性矩陣"](#)。

安裝 Active IQ Unified Manager

下載安裝程式

1. 下載 `ActiveIQUnifiedManager-<version>.zip` 安裝套件以及代碼簽署證書 (`.pem`) 和數位簽名 (`.sig`)。
2. 在下載安裝檔的目錄中，運行：

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

驗證完整性

執行以下命令驗證安裝程式包的完整性：

- 跑步 ``openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>`` 使用程式碼簽署憑證中的公鑰建立檔案。
- 跑步 ``openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip`` 驗證安裝程式包上的簽章。

驗證儲存庫配置

配置 Red Hat Enterprise Linux 儲存庫的過程是特定於站點的。您可以使用 `pre_install_check.sh` 安裝套件中包含的腳本來驗證您的作業系統的配置。如果您的系統已連接到互聯網，您將自動收到設定 Red Hat Enterprise Linux 儲存庫的說明。

```
# sudo ./pre_install_check.sh
```

安裝 Unified Manager

Unified Manager 使用 `yum` 實用程式來安裝軟體和任何相關軟體。由於 Red Hat Enterprise Linux 的映像各不相同，因此安裝的軟體包取決於映像中存在的軟體。這 `yum` 實用程式確定安裝所依賴的軟體包。如果您需要有關依賴軟體包的更多信息，請參閱["Linux 軟體和安裝需求"](#)。

若要安裝 Unified Manager，請以 root 使用者身分或使用下列命令執行 `sudo`，從安裝檔案解壓縮的目錄中：

```
# yum install netapp-um<version>.x86_64.rpm
```

或者

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

安裝結束時，將顯示連接到 Unified Manager Web UI 的資訊。如果您無法連線到 Web UI，請參閱 `README` 有關連接埠 443 限制的更多信息，請參閱軟體隨附的文件。

Windows 安裝快速入門說明

您可以下載安裝套件並安裝 Unified Manager 來監控和排除資料儲存容量、可用性、效能和保護問題。

系統需求

- 作業系統
 - Microsoft Windows Server 2019 標準版與資料中心版
 - Microsoft Windows Server 2022 標準版與資料中心版

Unified Manager 在 64 位元 Windows 作業系統上支援下列語言：

- 英語
- 日本人
- 簡體中文
- 記憶體：12 GB
- CPU：總計 9572 MHz
- 可用磁碟空間：100 GB 磁碟空間用於安裝目錄，50 GB 磁碟空間用於 MySQL 資料目錄

有關詳細的系統需求，請參閱["安裝 Unified Manager 的要求"](#)和["互通性矩陣"](#)。

安裝 Active IQ Unified Manager

下載安裝程式

1. 下載 `ActiveIQUnifiedManager-<version>.exe` 安裝包。
2. 將安裝檔案複製到目標系統上的目錄。

安裝 Unified Manager

若要安裝 Unified Manager，請確保已安裝 Microsoft .NET 4.5.2 或更高版本。作為安裝過程的一部分，Unified Manager 會根據需要安裝其他第三方軟體套件。有關依賴軟體包的更多信息，請參閱"[Windows 軟體和安裝要求](#)"。

1. 使用預設本機管理員帳戶登入 Windows。
2. 在下載安裝檔案的目錄中，以滑鼠右鍵按一下並以管理員身分執行 Unified Manager 執行檔 (.exe)。
3. 出現提示時，輸入使用者名稱和密碼以建立 Unified Manager 維護使用者。
4. 在資料庫連線精靈中，輸入 MySQL 根密碼。
5. 請按照其餘提示完成安裝。
6. 安裝結束時按一下“完成”，將顯示 Unified Manager Web UI。

在 VMware vSphere 系統上安裝 Unified Manager

Active IQ Unified Manager 簡介

Active IQ Unified Manager (以前稱為 OnCommand Unified Manager) 可讓您從單一介面監控和管理 ONTAP 儲存系統的運作狀況和效能。您可以在 Linux 伺服器、Windows 伺服器上部署 Unified Manager，也可以將其作為虛擬裝置部署在 VMware 主機上。

完成安裝並新增要管理的叢集後，Unified Manager 將提供一個圖形介面，顯示受監控儲存系統的容量、可用性、保護和效能狀態。

相關資訊

["NetApp 互通性表工具"](#)

Unified Manager 伺服器的功能

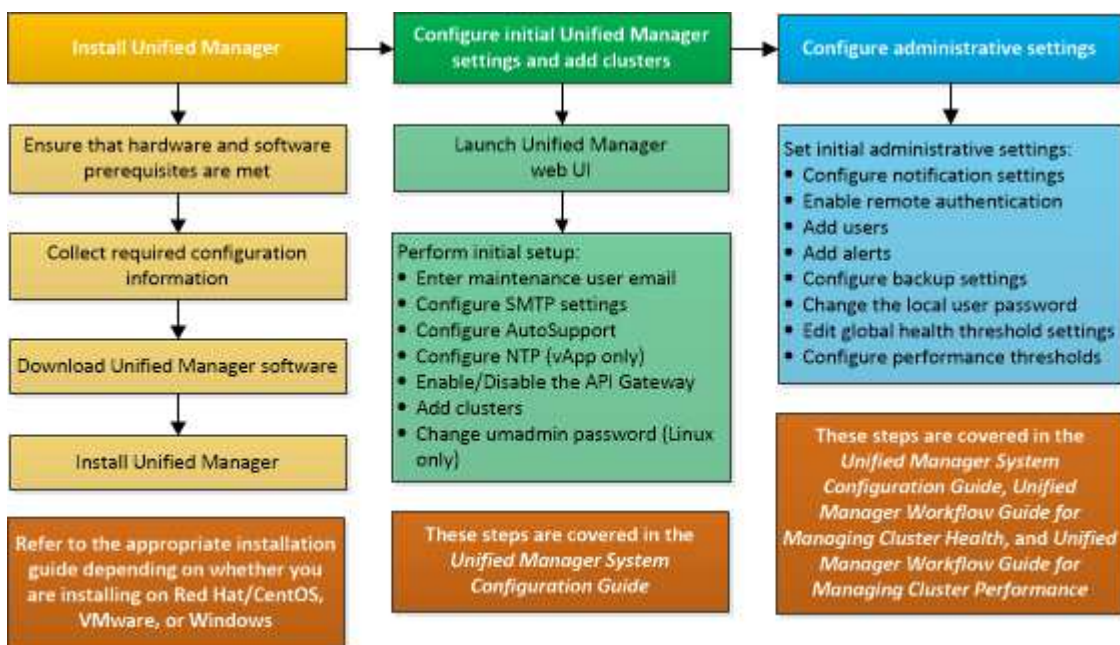
Unified Manager 伺服器基礎架構由資料收集單元、資料庫和應用程式伺服器組成。它提供發現、監控、基於角色的存取控制 (RBAC)、稽核和日誌記錄等基礎設施服務。

Unified Manager 收集叢集信息，將資料儲存在資料庫中，並分析資料以查看是否存在任何叢集問題。

安裝順序概述

安裝工作流程描述了您在使用 Unified Manager 之前必須執行的任務。

這些部分描述了下面工作流程中顯示的每個項目。



安裝 Unified Manager 的要求

在開始安裝程序之前，請確保您要安裝 Unified Manager 的伺服器符合特定的軟體、硬體、CPU 和記憶體需求。

NetApp 不支援對 Unified Manager 應用程式程式碼進行任何修改。如果您需要對 Unified Manager 伺服器套用任何安全措施，則應對安裝 Unified Manager 的作業系統進行這些變更。

有關將安全措施應用於 Unified Manager 伺服器的更多詳細信息，請參閱知識庫文章。

["適用於叢集模式 Data ONTAP 的 Active IQ Unified Manager 的安全措施的可支援性"](#)

相關資訊

有關詳細信息，請參閱 ["NetApp 互通性表工具"](#)

虛擬基礎架構和硬體系統需求

在虛擬基礎架構或實體系統上安裝 Unified Manager 應滿足記憶體、CPU 和磁碟空間的最低要求。

下表顯示了記憶體、CPU 和磁碟空間資源的建議值。這些值已經過限定，因此 Unified Manager 滿足可接受的效能水準。

硬體配置	推薦設定
記憶體	12 GB (最低要求 8 GB)
處理器	4 個 CPU
CPU 週期容量	總計 9572 MHz (最低需求 9572 MHz)
可用磁碟空間	<ul style="list-style-type: none">• 5 GB (精簡配置)• 152 GB (厚置備)

Unified Manager 可以安裝在具有少量記憶體的系統上，但建議使用 12 GB RAM，以確保有足夠的記憶體來實現最佳效能，並且隨著配置的增長，系統可以容納額外的叢集和儲存物件。您不應在部署 Unified Manager 的虛擬機器上設定任何記憶體限制，也不應啟用任何阻礙軟體利用系統上分配的記憶體的功能（例如，膨脹）。

此外，在安裝第二個 Unified Manager 實例之前，單一 Unified Manager 實例可以監控的節點數量是有限制的。有關詳細信息，請參閱 ["Unified Manager 最佳實務指南"](#)。

記憶體頁面交換會對系統和管理應用程式的效能產生負面影響。由於整體主機利用率而競爭不可用的 CPU 資源可能會降低效能。

專用要求

安裝 Unified Manager 的實體或虛擬系統應專門用於 Unified Manager，不應與其他應用程式共用。其他應用程

式可能會消耗系統資源並大幅降低 Unified Manager 的效能。

備份的空間需求

如果您打算使用 Unified Manager 備份和復原功能，請指派額外的容量，以便「資料」目錄或磁碟有 150 GB 的空間。備份可以寫入本機目標或遠端目標。最佳做法是確定 Unified Manager 主機系統外部至少具有 150 GB 空間的遠端位置。

主機連線需求

安裝 Unified Manager 的實體系統或虛擬系統應以成功的方式進行配置 `ping` 主機本身的主機名稱。如果是 IPv6 配置，您應該驗證 `ping6` 主機名稱是否成功，以確保 Unified Manager 安裝成功。

您可以使用主機名稱（或主機 IP 位址）存取產品 Web UI。如果您在部署期間為網路設定了靜態 IP 位址，那麼您就為網路主機指定了名稱。如果您使用 DHCP 配置網路，則應該從 DNS 取得主機名稱。

如果您打算允許使用者使用短名稱而不是使用完全限定網域名稱 (FQDN) 或 IP 位址存取 Unified Manager，則您的網路設定必須將此短名稱解析為有效的 FQDN。

VMware 軟體和安裝要求

安裝 Unified Manager 的 VMware vSphere 系統需要特定版本的作業系統和特定版本的支援軟體。

作業系統軟體

支援的作業系統是 VMware ESXi 8.0。



VMware vSphere 系統上的 Unified Manager OVA 在內部執行 Debian OS 12 (bookworm)。有關支援版本的 ESXi 伺服器可以支援的虛擬機器硬體版本的信息，請參閱 VMware 文件。

支援以下版本的 vSphere：

- VMware vCenter Server 7.0 和 8.0

請參閱互通性矩陣以取得受支援的 ESXi 版本的完整和最新清單。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

為了確保虛擬設備正常運作，VMware ESXi 伺服器時間應與 NTP 伺服器時間相同。將 VMware ESXi 伺服器時間與 NTP 伺服器時間同步可防止時間錯誤。

安裝要求

支援 Unified Manager 虛擬設備的 VMware High Availability。

如果在執行 ONTAP 軟體的儲存系統上部署 NFS 資料儲存庫，請使用適用於 VMware VAAI 的 NetApp NFS 外掛程式來使用厚配置。

如果由於資源不足導致使用啟用高可用性的環境進行部署失敗，則可能需要透過停用虛擬機器重新啟動優先權並保持主機隔離回應為開啟狀態來修改叢集功能虛擬機器選項。



安裝或升級 Unified Manager 時，所需的第三方軟體和安全性修補程式會在 VMware vSphere 系統上自動安裝或升級。由於 Unified Manager 安裝和升級程序控制這些元件，因此您不應嘗試獨立安裝或升級任何第三方元件。

支援的瀏覽器

若要存取 Unified Manager Web UI，請使用支援的瀏覽器。

互通性矩陣列出了受支援的瀏覽器版本。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

對於所有瀏覽器，停用彈出視窗阻止程式可確保軟體功能正常顯示。

如果您打算設定 Unified Manager 進行 SAML 驗證，以便身分提供者 (IdP) 可以對使用者進行驗證，那麼您也應該檢查 IdP 支援的瀏覽器清單。

協定和連接埠要求

所需的連接埠和協定支援 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間的通訊。

與 Unified Manager 伺服器的連接

在典型安裝中，連接到 Unified Manager Web UI 時無需指定連接埠號，因為請務必使用預設連接埠。例如，由於 Unified Manager 始終嘗試在其預設連接埠上執行，因此您可以輸入 `https://<host>` 而不是 `https://<host>:443`。

Unified Manager 伺服器使用特定協定存取下列介面：

介面	協定	港口	描述
Unified Manager Web UI	HTTP	80	用於存取 Unified Manager Web UI；自動重定向到安全連接埠 443。
Unified Manager Web UI 和使用 API 的程式	HTTPS	443	用於安全存取 Unified Manager Web UI 或進行 API 呼叫；API 呼叫只能使用 HTTPS 進行。
維護控制台	SSH/SFTP	22	用於存取維護控制台和檢索支援包。
Linux 命令列	SSH/SFTP	22	用於存取 Red Hat Enterprise Linux 命令列並檢索支援包。

介面	協定	港口	描述
系統日誌	UDP	514	用於從ONTAP系統存取基於訂閱的 EMS 訊息並根據這些訊息建立事件。
休息	HTTPS	9443	用於從經過驗證的ONTAP系統存取基於即時 REST API 的 EMS 事件。
MySQL 資料庫	MySQL	3306	用於啟用OnCommand Workflow Automation 和OnCommand API Services 對 Unified Manager 的存取。
AMQP QPID 代理	TCP/IP	56072	用於內部訊息通訊。
AMQP QPID 代理	透過 TCP 的 WebSocket	56080	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。
AMQP QPID 代理	透過 TCP 的 WebSocket	56443	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。透過此連接埠的通訊支援 TLS 或 SSL 提供的加密。




在 VMware vSphere 系統上安裝 Unified Manager 時，MySQL 的預設連接埠 3306 僅限於本機。這不會影響任何升級方案，因為先前的配置會保留。可以修改此配置，並且可以使用 `Control access to MySQL port 3306` 維護控制台上的選項。有關信息，請參閱["附加選單選項"](#)。可以使用 Unified Manager 維護控制台變更為 HTTP 和 HTTPS 通訊的連接埠（連接埠 80 和 443）。有關詳細信息，請參閱 ["維護控制台選單"](#)。

來自 Unified Manager 伺服器的連接

您應該配置防火牆以開啟端口，以便 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間進行通訊。如果連接埠未打開，則通訊失敗。

根據您的環境，您可以選擇修改 Unified Manager 伺服器用於連接到特定目的地的連接埠和協定。

Unified Manager 伺服器使用下列協定和連接埠連接到託管儲存系統、伺服器和其他元件：

目的地	協定	港口	描述
儲存系統	HTTPS	443/TCP	用於監控和管理儲存系統。 <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  <p>如果您使用此連接埠或任何其他連接埠連線至 VMware vCenter Server 或 ESXi 伺服器，請確保該連接埠可用且可在安全站點連線。</p> </div>
儲存系統	NDMP	10000/TCP	用於某些快照復原操作。
AutoSupport伺服器	HTTPS	443	用於發送AutoSupport資訊。需要網路存取才能執行此功能。
身份驗證伺服器	LDAP	389	用於發出身份驗證請求以及使用者和群組查找請求。
LDAPS	636	用於安全 LDAP 通訊。	郵件伺服器
SMTP	25	用於發送警報通知電子郵件。	SNMP 陷阱發送器
SNMPv1 或 SNMPv3	162/UDP	用於發送警報通知 SNMP 陷阱。	外部資料提供伺服器
TCP	2003	用於將效能資料傳送至外部資料提供者，例如 Graphite。	NTP 伺服器
NTP	123/UDP	用於將 Unified Manager 伺服器上的時間與外部 NTP 時間伺服器同步。（僅限 VMware 系統）	系統日誌

完成工作表

在安裝和設定 Unified Manager 之前，您應該準備好有關您的環境的具體資訊。您可以在工作表中記錄該資訊。

Unified Manager 安裝訊息

安裝 Unified Manager 所需的詳細資訊。

部署軟體的系統	你的價值
ESXi 伺服器 IP 位址	
主機完全限定域名	
主機 IP 位址	
網路遮罩	
網關 IP 位址	
主 DNS 位址	
輔助 DNS 位址	
搜尋域名	
維護用戶名	
維護用戶密碼	

Unified Manager 設定訊息

安裝後設定 Unified Manager 的詳細資訊。根據您的配置，某些值是可選的。

環境	你的價值
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	

環境	你的價值
SMTP 密碼	
SMTP 連接埠	25 (預設值)
發送警報通知的電子郵件	
身份驗證伺服器主機名稱或 IP 位址	
Active Directory 管理員名稱或 LDAP 綁定可分辨名稱	
Active Directory 密碼或 LDAP 綁定密碼	
認證伺服器基礎可分辨名稱	
身分識別提供者 (IdP) URL	
身分提供者 (IdP) 元資料	
SNMP 陷阱目標主機 IP 位址	
SNMP 連接埠	

集群資訊

使用 Unified Manager 管理的儲存系統的詳細資訊。

N 的簇 1	你的價值
主機名稱或叢集管理 IP 位址	
ONTAP 管理員使用者名稱  必須為管理員指派“admin”角色。	
ONTAP 管理員密碼	
協定	HTTPS

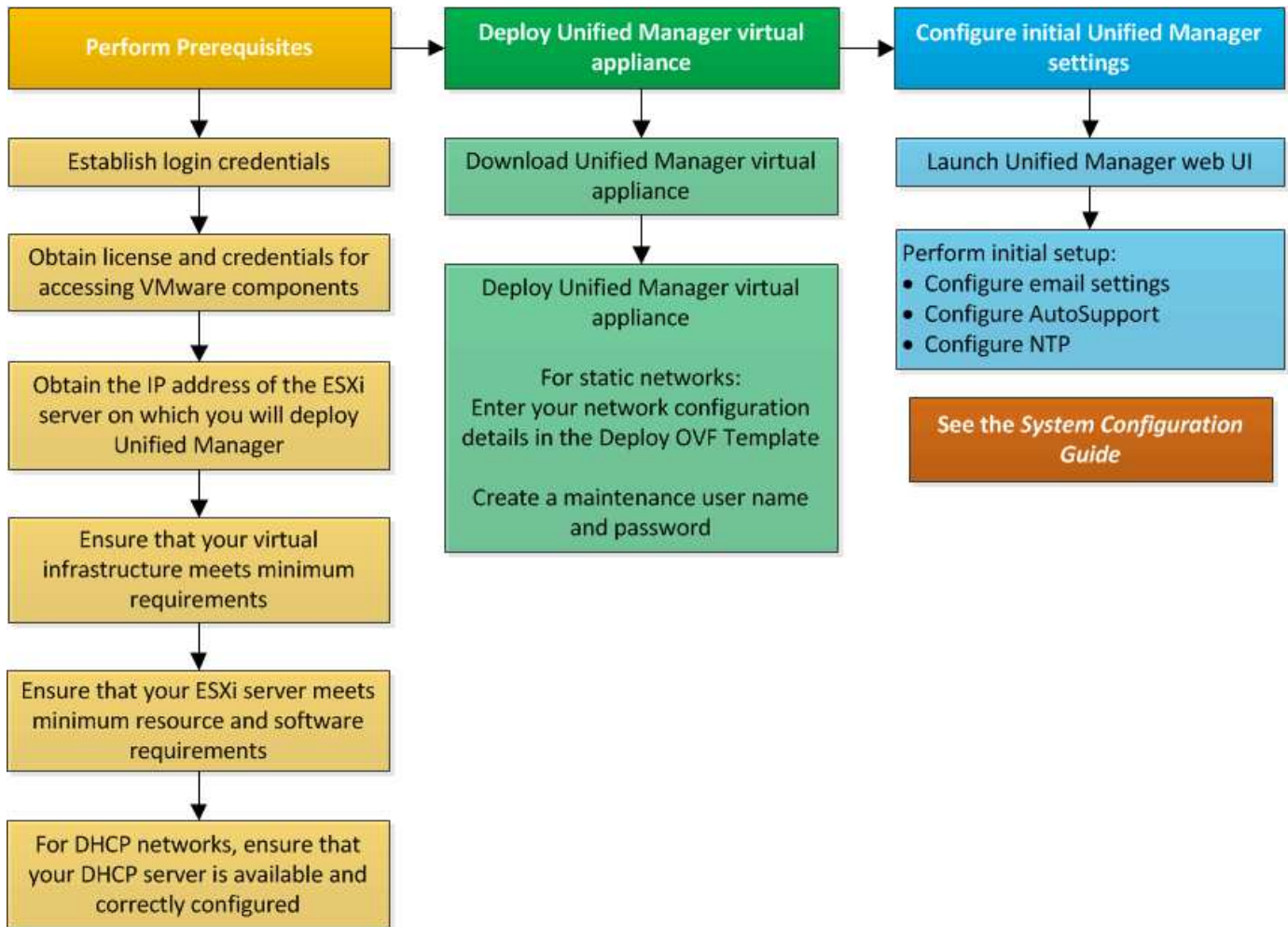
安裝、升級和刪除 Unified Manager 軟體

在 VMware vSphere 系統上，您可以安裝 Unified Manager、升級至較新版本的軟體或移

除 Unified Manager 虛擬設備 (vApp)。

部署流程概述

部署工作流程描述了您在使用 Unified Manager 之前必須執行的任務。



部署 Unified Manager

部署 Unified Manager 包括下載軟體、部署虛擬設備、建立維護使用者名稱和密碼以及在 Web UI 中執行初始設定。

開始之前

- 您應該驗證並完成部署的系統需求。

看"系統需求"。

- 確保您擁有以下資訊：
 - NetApp支援網站的登入憑證
 - 用於存取 VMware vCenter Server 和 vSphere Web Client 的憑證
 - 您要部署 Unified Manager 虛擬設備的 ESXi 伺服器的 IP 位址

- 有關資料中心的詳細信息，例如資料儲存中的儲存空間和記憶體要求
- 如果您打算使用 IPv6 位址，則應在主機上啟用 IPv6。

您可以將 Unified Manager 以虛擬設備部署在 VMware ESXi 伺服器上。

您應該使用 VMware 控制台存取維護控制台，而不是使用 SSH。



從 Unified Manager 9.8 開始，VMware Tools 已被 Open VM Tools 取代 (open-vm-tools)。您不再需要在安裝過程中安裝 VMware Tools，因為 `open-vm-tools` 包含在 Unified Manager 安裝套件中。

完成部署和初始設置後，您可以新增集群，或在維護控制台中配置其他網路設置，然後存取 Web UI。

步驟

1. 請依照以下步驟操作"[下載 Unified Manager](#)"。
2. 此外，請按照"[部署 Unified Manager 虛擬設備](#)"。

下載 **Unified Manager** 安裝文件

從 NetApp 支援網站下載 Unified Manager 安裝文件，將 Unified Manager 部署為虛擬裝置。

開始之前

您應該擁有 NetApp 支援網站的登入憑證。

安裝檔案是 `.tar` 包含根證書的文件 `README` 文件，以及 `OVA` 包含為虛擬裝置設定的 Unified Manager 軟體的檔案。

步驟

1. 登入 NetApp 支援站點，然後導覽至 Unified Manager 的下載頁面：

["NetApp 支援站點"](#)

2. 選擇所需版本的 Unified Manager 並接受最終使用者授權協議 (EULA)。
3. 下載並儲存 `.tar` 將 VMware vSphere 安裝檔案複製到 vSphere Client 可以存取的本機目錄或網路目錄。
4. 驗證校驗和以確保軟體正確下載。
5. 導航到您下載的目錄 `.tar` 檔案並在終端機視窗中輸入以下命令以展開 Unified Manager 套件：

```
tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
```

所需的 `OVA` 文件、根證書和 `README` Unified Manager 的檔案解壓縮到目標目錄。

6. 驗證完整性 `OVA` 依照提供的步驟 `README` 文件。

部署 Unified Manager 虛擬設備

下載安裝檔案後，您可以將 Unified Manager 部署為虛擬裝置。使用 vSphere Web Client 在 ESXi 伺服器上部署虛擬設備。部署虛擬設備時，會建立一個虛擬機器。

開始之前

您應該查看系統要求。在部署 Unified Manager 虛擬設備之前進行必要的變更。

看"虛擬基礎架構要求"。

看"VMware 軟體和安裝要求"。

如果使用動態主機設定協定 (DHCP)，請確保 DHCP 伺服器可用，且 DHCP 和虛擬機器 (VM) 網路介面卡配置正確。DHCP 是預設配置的。

如果使用靜態網路配置，請確保 IP 位址在相同子網路中不會重複，並且已配置適當的 DNS 伺服器項目。

部署虛擬設備之前取得以下資訊：

- 用於存取 VMware vCenter Server 和 vSphere Web Client 的憑證
- 您要部署 Unified Manager 虛擬設備的 ESXi 伺服器的 IP 位址
- 有關資料中心的詳細信息，例如儲存空間的可用性
- 如果您不使用 DHCP，請取得您計劃連接的網路設備的 IPv4 或 IPv6 位址：
 - 主機的完全限定網域名稱 (FQDN)
 - 主機的 IP 位址
 - 網路遮罩
 - 預設網關的 IP 位址
 - 主 DNS 位址和輔助 DNS 位址
 - 搜尋域名

從 Unified Manager 9.8 開始，VMware Tools 已被 Open VM Tools 取代 (*open-vm-tools*)。您無需在安裝過程中安裝 VMware Tools，因為 *open-vm-tools* 包含在 Unified Manager 安裝套件中。

部署虛擬裝置時，會產生用於 HTTPS 存取的唯一自簽章憑證。造訪 Unified Manager Web UI 時，您可能看到有關不受信任的憑證的瀏覽器警告。

支援 Unified Manager 虛擬設備的 VMware High Availability。

步驟

1. 在 vSphere Client 中，按一下 檔案 > 部署 **OVF** 範本。
2. 完成部署 OVF 範本精靈以部署 Unified Manager 虛擬設備。

在「審核詳情」頁面：

- 驗證發布者部分的詳細資訊。訊息 **Entrust Code Signing - OVCS2 (Trusted certificate)** 確認下載的完整性 `OVA` 文件。+ 如果您看到訊息 **Entrust Code Signing - OVCS2** (無效憑證)，請將 VMware vCenter Server 升級至 7.0U3E 或更高版本。

在「自訂模板」頁面上：

- 使用 DHCP 和 IPv4 尋址時，將所有欄位留空。
- 選取「啟用自動 IPv6 位址」框，並在使用 DHCP 和 IPv6 位址時將所有其他欄位留空。
- 如果您想使用靜態網路配置，您可以填寫此頁面上的字段，這些設定在部署期間會套用。確保 IP 位址對於部署它的主機是唯一的、尚未使用且具有有效的 DNS 項目。

3. 將 Unified Manager 虛擬設備部署到 ESXi 伺服器後，以滑鼠右鍵按一下虛擬機，然後選擇 啟動 來啟動虛擬機。



如果因資源不足導致開機操作失敗，請新增資源，然後重試安裝。

4. 按一下「控制台」標籤。

初始啟動過程需要幾分鐘才能完成。

5. 若要設定您的時區，請依照 VM 控制台視窗中的指示輸入您的地理區域和城市或地區。

所有顯示的日期資訊均使用為 Unified Manager 設定的時區，而不管託管裝置上的時區設定為何。如果您的儲存系統和管理伺服器配置了相同的 NTP 伺服器，則它們指的是相同的時間點，即使它們看起來不同。例如，如果您使用與管理伺服器配置不同時區的裝置建立 Snapshot 副本，時間戳記就是管理伺服器時間。

6. 如果沒有可用的 DHCP 服務，或靜態網路設定的詳細資訊有錯誤，請選擇下列選項之一：

如果您使用...	然後這樣做...
DHCP	<p>選擇*重試 DHCP*。如果您打算使用 DHCP，則應確保其配置正確。</p> <p>如果您使用啟用 DHCP 的網路，FQDN 和 DNS 伺服器項目將自動提供給虛擬設備。如果 DHCP 未正確配置 DNS，則會自動指派主機名稱「UnifiedManager」並將其與安全性憑證關聯。如果您尚未設定啟用 DHCP 的網路，則應手動輸入網路設定資訊。</p>
靜態網路配置	<p>a. 選擇*輸入靜態網路配置的詳細資訊*。</p> <p>配置過程需要幾分鐘才能完成。</p> <p>b. 確認您輸入的值，然後選擇 Y。</p>

7. 在提示符號下，輸入維護用戶名，然後按一下 **Enter**。

維護使用者名稱應以 az 的字母開頭，後面跟著 -、az 或 0-9 的任意組合。

8. 在提示符號下，輸入密碼，然後按一下「**Enter**」。

VM 控制台顯示 Unified Manager Web UI 的 URL。

您可以存取 Web UI 來執行 Unified Manager 的初始設置，例如["配置Active IQ Unified Manager"](#)。

升級 Unified Manager

您只能將Active IQ Unified Manager從版本 9.13 或 9.14 升級到版本 9.16。

在升級過程中，Unified Manager 不可用。在升級 Unified Manager 之前，您應該完成所有正在執行的操作。

如果 Unified Manager 與OnCommand Workflow Automation實例配對，且這兩種產品都有新版本的軟體可用，則必須中斷這兩種產品的連接，然後在執行升級後建立新的 Workflow Automation 連接。如果您只對其中一個產品進行升級，則應在升級後登入工作流程自動化並驗證它是否仍在從 Unified Manager 取得資料。

步驟

1. 請依照以下步驟操作["下載 Unified Manager ISO 映像"](#)。
2. 此外，請按照["升級 Unified Manager"](#)。

Unified Manager 版本支援的升級路徑

Active IQ Unified Manager支援每個版本的特定升級路徑。

並非所有版本的 Unified Manager 都可以執行就地升級到更高版本。Unified Manager 升級僅限於 N-2 型號，這表示升級只能在所有平台上的下 2 個版本內進行。例如，您只能從 Unified Manager 9.13 和 9.14 升級到 Unified Manager 9.16。

如果您執行的版本早於支援的版本，則需要先將 Unified Manager 實例升級到支援的版本之一，然後再升級至目前版本。

例如，如果您安裝的版本是 Unified Manager 9.9，並且您想要升級到 Unified Manager 9.14，請遵循一系列升級作業。

升級路徑範例：

1. 升級 9.11 → 9.13
2. 升級 9.13 → 9.14
3. 升級 9.13 → 9.16
4. 升級 9.14 → 9.16

有關升級路徑矩陣的更多信息，請參閱 ["知識庫 \(KB\) 文章"](#)。

下載 Unified Manager 升級文件

在升級 Unified Manager 之前，請從NetApp支援網站下載 Unified Manager 升級檔案。

開始之前

您應該擁有NetApp支援網站的登入憑證。

步驟

1. 登入NetApp支援站點：

"NetApp支援站點"

2. 導覽至用於升級 VMware vSphere 上的 Unified Manager 的下載頁面。
3. 下載`.iso`升級映像，並將其儲存到 vSphere Client 可以存取的本機目錄或網路目錄中。
4. 驗證校驗和以確保軟體已正確下載。

升級 Unified Manager 虛擬設備

您可以將Active IQ Unified Manager虛擬裝置從版本 9.13 或 9.14 升級到 9.16。

開始之前

確保以下事項：

- 您已從NetApp支援網站下載升級文件，即 ISO 映像。
- 若要升級 Unified Manager 的系統符合系統和軟體需求。

看"[虛擬基礎架構要求](#)"。

看"[VMware 軟體和安裝要求](#)"。

- 對於 vSphere 6.5 及更高版本的用戶，您已安裝 VMware 遠端控制台 (VMRC)。
- 在升級過程中，系統可能會提示您確認是否要保留先前的預設設定（將效能資料保留 13 個月）或將其變更為 6 個月。確認後，歷史績效數據將在 6 個月後清除。
- 您有以下資訊：
 - NetApp支援網站的登入憑證
 - 用於存取 VMware vCenter Server 和 vSphere Web Client 的憑證
 - Unified Manager 維護使用者的憑證

在升級過程中，Unified Manager 不可用。在升級 Unified Manager 之前，您應該完成所有正在執行的操作。

如果您已將 Workflow Automation 與 Unified Manager 配對，則應手動更新 Workflow Automation 中的主機名稱。

步驟

1. 在 vSphere Client 中，按一下 首頁 > 清單 > 虛擬機器和範本。
2. 選擇安裝了 Unified Manager 虛擬設備的虛擬機器 (VM)。
3. 如果 Unified Manager VM 正在運行，請導覽至 **Summary > Commands > Shut Down Guest**。
4. 建立 Unified Manager VM 的備份副本（例如快照或複製）以建立應用程式一致的備份。
5. 從 vSphere Client 啟動 Unified Manager VM。
6. 啟動 VMware 遠端控制台。
7. 按一下 **CDROM** 圖標，然後選擇 連接到磁碟映像檔 (.iso)。
8. 選擇 `ActiveIQUnifiedManager-<version>-virtual-update.iso` 文件，然後按一下*開啟*。
9. 按一下「控制台」標籤。

10. 登入 Unified Manager 維護控制台。

11. 在主選單中，選擇*升級*。

顯示一則訊息，指出 Unified Manager 在升級過程中不可用，升級完成後將恢復。

12. 類型 `y` 繼續。

將顯示警告，提醒您備份虛擬設備所在的虛擬機器。

13. 類型 `y` 繼續。

升級程序和 Unified Manager 服務的重新啟動可能需要幾分鐘才能完成。

14. 按任意鍵繼續。

您將自動退出維護控制台。

15. *選用：*登入維護控制台，並驗證 Unified Manager 的版本。

您可以在支援的 Web 瀏覽器的新視窗中啟動 Web UI，然後登入以使用升級版的 Unified Manager。請注意，您需要等待發現過程完成，然後才能在 UI 中執行任何任務。

重新啟動 Unified Manager 虛擬機

您可以從維護控制台重新啟動 Unified Manager 虛擬機器 (VM)。產生新的安全性憑證後，或當虛擬機器出現問題時，您應該重新啟動虛擬機器。

開始之前

- 虛擬設備應已啟動。
- 您應該以維護使用者身分登入 Unified Manager 維護控制台。

您也可以使用 VMware 重新啟動客戶機 選項從 vSphere 重新啟動虛擬機器。參考 ["Broadcom 的 VMware vSphere PowerCLI CMDLET 參考中的 Restart-VMGuest cmdlet。"](#)

步驟

1. 在維護控制台中，選擇*系統設定*>*重新啟動虛擬機器*。
2. 從您的瀏覽器啟動 Unified Manager Web UI，然後登入。

刪除 Unified Manager

您可以透過刪除安裝了 Unified Manager 軟體的虛擬機器 (VM) 來解除安裝 Unified Manager。

開始之前

- 您應該擁有存取 VMware vCenter Server 和 vSphere Web Client 的憑證。
- 應關閉 Unified Manager 伺服器與工作流程自動化伺服器的任何活動連線。
- 在刪除虛擬機器 (VM) 之前，應從 Unified Manager 伺服器中刪除所有叢集 (資料來源)。

步驟

1. 使用 Unified Manager 維護控制台驗證 Unified Manager 伺服器是否沒有與外部資料提供者的活動連線。
2. 在 vSphere Client 中，按一下 首頁 > 清單 > 虛擬機器和範本。
3. 選擇要刪除的虛擬機，然後按一下「摘要」標籤。
4. 如果虛擬機器正在運行，請按一下*電源*>*關閉客戶機*。
5. 右鍵單擊要刪除的虛擬機，然後按一下「從磁碟刪除」。

在 Linux 系統上安裝 Unified Manager

Active IQ Unified Manager 簡介

Active IQ Unified Manager (以前稱為 OnCommand Unified Manager) 可讓您從單一介面監控和管理 ONTAP 儲存系統的運作狀況和效能。您可以在 Linux 伺服器、Windows 伺服器上部署 Unified Manager，也可以將其作為虛擬裝置 (vApp) 部署在 VMware 主機上。

完成安裝並新增要管理的叢集後，Unified Manager 將提供一個圖形介面，顯示受監控儲存系統的容量、可用性、保護和效能狀態。

相關資訊

["NetApp 互通性表工具"](#)

Unified Manager 伺服器的功能

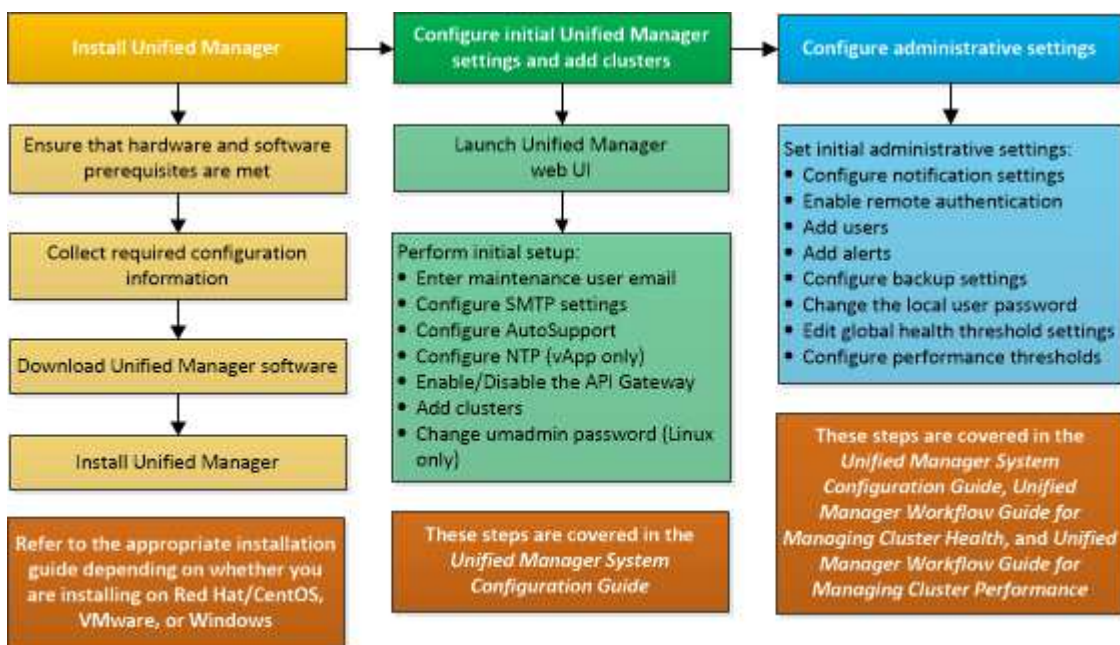
Unified Manager 伺服器基礎架構由資料收集單元、資料庫和應用程式伺服器組成。它提供發現、監控、基於角色的存取控制 (RBAC)、稽核和日誌記錄等基礎設施服務。

Unified Manager 收集叢集信息，將資料儲存在資料庫中，並分析資料以查看是否存在任何叢集問題。

安裝順序概述

安裝工作流程描述了您在使用 Unified Manager 之前必須執行的任務。

這些部分描述了下面工作流程中顯示的每個項目。



安裝 Unified Manager 的要求

在開始安裝程序之前，請確保您要安裝 Unified Manager 的伺服器符合特定的軟體、硬體、CPU 和記憶體需求。

NetApp 不支援對 Unified Manager 應用程式程式碼進行任何修改。如果您需要對 Unified Manager 伺服器套用任何安全措施，則應對安裝 Unified Manager 的作業系統進行這些變更。

有關將安全措施應用於 Unified Manager 伺服器的更多詳細信息，請參閱知識庫文章。

["適用於叢集模式 Data ONTAP 的 Active IQ Unified Manager 的安全措施的可支援性"](#)


相關資訊

["NetApp 互通性表工具"](#)

虛擬基礎架構和硬體系統需求

在虛擬基礎架構或實體系統上安裝 Unified Manager 應滿足記憶體、CPU 和磁碟空間的最低要求。

下表顯示了記憶體、CPU 和磁碟空間資源的建議值。這些值已經過限定，因此 Unified Manager 滿足可接受的效能水準。

硬體配置	推薦設定
記憶體	12 GB (最低要求 8 GB)
處理器	4 個 CPU
CPU 週期容量	總計 9572 MHz (最低需求 9572 MHz)
可用磁碟空間	150GB，容量分配如下： <ul style="list-style-type: none">• 分配給根分割區 50 GB• 分配給 <code>/opt/netapp/data</code> 目錄，安裝在 LVM 磁碟機上或安裝在目標系統上的單獨本機磁碟上 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> 對於單獨安裝 <code>/opt</code> 和 <code>/var/log</code> 目錄，確保 <code>/opt</code> 有 15 GB 並且 <code>/var/log</code> 有 16 GB 的可用空間。這 <code>/tmp</code> 目錄應至少有 10 GB 的可用空間。</div>

Unified Manager 可以安裝在具有少量記憶體的系統上，但建議使用 12 GB RAM，以確保有足夠的記憶體來實現最佳效能，並且隨著配置的增長，系統可以容納額外的叢集和儲存物件。您不應在部署 Unified Manager 的虛擬機器上設定任何記憶體限制，也不應啟用任何阻礙軟體利用系統上分配的記憶體的功能（例如，膨脹）。

此外，在安裝第二個 Unified Manager 實例之前，單一 Unified Manager 實例可以監控的節點數量是有限制的。

有關更多信息，請參閱《最佳實踐指南》。

"技術報告 4621：Unified Manager 最佳實務指南"

記憶體頁面交換會對系統和管理應用程式的效能產生負面影響。由於整體主機利用率而競爭不可用的 CPU 資源可能會降低效能。

專用要求

安裝 Unified Manager 的實體或虛擬系統應專門用於 Unified Manager，不應與其他應用程式共用。其他應用程式可能會消耗系統資源並大幅降低 Unified Manager 的效能。

備份的空間需求

如果您打算使用 Unified Manager 備份和復原功能，請指派額外的容量，以便「資料」目錄或磁碟有 150 GB 的空間。備份可以寫入本機目標或遠端目標。最佳做法是確定 Unified Manager 主機系統外部至少具有 150 GB 空間的遠端位置。

主機連線需求

安裝 Unified Manager 的實體系統或虛擬系統應以成功的方式進行配置 `ping` 主機本身的主機名稱。如果是 IPv6 配置，您應該驗證 `ping6` 主機名稱是否成功，以確保 Unified Manager 安裝成功。

您可以使用主機名稱（或主機 IP 位址）存取產品 Web UI。如果您在部署期間為網路設定了靜態 IP 位址，那麼您就為網路主機指定了名稱。如果您使用 DHCP 配置網路，則應該從 DNS 取得主機名稱。

如果您打算允許使用者使用短名稱而不是使用完全限定網域名稱 (FQDN) 或 IP 位址存取 Unified Manager，則您的網路設定必須將此短名稱解析為有效的 FQDN。

Linux 軟體和安裝需求

安裝 Unified Manager 的 Linux 系統需要特定版本的作業系統和支援軟體。

作業系統軟體

Linux 系統必須安裝以下版本的作業系統及支援軟體：

- Red Hat Enterprise Linux 8.x 與 9.4 版本，基於 x86_64 架構。

請參閱互通性矩陣以取得受支援的 Red Hat Enterprise Linux 版本的完整和最新清單。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

該伺服器應專用於執行 Unified Manager。伺服器上不應安裝任何其他應用程式。由於公司規定，您的 Linux 系統上可能安裝了像 Qualys 這樣的漏洞掃描程式。您應該在安裝 Unified Manager 之前停用漏洞掃描程序，以防止安裝失敗。



漏洞掃描程式（例如 Qualys）在內部掃描虛擬機器 (VM)（其中 Unified Manager 和漏洞掃描程式安裝在同一 VM 上）或外部掃描虛擬機器（其中 Unified Manager 和漏洞掃描程式安裝在兩個不同的伺服器上，且漏洞掃描程式掃描安裝了 Unified Manager 的 VM）時可能會導致 CPU 使用率過高。此問題通常會導致虛擬機器無回應並影響 Unified Manager 服務。因此，NetApp 建議在安裝了 Unified Manager 的 VM 中停用漏洞掃描程式。如果無法停用掃描儀，則在非工作時間掃描虛擬機，並在掃描完成後重新啟動服務。

第三方軟體

Unified Manager 部署在 WildFly Web 伺服器上。WildFly 26.1.3 與 Unified Manager 捆綁並配置。

以下第三方軟體套件是必要的，但不包含在 Unified Manager 中。這些軟體包由 `yum` 安裝程序，前提是您已按照以下部分所述配置了儲存庫。

- MySQL 社群版 8.4.4 版（來自 MySQL 儲存庫）
- OpenJDK 版本 11.0.25（來自 Red Hat Extra Enterprise Linux Server 儲存庫）
- Python 3.9.x（來自 Red Hat Extra Enterprise Linux Server 儲存庫）
- p7zip 版本 16.02 或更高版本（來自 Red Hat Extra Packages for Enterprise Linux 儲存庫）



在升級任何第三方軟體之前，您必須關閉正在執行的 Unified Manager 實例。第三方軟體安裝完成後，您可以重新啟動 Unified Manager。

使用者授權要求

Linux 系統上的 Unified Manager 安裝可由 root 使用者或非 root 使用者使用 `sudo` 命令。

此外，預設 Unified Manager 安裝在 sudoers 檔案中包含 umadmin 用戶（預設為維護用戶）和 jboss 用戶 (ocum_sudoers 和 ocie_sudoers) 在 `/etc/sudoers.d/` 目錄。如果您因為安全性原則或安全監控工具而從環境中刪除此內容，則必須將其加回。您需要保留 sudoers 配置，因為某些 Unified Manager 操作需要這些 sudo 權限。

安裝要求

以下列出了在您的系統上安裝 Red Hat Enterprise Linux 和相關儲存庫的最佳實務。以不同方式安裝或設定的系統，或在異地（在雲端）部署的系統可能需要額外的步驟，而 Unified Manager 可能無法在這樣的部署中正常運作。

- 您必須按照 Red Hat 最佳實務安裝 Red Hat Enterprise Linux，並且應該選擇以下預設選項，這需要選擇「具有 GUI 的伺服器」基礎環境。
- 在 Red Hat Enterprise Linux 上安裝 Unified Manager 時，系統必須能夠存取對應的儲存庫，以便安裝程式可以存取和安裝所有必要的軟體相依性。
- 對於 `yum` 安裝程式在 Red Hat Enterprise Linux 儲存庫中尋找相關軟體，您必須在 Red Hat Enterprise Linux 安裝期間或之後使用有效的 Red Hat 訂閱註冊系統。

有關 Red Hat 訂閱管理員的信息，請參閱 Red Hat 文件。

- 您必須啟用 Extra Packages for Enterprise Linux (EPEL) 儲存庫才能在系統上成功安裝所需的第三方公用程式。

如果您的系統上未配置 EPEL 儲存庫，則必須手動下載並配置儲存庫。

看"[手動配置 EPEL 儲存庫](#)"。

- 如果未安裝正確版本的 MySQL，則必須啟用 MySQL 儲存庫才能在系統上成功安裝 MySQL 軟體。

如果您的系統上未配置 MySQL 儲存庫，則必須手動下載並設定儲存庫。

看"[手動設定 MySQL 儲存庫](#)"。

- 您必須在 Unified Manager 主機上僅安裝一個版本的 Java；否則，系統可能無法確定要使用哪個版本。看 "[在 Active IQ Unified Manager 主機上更新 Java 後，服務將無法啟動](#)"。

如果您的系統無法存取互聯網，且儲存庫沒有從連接互聯網的系統鏡像到未連接的系統，則您應該按照安裝說明確定系統的外部軟體依賴項。然後，您可以將所需的軟體下載到已連接互聯網的系統，並將`.rpm`檔案到您計劃安裝 Unified Manager 的系統。要下載工件和包，您必須使用`yum install`命令。您必須確保兩個系統運行相同的作業系統版本，並且訂閱授權適用於適當的 Red Hat Enterprise Linux。



您不得從此處列出的儲存庫以外的儲存庫安裝所需的第三方軟體。從 Red Hat 儲存庫安裝的軟體專為 Red Hat Enterprise Linux 而設計，並符合 Red Hat 最佳實務（目錄佈局、權限等）。其他位置的軟體可能不遵循這些準則，這可能會導致 Unified Manager 安裝失敗，或可能導致未來升級出現問題。

連接埠 443 要求

Red Hat Enterprise Linux 的通用映像可能會阻止對連接埠 443 的外部存取。由於此限制，您可能無法在安裝 Unified Manager 後連線至管理員 Web UI。執行以下命令允許通用 Red Hat Enterprise Linux 上的所有外部使用者和應用程式存取連接埠 443。

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd --reload
```

您必須使用「具有 GUI 的伺服器」基礎環境安裝 Red Hat Enterprise Linux。它提供了 Unified Manager 安裝說明所使用的命令。其他基礎環境可能需要您安裝其他指令來驗證或完成安裝。如果`firewall-cmd`在您的系統上不可用，您必須透過執行以下命令來安裝它：

```
# sudo yum install firewalld
```

執行命令之前請聯絡您的 IT 部門，以了解您的安全策略是否需要不同的程序。



Red Hat 系統上應停用 THP（透明大頁面）。啟用後，在某些情況下，當某些進程消耗過多記憶體並終止時，它可能會導致 Unified Manager 關閉。

支援的瀏覽器

若要存取 Unified Manager Web UI，請使用支援的瀏覽器。

互通性矩陣列出了受支援的瀏覽器版本。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

對於所有瀏覽器，停用彈出視窗阻止程式可確保軟體功能正常顯示。

如果您打算設定 Unified Manager 進行 SAML 驗證，以便身分提供者 (IdP) 可以對使用者進行驗證，那麼您也應該檢查 IdP 支援的瀏覽器清單。

協定和連接埠要求

所需的連接埠和協定支援 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間的通訊。

與 Unified Manager 伺服器的連接

在典型安裝中，連接到 Unified Manager Web UI 時無需指定連接埠號，因為請務必使用預設連接埠。例如，由於 Unified Manager 始終嘗試在其預設連接埠上執行，因此您可以輸入 `https://<host>` 而不是 `https://<host>:443`。

Unified Manager 伺服器使用特定協定存取下列介面：

介面	協定	港口	描述
Unified Manager Web UI	HTTP	80	用於存取 Unified Manager Web UI；自動重定向到安全連接埠 443。
Unified Manager Web UI 和使用 API 的程式	HTTPS	443	用於安全存取 Unified Manager Web UI 或進行 API 呼叫；API 呼叫只能使用 HTTPS 進行。
維護控制台	SSH/SFTP	22	用於存取維護控制台和檢索支援包。
Linux 命令列	SSH/SFTP	22	用於存取 Red Hat Enterprise Linux 命令列並檢索支援包。
MySQL 資料庫	MySQL	3306	用於啟用 OnCommand Workflow Automation 和 OnCommand API Services 對 Unified Manager 的存取。
系統日誌	UDP	514	用於從 ONTAP 系統存取基於訂閱的 EMS 訊息並根據這些訊息建立事件。
休息	HTTPS	9443	用於從經過驗證的 ONTAP 系統存取基於即時 REST API 的 EMS 事件。

介面	協定	港口	描述
MySQL 資料庫	MySQL	3306	用於啟用 OnCommand Workflow Automation 和 OnCommand API Services 對 Unified Manager 的存取。
AMQP QPID 代理	TCP/IP	56072	用於內部訊息通訊。
AMQP QPID 代理	透過 TCP 的 WebSocket	56080	用於在此連接埠上偵聽從 ONTAP (雲端代理) 接收的訊息。
AMQP QPID 代理	透過 TCP 的 WebSocket	56443	用於在此連接埠上偵聽從 ONTAP (雲端代理) 接收的訊息。透過此連接埠的通訊支援 TLS 或 SSL 提供的加密。



在 Linux 系統上安裝 Unified Manager 時，MySQL 的預設連接埠 3306 僅限於本機。這不會影響任何升級方案，因為先前的配置會保留。可以修改此配置，並且可以使用 `Control access to MySQL port 3306` 維護控制台上的選項。有關信息，請參閱["附加選單選項"](#)。可以使用 Unified Manager 維護控制台變更為用於 HTTP 和 HTTPS 通訊的連接埠 (連接埠 80 和 443)。有關詳細信息，請參閱["維護控制台選單"](#)。

來自 Unified Manager 伺服器的連接

您應該配置防火牆以開啟端口，以便 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間進行通訊。如果連接埠未打開，則通訊失敗。

根據您的環境，您可以選擇修改 Unified Manager 伺服器用於連接到特定目的地的連接埠和協定。

Unified Manager 伺服器使用下列協定和連接埠連接到託管儲存系統、伺服器和其他元件：

目的地	協定	港口	描述
儲存系統	HTTPS	443/TCP	用於監控和管理儲存系統。
儲存系統	NDMP	10000/TCP	用於某些快照復原操作。
AutoSupport 伺服器	HTTPS	443	用於發送 AutoSupport 資訊。需要網路存取才能執行此功能。

目的地	協定	港口	描述
身份驗證伺服器	LDAP	389	用於發出身份驗證請求以及使用者和群組查找請求。
LDAPS	636	用於安全 LDAP 通訊。	郵件伺服器
SMTP	25	用於發送警報通知電子郵件。	SNMP 陷阱發送器
SNMPv1 或 SNMPv3	162/UDP	用於發送警報通知 SNMP 陷阱。	外部資料提供伺服器
TCP	2003	用於將效能資料傳送至外部資料提供者，例如 Graphite。	NTP 伺服器
NTP	123/UDP	用於將 Unified Manager 伺服器上的時間與外部 NTP 時間伺服器同步。（僅限 VMware 系統）	系統日誌

完成工作表

在安裝和設定 Unified Manager 之前，您應該準備好有關您的環境的具體資訊。您可以在工作表中記錄該資訊。

Unified Manager 安裝訊息

安裝 Unified Manager 所需的詳細資訊。

部署軟體的系統	你的價值
主機完全限定域名	
主機 IP 位址	
網路遮罩	
網關 IP 位址	
主 DNS 位址	
輔助 DNS 位址	

部署軟體的系統	你的價值
搜尋域名	
維護用戶名	
維護用戶密碼	

Unified Manager 設定訊息

安裝後設定 Unified Manager 的詳細資訊。根據您的配置，某些值是可選的。

環境	你的價值
維護使用者電子郵件地址	
SMTP 伺服器主機名稱或 IP 位址	
SMTP使用者名稱	
SMTP 密碼	
SMTP 連接埠	25 (預設值)
發送警報通知的電子郵件	
身份驗證伺服器主機名稱或 IP 位址	
Active Directory 管理員名稱或 LDAP 綁定可分辨名稱	
Active Directory 密碼或 LDAP 綁定密碼	
認證伺服器基礎可分辨名稱	
身分識別提供者 (IdP) URL	
身分提供者 (IdP) 元資料	
SNMP 陷阱目標主機 IP 位址	
SNMP 連接埠	

集群資訊

使用 Unified Manager 管理的儲存系統的詳細資訊。

N 的簇 1	你的價值
主機名稱或叢集管理 IP 位址	
ONTAP 管理員使用者名稱  必須為管理員指派“admin”角色。	
ONTAP 管理員密碼	
協定	HTTPS

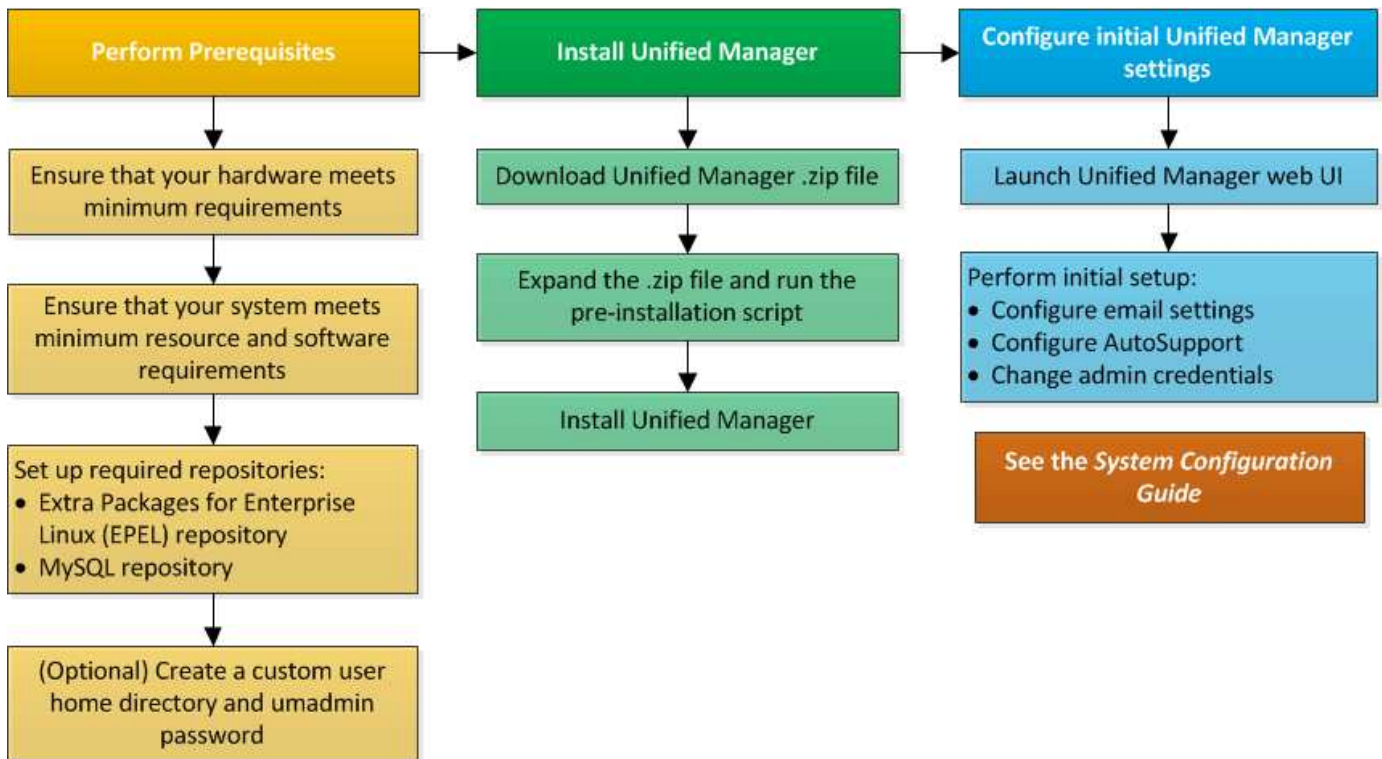
安裝、升級和刪除 Unified Manager 軟體

在 Linux 系統上，您可以安裝 Unified Manager 軟體、升級至較新版本的軟體或刪除 Unified Manager。

Unified Manager 可以安裝在 Red Hat Enterprise Linux 伺服器上。安裝 Unified Manager 的 Linux 伺服器可以在實體機器上運行，也可以在 VMware ESXi、Microsoft Hyper-V 或 Citrix XenServer 上運行的虛擬機器上運行。

安裝過程概述

安裝工作流程描述了您在使用 Unified Manager 之前必須執行的任務。



設定所需的軟體儲存庫

系統必須能夠存取某些儲存庫，以便安裝程式可以存取和安裝所有必要的軟體相依性。

手動配置 EPEL 儲存庫

如果您安裝 Unified Manager 的系統無法存取 Extra Packages for Enterprise Linux (EPEL) 儲存庫，則必須手動下載並設定儲存庫才能成功安裝。

EPEL 儲存庫提供對必須在您的系統上安裝的所需第三方實用程式的存取。您可以使用 EPEL 儲存庫在 Red Hat Enterprise Linux 系統上安裝 Unified Manager。

步驟

1. 下載用於安裝的 EPEL 儲存庫。對於版本 8，請從以下位置下載：

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

對於版本 9，請從以下位置下載：

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

2. 配置 EPEL 儲存庫：

```
yum install epel-release-latest-<version>.noarch.rpm
```

對於 Red Hat Enterprise Linux 8 系統，如果您有包含模組化 RPM 套件的內部儲存庫，例如，`javapackages-filessystem-<version>.module.rpm`，確保模組化包的元資料也可在同一個儲存庫中使用。

手動設定 MySQL 儲存庫

如果您安裝 Unified Manager 的系統無法存取 MySQL 社群版儲存庫，則必須手動下載並設定儲存庫才能成功安裝。

MySQL 儲存庫提供對必須安裝在您的系統上的所需 MySQL 軟體的存取。



如果系統沒有網路連接，此任務可能會失敗。如果您安裝 Unified Manager 的系統無法存取互聯網，請參閱 MySQL 文件。

步驟

1. 下載適合您的安裝的 MySQL 儲存庫。對於版本 8，請從以下位置下載：

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/8/x86_64/mysql84-community-release-el8-1.noarch.rpm
```

對於版本 9，請從以下位置下載：

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/9/x86_64/mysql84-community-release-el9-1.noarch.rpm
```

2. 配置 MySQL 儲存庫：

```
yum install mysql84-community-release-.noarch.rpm
```

對於 Red Hat Enterprise Linux 8 系統，如果您有包含 java-11-openjdk、p7zip 以及 AppStream 儲存庫提供的其他軟體包的內部儲存庫，則必須停用您的 AppStream 儲存庫並安裝 MySQL Community Server。運行以下命令：

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install mysql-community-server
```

如果您收到缺少密鑰或密鑰不匹配的錯誤，並且安裝失敗，請嘗試以下步驟：

- 在連接的系統上，透過執行下列命令匯入更新的 MySQL 金鑰：

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>  
  
for example:  
  
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```

- 在沒有網路連線的系統上，更新 MySQL repo 檔案並停用 gpgcheck 透過標記 `gpgcheck=0`。

NFS 和 CIFS 共享上的 SELinux 要求

如果您打算安裝 `/opt/netapp` 或者 `/opt/netapp/data` 在 NAS 或 SAN 設備上，並且啟用了 SELinux，您需要注意一些事項。

如果您打算安裝 `/opt/netapp` 或者 `/opt/netapp/data` 從根檔案系統以外的任何地方，並且您的環境中啟用了 SELinux，您應該為已掛載的目錄設定正確的上下文。對於您環境中的適用場景，請依照下列步驟設定並確認正確的 SELinux 上下文。

配置 SELinux 上下文 `/opt/netapp/data` 已安裝

如果您已安裝 `/opt/netapp/data` 在您的系統中，SELinux 設定為 `Enforcing`，確保 SELinux 上下文類型為 `/opt/netapp/data` 設定為 `mysqld_db_t`，這是資料庫檔案位置的預設上下文元素。

1. 運行此命令來檢查上下文：

```
ls -dZ /opt/netapp/data
```

範例輸出：

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
/opt/netapp/data
```



在此輸出中，上下文是 `default_t`。您應該將此上下文變更為 `mysqld_db_t`。

2. 執行以下步驟，根據您安裝的方式設定上下文 `/opt/netapp/data`。

- a. 運行以下命令將上下文設定為 `mysqld_db_t`：

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```

- b. 如果您已配置 `/opt/netapp/data` 在 `/etc/fstab`，你應該編輯 `/etc/fstab` 文件。對於 `/opt/netapp/data` 的 `mount` 選項，新增 MySQL 標籤為：

```
context=system_u:object_r:mysqld_db_t:s0
```

- c. 解除安裝並重新安裝 `/opt/netapp/data` 用於啟用上下文。

- d. 如果您有直接 NFS 掛載，請執行下列命令將上下文設為 `mysqld_db_t`：

```
mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
context=system_u:object_r:mysqld_db_t:s0
```

3. 驗證上下文是否設定正確：

```
ls -dZ /opt/netapp/data/
```

範例輸出：

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqldb_t:s0
/opt/netapp/data/
```

配置 SELinux 上下文 `/opt/netapp` 已安裝，並且 `/opt/netapp/data` 也單獨安裝

在這種情況下，首先，你應該設定上下文 `/opt/netapp/data/` 如上一節所述。在設定正確的上下文之後 `/opt/netapp/data/`，確保父目錄 `/opt/netapp` 沒有將 SELinux 上下文設定為 `file_t`。

步驟

1. 運行此命令來檢查上下文：

```
ls -dZ /opt/netapp
```

範例輸出：

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

在此輸出中，上下文是 `file_t` 應該改變。以下命令將上下文設定為 `usr_t`。您可以將上下文設定為除 `file_t` 根據您的安全要求。

2. 根據您安裝的方式執行以下步驟來設定上下文 `/opt/netapp`。

- a. 執行以下命令來設定上下文：

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. 如果您已配置 `/opt/netapp` 在 `/etc/fstab`，你應該編輯 `/etc/fstab` 文件。對於 `/opt/netapp` mount 選項，新增 MySQL 標籤為：

```
context=system_u:object_r:usr_t:s0
```

2. 卸載，然後重新安裝 `/opt/netapp` 用於啟用上下文。
3. 如果您有直接 NFS 掛載，請執行下列命令來設定上下文：

```
mount <nfsshare>:<mountpoint> /opt/netapp -o
context=system_u:object_r:usr_t:s0
```

- a. 驗證上下文是否設定正確：

```
ls -dZ /opt/netapp
```

範例輸出

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

配置 SELinux 上下文 `/opt/netapp` 已安裝，並且 `/opt/netapp/data/` 不單獨安裝

如果您已安裝 `/opt/netapp` 在您的系統中，SELinux 設定為 `Enforcing`，確保 SELinux 上下文類型為 `/opt/netapp` 設定為 `mysql_d_b_t`，這是資料庫檔案位置的預設上下文元素。

步驟

1. 運行此命令來檢查上下文：

```
ls -dZ /opt/netapp
```

範例輸出：

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
```



在此輸出中，上下文是 `default_t`。您應該將此上下文變更為 `mysql_d_b_t`。

2. 執行以下步驟，根據您安裝的方式設定上下文 `/opt/netapp`。

- a. 運行以下命令將上下文設定為 `mysql_d_b_t`：

```
semanage fcontext -a -t mysql_d_b_t "/opt/netapp"  
`restorecon -R -v /opt/netapp
```

- b. 如果您已配置 `/opt/netapp` 在 `/etc/fstab`，編輯 `/etc/fstab` 文件。對於 `/opt/netapp/`mount` 選項，新增 MySQL 標籤為：
``context=system_u:object_r:mysql_d_b_t:s0`

- c. 卸載，然後重新安裝 `/opt/netapp/` 用於啟用上下文。

- d. 如果您有直接 NFS 掛載，請執行下列命令將上下文設為 `mysql_d_b_t`：

```
mount <nfsshare>:<mountpoint> /opt/netapp -o  
context=system_u:object_r:mysql_d_b_t:s0
```

3. 驗證上下文是否設定正確：

```
ls -dZ /opt/netapp/
```

範例輸出：

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_d_b_t:s0 /opt/netapp/
```

在 Linux 系統上安裝 Unified Manager

重要的是，您要了解下載和安裝 Unified Manager 的步驟順序會根據您的安裝場景而有所不同。

在安裝之前建立自訂使用者主目錄和 **umadmin** 密碼

您可以在安裝 Unified Manager 之前建立自訂主目錄並定義自己的 umadmin 使用者密碼。此任務是可選的，但某些網站可能需要靈活地覆寫 Unified Manager 安裝預設設定。

開始之前

- 系統必須滿足"[硬體系統需求](#)"。
- 您必須能夠以 root 使用者身分登入 Red Hat Enterprise Linux 系統。

預設 Unified Manager 安裝執行下列任務：

- 使用以下命令建立 umadmin 用戶 `/home/umadmin` 作為主目錄。
- 為 umadmin 使用者指派預設密碼「admin」。

由於某些安裝環境限制訪問 `/home`，安裝失敗。您必須在不同位置建立主目錄。此外，某些網站可能有關於密碼複雜性的規則，或要求密碼由本機管理員設置，而不是由安裝程式設定。

如果您的安裝環境要求您覆寫這些安裝預設設置，請按照下列步驟建立自訂主目錄並定義 umadmin 使用者的密碼。

如果在安裝之前定義了這些訊息，安裝腳本就會發現這些設定並使用定義的值，而不是使用安裝預設設定。

此外，預設的 Unified Manager 安裝在 `sudoers` 檔案中包含 umadmin 用戶 (`ocum_sudoers` 和 `ocie_sudoers`) 在 `/etc/sudoers.d/` 目錄。如果您因為安全性原則或某些安全監控工具而從您的環境中刪除了此內容，則必須將其加回。您需要保留 `sudoers` 配置，因為某些 Unified Manager 操作需要這些 `sudo` 權限。

您環境中的安全性策略不得限制 Unified Manager 維護使用者的 `sudo` 權限。如果權限受到限制，某些 Unified Manager 操作可能會失敗。驗證安裝成功後以 umadmin 使用者登入時是否能夠執行以下 `sudo` 命令。

```
sudo systemctl status ocie
```

此命令應傳回 `ocie` 服務的適當狀態，且不會出現任何錯誤。

步驟

1. 以 root 使用者身分登入伺服器。
2. 建立名為「maintenance」的 umadmin 群組帳戶：

```
groupadd maintenance
```

3. 在您選擇的主目錄下的維護群組中建立使用者帳戶「umadmin」：

```
adduser --home <home_directory> -g maintenance umadmin
```

4. 定義 umadmin 密碼：

```
passwd umadmin
```

系統提示您輸入 umadmin 使用者的新密碼字串。

安裝 Unified Manager 後，您必須指定 umadmin 使用者登入 shell。

下載 Unified Manager

您必須下載 Unified Manager `.zip` 檔案從 NetApp 支援網站安裝 Unified Manager。

開始之前

您必須擁有 NetApp 支援網站的登入憑證。

下載適用於 Red Hat Enterprise Linux 系統的 Unified Manager 安裝套件。

步驟

1. 登入 NetApp 支援站點，然後導覽至 Unified Manager 的下載頁面：

["NetApp 支援站點"](#)

2. 選擇所需版本的 Unified Manager 並接受最終使用者授權協議 (EULA)。
3. 下載適用於 Linux 的 Unified Manager 安裝程式文件，並儲存 `.zip` 檔案複製到目標系統上的目錄。



- 確保您為您的 Red Hat Enterprise Linux 系統下載了正確版本的安裝程式檔案。根據您是否安裝了 Red Hat Enterprise Linux 8 或 9，請確保下載適當版本的 Unified Manager `.zip` 文件。
- NetApp 建議您下載程式碼簽署證書 (`.pem`) 和數位簽名 (`.sig`) 以及 `.zip` 文件。

4. 驗證下載軟體的完整性校驗和。
5. 如果您已經下載了程式碼簽名憑證和數位簽名，您可以驗證安裝程式檔案的完整性。您可以使用以下命令來驗證安裝程式檔案的完整性：
 - 此命令使用程式碼簽署憑證中的公鑰建立一個檔案：

```
openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >  
<public_key_file_name>
```

- 其中 **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** 是包含代碼簽署憑證的檔案。

- 此命令驗證安裝程式檔案上的簽名：

```
openssl dgst -sha256 -verify <public_key_file_name> -signature  
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

類似於以下的訊息 `Verified Ok` 確認安裝程式檔案可以安全使用。

安裝 Unified Manager

您可以在實體或虛擬 Red Hat Enterprise Linux 平台上安裝 Unified Manager。

開始之前

- 您要安裝 Unified Manager 的系統必須符合系統和軟體需求。

看["硬體系統需求"](#)。

看["Linux 軟體和安裝需求"](#)。

- 您必須已下載 Unified Manager `.zip` 檔案從 NetApp 支援網站複製到目標系統。
- 您應該已經驗證了下載的 `.zip` 文件。
- 您必須擁有受支援的 Web 瀏覽器。
- 您的終端模擬軟體必須啟用回溯功能。

Red Hat Enterprise Linux 系統可能安裝了所有必要的支援軟體（Java、MySQL、附加實用程式）的必要版本，可能只安裝了部分必要的軟體，或者可能是新安裝的系統，沒有安裝任何必要的軟體。

步驟

1. 登入要安裝 Unified Manager 的伺服器。
2. 輸入適當的命令來評估哪些軟體可能需要在目標系統上安裝或升級以支援安裝：

所需軟體和最低版本	驗證軟體和版本的命令
OpenJDK 版本 11.0.25	<code>java -version</code>
MySQL 8.4.4 社群版	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

3. 如果安裝的 MySQL 版本低於 MySQL 8.4.4 社群版，請輸入下列指令進行解除安裝：

```
rpm -e <mysql_package_name>
```

如果收到依賴性錯誤，則必須新增 `--nodeps`` 卸載組件的選項。

4. 導航至下載安裝的目錄 `.zip`` 檔案並展開 Unified Manager 套裝組合：

```
unzip ActiveIQUnifiedManager-<version>.zip
```

所需的 `.rpm`` Unified Manager 的模組解壓縮到目標目錄。

5. 驗證目錄中是否有以下模組：

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

6. 執行預先安裝腳本以確保沒有系統設定設定或任何可能與 Unified Manager 安裝衝突的已安裝軟體：

```
sudo ./pre_install_check.sh
```

預先安裝腳本檢查系統是否有有效的 Red Hat Enterprise Linux 訂閱，以及是否可以存取所需的軟體儲存庫。如果腳本發現任何問題，則必須在安裝 Unified Manager 之前修復這些問題。

對於 Red Hat Enterprise Linux 8 系統，如果您有帶有 JDK 11 的內部儲存庫 - OpenJDK、p7zip 和 AppStream 儲存庫提供的其他軟體包，則必須停用您的 AppStream 儲存庫並安裝 MySQL Community Server。運行以下命令：

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
mysql-community-server
```

7. *可選：*只有當您的系統未連接到互聯網並且必須手動下載安裝所需的軟體包時，您才必須執行步驟 7。如果您的系統可以存取網路並且所有必需的軟體包都可用，請前往步驟 8。對於未連接到網際網路或未使用 Red Hat Enterprise Linux 儲存庫的系統，請執行下列步驟來確定是否缺少任何所需的軟體包，然後下載這些軟體包：

- a. 在安裝 Unified Manager 的系統上，檢視可用和不可用軟體套件的清單：

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

「安裝：」部分中的項目是目前目錄中可用的軟體包，「安裝依賴項：」部分中的項目是系統中缺少的軟體包。

- b. 在可以存取網路的系統上，下載缺少的軟體包：

```
yum install <package_name> --downloadonly --downloaddir=.
```



由於外掛程式「yum-plugin-downloadonly」在 Red Hat Enterprise Linux 系統上並不總是啟用的，您可能需要啟用該功能來下載軟體包而不安裝它：

```
yum install yum-plugin-downloadonly
```

- a. 將缺少的軟體包從網路連線的系統複製到您的安裝系統。

8. 以 root 使用者身份，或使用 sudo，執行以下命令安裝軟體：

```
yum install netapp-um<version>.x86_64.rpm
```

此命令安裝 .rpm 軟體包、所有其他必要的支援軟體以及 Unified Manager 軟體。

如果安裝失敗並出現 GPG NOKEY 錯誤，請使用 `rpm --import` 從 URL 匯入金鑰：

```
rpm --導入 https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```



不要嘗試使用其他命令進行安裝（例如 `rpm -ivh`）。在 Red Hat Enterprise Linux 系統上成功安裝 Unified Manager 要求所有 Unified Manager 檔案和相關檔案都依照特定順序安裝到由 `yum install netapp-um<version>.x86_64.rpm` 命令。

9. 忽略安裝訊息後立即顯示的電子郵件通知。

該電子郵件通知 root 使用者初始 cron 作業失敗，但這對安裝沒有不利影響。

10. 安裝訊息完成後，向後捲動訊息，直到看到系統顯示 Unified Manager Web UI 的 IP 位址或 URL、維護使用

者名稱 (umadmin) 和預設密碼的訊息。

該訊息類似於以下內容：

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/      (if using IPv4)
https://[default_ip_address]/    (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. 記錄 IP 位址或 URL、指派的使用者名稱 (umadmin) 和目前密碼。
12. 如果您在安裝 Unified Manager 之前建立了具有自訂主目錄的 umadmin 使用者帳戶，則必須指定 umadmin 使用者登入 shell：

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

存取 Web UI 以變更 umadmin 使用者的預設密碼，並執行 Unified Manager 的初始設置，如中所述"[配置Active IQ Unified Manager](#)"。必須更改 umadmin 使用者的預設密碼。

Unified Manager 安裝期間建立的使用者

在 Red Hat Enterprise Linux 上安裝 Unified Manager 時，Unified Manager 和第三方公用程式會建立下列使用者：umadmin、jboss 和 mysql。

- **umadmin**

用於首次登入 Unified Manager。該使用者被指派了「應用程式管理員」使用者角色，並配置為「維護使用者」類型。此使用者由 Unified Manager 建立。

- **jboss**

用於執行與 JBoss 公用程式相關的 Unified Manager 服務。此使用者由 Unified Manager 建立。

- **mysql**

用於執行 Unified Manager 的 MySQL 資料庫查詢。該用戶由 MySQL 第三方實用程式創建。

除了這些使用者之外，Unified Manager 還建立了對應的群組：maintenance、jboss 和 mysql。維護和 jboss 群組由 Unified Manager 創建，而 mysql 群組由第三方實用程式建立。



如果您在安裝 Unified Manager 之前建立了自訂主目錄並定義了自己的 umadmin 使用者密碼，則安裝程式不會重新建立維護群組或 umadmin 使用者。

更改 JBoss 密碼

您可以重設安裝期間設定的特定於實例的 JBoss 密碼。如果您的網站需要此安全功能來覆寫 Unified Manager 安裝設置，您可以選擇重設密碼。此操作也會更改 JBoss 用於存取 MySQL 的密碼。

- 您必須具有安裝 Unified Manager 的 Red Hat Enterprise Linux 系統的 root 使用者存取權。
- 您必須能夠存取 NetApp 提供的 password.sh 目錄中的腳本 `/opt/netapp/essentials/bin`。

步驟

1. 以 root 使用者登入系統。
2. 以所示順序輸入以下指令來停止 Unified Manager 服務：

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

不要停止相關的 MySQL 軟體。

3. 輸入以下命令開始密碼更改程序：

```
/opt/netapp/essentials/bin/password.sh resetJBossPassword
```

4. 出現提示時，輸入新的 JBoss 密碼，然後再次輸入以進行確認。

請注意，密碼應介於 8 到 16 個字元之間，並且必須至少包含一個數字、一個大寫字母和一個小寫字母，以及至少一個以下特殊字元：

```
!@%^*-_=[]:<>./~+
```

5. 腳本完成後，按所示順序輸入以下命令來啟動 Unified Manager 服務：

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. 所有服務啟動後，您可以登入 Unified Manager UI。

在 Red Hat Enterprise Linux 上升級 Union Manager

當有新版本可用時，您可以升級 Unified Manager。

當 NetApp 提供 Unified Manager 軟體的修補程式版本時，其安裝流程與新版本相同。

如果 Unified Manager 與 OnCommand Workflow Automation 實例配對，且這兩種產品都有新版本的軟體可用，則必須中斷這兩種產品的連接，然後在執行升級後建立新的 Workflow Automation 連接。如果您只對其中一個產品進行升級，則應在升級後登入工作流程自動化並驗證它是否仍在從 Unified Manager 取得資料。

Unified Manager 版本支援的升級路徑

Active IQ Unified Manager 支援每個版本的特定升級路徑。

並非所有版本的 Unified Manager 都可以執行就地升級到更高版本。Unified Manager 升級僅限於 N-2 型號，這表示升級只能在所有平台上的下 2 個版本內進行。例如，您只能從 Unified Manager 9.13 和 9.14 升級到 Unified Manager 9.16。

如果您執行的版本早於支援的版本，則需要先将 Unified Manager 實例升級到支援的版本之一，然後再升級至目前版本。

例如，如果您安裝的版本是 Unified Manager 9.9，並且您想要升級到 Unified Manager 9.14，請遵循一系列升級作業。

升級路徑範例：

1. 升級 9.11 → 9.13
2. 升級 9.13 → 9.14
3. 升級 9.13 → 9.16
4. 升級 9.14 → 9.16

有關升級路徑矩陣的更多信息，請參閱 ["知識庫 \(KB\) 文章"](#)。

升級 Unified Manager

您可以透過在 Linux 平台上下載並執行安裝檔案從 Unified Manager 9.13 或 9.14 升級到 9.16。

開始之前

- 要升級 Unified Manager 的系統必須符合系統和軟體需求。

看 ["硬體系統需求"](#)。

看 ["Linux 軟體和安裝需求"](#)。

- 您必須訂閱 Red Hat Enterprise Linux 訂閱管理員。
- 在升級 Unified Manager 之前，您必須安裝或升級到正確版本的 OpenJDK。

看 ["在 Linux 上升級 JRE"](#)。

- 為避免資料遺失，您必須建立 Unified Manager 資料庫的備份，以防升級期間出現問題。NetApp 建議您將備份檔案從 `/opt/netapp/data` 目錄到外部位置。
- 升級過程中，系統可能會提示您確認是否要保留先前的預設設定（即保留效能資料 13 個月）或將其變更為 6 個月。確認後，歷史績效數據將在 6 個月後清除。
- 您應該已經完成所有正在執行的操作，因為 Unified Manager 在升級過程中不可用。
- MySQL 社群版會在 Unified Manager 升級期間自動升級。如果您系統上安裝的 MySQL 版本早於 8.4.4，則 Unified Manager 升級過程會自動將 MySQL 升級到 8.4.4。

步驟

1. 登入目標 Red Hat Enterprise Linux 伺服器。
2. 將 Unified Manager 套裝組合下載到伺服器。

看"下載適用於 Linux 的 Unified Manager"。

3. 導覽至目標目錄並展開 Unified Manager 套件：

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Unified Manager 所需的 RPM 模組已解壓縮到目標目錄。

4. 驗證目錄中是否有以下模組：

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

5. 執行預先安裝腳本以確保沒有系統設定設定或任何可能與升級衝突的已安裝軟體：

```
sudo ./pre_install_check.sh
```

預先安裝腳本檢查系統是否有有效的 Red Hat Enterprise Linux 訂閱，以及是否可以存取所需的軟體儲存庫。如果腳本發現任何問題，您必須修復這些問題並繼續升級。

如果偵測到任何缺少的包，請執行"遺失包裹時需要執行的額外步驟"。如果沒有遺失任何包，請繼續下一個步驟。

6. 使用以下腳本升級 Unified Manager：

```
upgrade.sh
```

此腳本會自動執行 RPM 模組，升級必要的支援軟體和在其上執行的 Unified Manager 模組。此外，升級腳本還會檢查是否有任何系統配置設定或任何已安裝的軟體可能與升級相衝突。如果腳本發現任何問題，則必須在升級 Unified Manager 之前修復這些問題。如果您在升級 Unified Manager 之前安裝了軟體套件（例如 *net-snmp*），則 MySQL 依賴項可能會在升級過程中解除安裝該軟體套件。您需要再次手動安裝該套件才能繼續使用它。

7. 升級完成後，向後捲動訊息，直到看到顯示 Unified Manager Web UI 的 IP 位址或 URL、維護使用者名稱 (umadmin) 和預設密碼的訊息。

該訊息類似於以下內容：

```
Active IQ Unified Manager upgraded successfully.
Use a web browser and one of the following URLs to access the Unified
Manager GUI:
```

```
https://default_ip_address/      (if using IPv4)
```

```
https://[default_ip_address]/    (if using IPv6)
```

```
https://fully_qualified_domain_name/
```

在支援的 Web 瀏覽器的新視窗中輸入指定的 IP 位址或 URL 以啟動 Unified Manager Web UI，然後使用您先前設定的相同維護使用者名稱 (umadmin) 和密碼登入。

遺失包裹時需要執行的額外步驟

如果在升級過程中偵測到您的網站缺少任何軟體包，或者您的系統未連接到互聯網，或者您沒有使用 Red Hat Enterprise Linux 儲存庫，請執行以下步驟來確定是否缺少任何所需的軟體包並下載這些軟體包。



這些步驟需要在主程式的步驟_5_之後執行。此程序將升級 Unified Manager，您無需執行任何其他升級步驟。

1. 查看可用和不可用套件的清單：

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

「安裝：」部分中的項目是目前目錄中可用的軟體包，「安裝依賴項：」部分中的項目是系統中缺少的軟體包。

2. 在具有網路存取權限的其他系統上，執行以下命令來下載缺少的軟體包。

```
yum install package_name --downloadonly --downloaddir=.
```

軟體包下載到指定的目錄中 --downloaddir=。

由於外掛程式「yum-plugin-downloadonly」在 Red Hat Enterprise Linux 系統上並不總是啟用的，您可能需要啟用該功能來下載軟體包而不安裝它：

```
yum install yum-plugin-downloadonly
```

3. 將下載的軟體包複製到安裝系統上解壓縮 Unified Manager 套件的目錄。
4. 將目錄變更為該目錄並執行以下命令來安裝缺少的軟體包及其相依性。

```
yum install *.rpm
```

5. 啟動 Unified Manager 伺服器。運行以下命令：

```
systemctl start ocie
```

```
systemctl start ocieau
```

此程序完成 Unified Manager 升級程序。在支援的 Web 瀏覽器的新視窗中輸入指定的 IP 位址或 URL 以啟動 Unified Manager Web UI，然後使用您先前設定的相同維護使用者名稱 (umadmin) 和密碼登入。

將主機作業系統從 **Red Hat Enterprise Linux 7.x** 升級到 **8.x**

如果您先前在 Red Hat Enterprise Linux 7.x 系統上安裝了 Unified Manager，並且需要升級至 Red Hat Enterprise Linux 8.x，則必須遵循本主題中所列的步驟之一。在這兩種情況下，您都必須在 Red Hat Enterprise Linux 7.x 系統上建立 Unified Manager 的備份，然後將備份還原到 Red Hat Enterprise Linux 8.x 系統上。請注意，Red Hat Enterprise Linux 支援的版本是從 8.0 到 8.10。

下面列出的兩個選項之間的差異在於，在一種情況下，您正在將 Unified Manager 還原到新的 8.x 伺服器上，而在另一種情況下，您正在在同一台伺服器上執行還原操作。

由於此任務要求您在 Red Hat Enterprise Linux 7.x 系統上建立 Unified Manager 的備份，因此您應該只在準備完成整個升級程序時才建立備份，以便 Unified Manager 在最短的時間內處於離線狀態。在 Red Hat Enterprise Linux 7.x 系統關閉期間和新 Red Hat Enterprise Linux 8.x 啟動之前的一段時間內，Unified Manager UI 中收集的資料會出現缺口。

看"[管理備份和復原作業](#)"如果您需要查看備份和復原過程的詳細說明。

如果您有一個備用系統，可以在其中安裝 Red Hat Enterprise Linux 8.x 軟體，請按照下列步驟操作，以便在 Red Hat Enterprise Linux 7.x 系統仍然可用時可以在該系統上執行 Unified Manager 還原。

1. 使用 Red Hat Enterprise Linux 8.x 軟體安裝和設定新伺服器。

看"[Linux 軟體和安裝需求](#)"。

2. 在 Red Hat Enterprise Linux 8.x 系統上，安裝與現有 Red Hat Enterprise Linux 7.x 系統上相同版本的 Unified Manager 軟體。

看"[在 Linux 上安裝 Unified Manager](#)"。

安裝完成後，請勿啟動 UI 或設定任何叢集、使用者或身份驗證設定。備份檔案在復原過程中填入此資訊。

3. 在 Red Hat Enterprise Linux 7.x 系統上，從 Web UI 中的管理選單建立 Unified Manager 備份，然後複製備份文件(.7z`文件) 和資料庫儲存庫目錄的內容 (/database-dumps-repo`子目錄) 複製到外部位置。
4. 在 Red Hat Enterprise Linux 7.x 系統上，關閉 Unified Manager。
5. 在 Red Hat Enterprise Linux 8.x 系統上，複製備份文件(.7z`文件) 從外部位置到 `/opt/netapp/data/ocum-backup/` 以及資料庫儲存庫文件 `/database-dumps-repo` 下的子目錄 `/ocum-backup` 目錄。
6. 輸入以下指令從備份檔案還原 Unified Manager 資料庫：

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. 在您的 Web 瀏覽器中輸入 IP 位址或 URL 以啟動 Unified Manager Web UI，然後登入系統。

一旦您驗證系統正常運作，您就可以從 Red Hat Enterprise Linux 7.x 系統中刪除 Unified Manager。

在同一台伺服器上升級主機作業系統

如果您沒有可以安裝 Red Hat Enterprise Linux 8.x 軟體的備用系統，請依照下列步驟操作。

1. 從 Web UI 中的管理選單，建立 Unified Manager 備份，然後複製備份文件(.7z`文件) 和資料庫儲存庫目錄的內容 (/database-dumps-repo`子目錄) 複製到外部位置。
2. 從系統中刪除 Red Hat Enterprise Linux 7.x 映像並徹底清除系統。
3. 在同一系統上安裝並設定 Red Hat Enterprise Linux 8.x 軟體。

看"[Linux 軟體和安裝需求](#)"。

4. 在 Red Hat Enterprise Linux 8.x 系統上，安裝與 Red Hat Enterprise Linux 7.x 系統上相同版本的 Unified Manager 軟體。

看"[在 Linux 上安裝 Unified Manager](#)"。

安裝完成後，請勿啟動 UI 或設定任何叢集、使用者或身份驗證設定。備份檔案在復原過程中填入此資訊。

5. 複製備份文件（.7z 文件）從外部位置到 `/opt/netapp/data/ocum-backup/` 以及資料庫儲存庫文件 `/database-dumps-repo` 下的子目錄 `/ocum-backup` 目錄。
6. 輸入以下指令從備份檔案還原 Unified Manager 資料庫：

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. 在您的 Web 瀏覽器中輸入 IP 位址或 URL 以啟動 Unified Manager Web UI，然後登入系統。

安裝 Unified Manager 後升級第三方產品

當 Unified Manager 已安裝在 Linux 系統上時，您可以升級第三方產品，例如 JRE。

開發這些第三方產品的公司會定期報告安全漏洞。您可以按照自己的時間表升級到該軟體的較新版本。

在 Linux 上升級 OpenJDK

您可以在安裝了 Unified Manager 的 Linux 伺服器上升級到較新版本的 OpenJDK，以取得安全漏洞的修復。

開始之前

您必須擁有安裝 Unified Manager 的 Linux 系統的 root 權限。

您可以在發行系列中更新 OpenJDK 版本。例如，您可以從 OpenJDK 11.0.14 升級到 OpenJDK 11.0.17，但不能直接從 OpenJDK 11 更新到 OpenJDK 12。

步驟

1. 以 root 使用者身分登入 Unified Manager 主機。
2. 將適當版本的 OpenJDK（64 位元）下載到目標系統。
3. 停止 Unified Manager 服務：

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

4. 在系統上安裝最新的 OpenJDK。
5. 啟動 Unified Manager 服務：

```
systemctl start ocie
```

```
systemctl start ocieau
```

重新啟動 Unified Manager

更改配置後，您可能需要重新啟動 Unified Manager。

開始之前

您必須具有安裝了 Unified Manager 的 Red Hat Enterprise Linux 伺服器的 root 使用者存取權。

步驟

1. 以 root 使用者身分登入要重新啟動 Unified Manager 服務的伺服器。
2. 依下列順序停止 Unified Manager 服務和關聯的 MySQL 服務：

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. 依照下列順序啟動 MySQL 和 Unified Manager 服務：

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



‘mysqld’是啟動和停止 MySQL 伺服器所需的守護程序。

刪除 Unified Manager

您可以使用單一指令從 Red Hat Enterprise Linux 主機停止並解除安裝 Unified Manager。

開始之前

- 您必須具有要從中刪除 Unified Manager 的伺服器的 root 使用者存取權限。
- 必須在 Linux 系統上停用安全增強 Linux (SELinux)。使用下列命令將 SELinux 運行時模式變更為“Permissive” `setenforce 0` 命令。
- 在刪除該軟體之前，必須從 Unified Manager 伺服器中刪除所有叢集（資料來源）。
- 您應該手動刪除為允許或封鎖 MySQL 連接埠 3306 而建立的防火牆規則。防火牆規則不會被自動刪除。

步驟

1. 以 root 使用者身分登入要刪除 Unified Manager 的伺服器。
2. 停止並從伺服器中刪除 Unified Manager：

```
rpm -e netapp-um
```

此步驟將移除所有相關的 NetApp RPM 軟體包。它不會刪除必備的軟體模組，例如 Java、MySQL 和 p7zip。

3. *可選：*如果適用，請移除支援軟體模組，例如 Java、MySQL 和 p7zip：

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-  
common mysql-community-libs java-x.y
```

此操作完成後，軟體將被刪除。所有數據來自 `/opt/netapp/data` 目錄被移動到 `/opt/netapp/data/BACKUP` 卸載後的資料夾。卸載 Unified Manager 也會刪除 Java 和 MySQL 軟體包，除非系統上的任何其他應用程式需要並使用這些軟體包。但是，MySQL 資料不會被刪除。

刪除自訂 **umadmin** 使用者和維護群組

如果您在安裝 Unified Manager 之前建立了自訂主目錄來定義您自己的 **umadmin** 使用者和維護帳戶，則應在解除安裝 Unified Manager 後刪除這些項目。

標準 Unified Manager 卸載不會刪除自訂的 **umadmin** 使用者和維護帳戶。您必須手動刪除這些項目。

步驟

1. 以 root 使用者登入 Red Hat Enterprise Linux 伺服器。
2. 刪除 **umadmin** 用戶：

```
userdel umadmin
```

3. 刪除維護組：

```
groupdel maintenance
```


在 Windows 系統上安裝 Unified Manager

Active IQ Unified Manager簡介

Active IQ Unified Manager（以前稱為OnCommand Unified Manager）可讓您從單一介面監控和管理ONTAP儲存系統的運作狀況和效能。您可以在 Linux 伺服器、Windows 伺服器上部署 Unified Manager，也可以將其作為虛擬裝置部署在 VMware 主機上。

完成安裝並新增要管理的叢集後，Unified Manager 將提供一個圖形介面，顯示受監控儲存系統的容量、可用性、保護和效能狀態。

相關資訊

["NetApp互通性表工具"](#)

Unified Manager 伺服器的功能

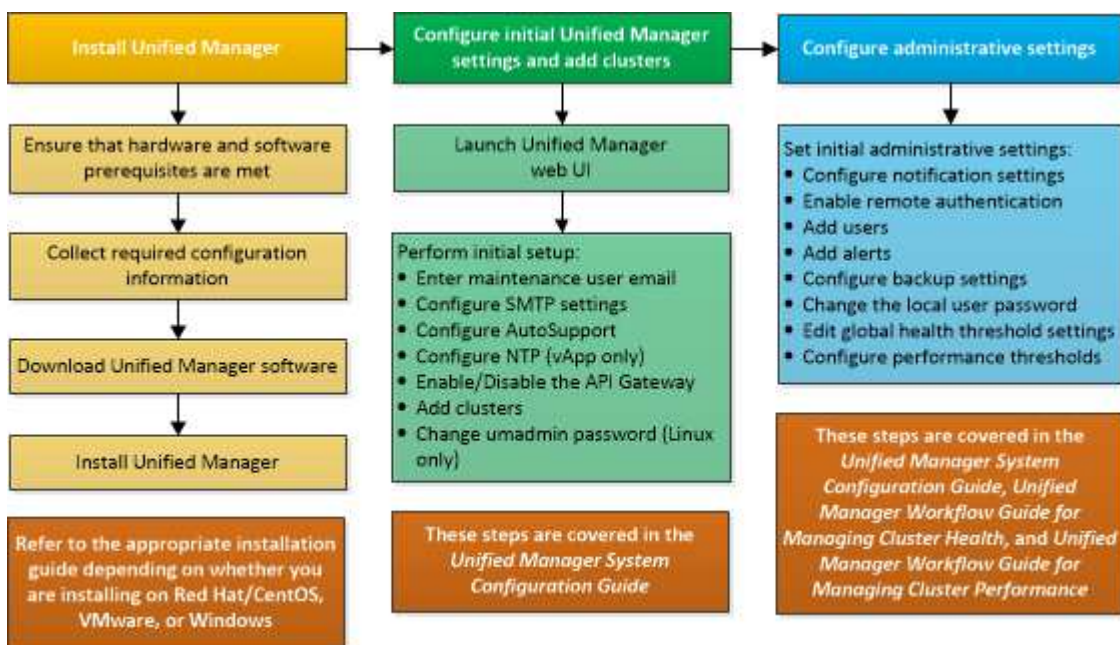
Unified Manager 伺服器基礎架構由資料收集單元、資料庫和應用程式伺服器組成。它提供發現、監控、基於角色的存取控制 (RBAC)、稽核和日誌記錄等基礎設施服務。

Unified Manager 收集叢集信息，將資料儲存在資料庫中，並分析資料以查看是否存在任何叢集問題。

安裝順序概述

安裝工作流程描述了您在使用 Unified Manager 之前必須執行的任務。

這些部分描述了下面工作流程中顯示的每個項目。



安裝 Unified Manager 的要求

在開始安裝程序之前，請確保您要安裝 Unified Manager 的伺服器符合特定的軟體、硬體、CPU 和記憶體需求。

NetApp不支援對 Unified Manager 應用程式程式碼進行任何修改。如果您需要對 Unified Manager 伺服器套用任何安全措施，則應對安裝 Unified Manager 的作業系統進行這些變更。

有關將安全措施應用於 Unified Manager 伺服器的更多詳細信息，請參閱知識庫文章。

["適用於叢集模式Data ONTAP的Active IQ Unified Manager的安全措施的可支援性"](#)

相關資訊

["NetApp互通性表工具"](#)

虛擬基礎架構和硬體系統需求

在虛擬基礎架構或實體系統上安裝 Unified Manager 應滿足記憶體、CPU 和磁碟空間的最低要求。

下表顯示了記憶體、CPU 和磁碟空間資源的建議值。這些值已經過限定，因此 Unified Manager 滿足可接受的效能水準。

硬體配置	推薦設定
記憶體	12 GB (最低要求 8 GB)
處理器	4 個 CPU
CPU 週期容量	總計 9572 MHz (最低需求 9572 MHz)
可用磁碟空間	150GB，容量分配如下： <ul style="list-style-type: none">• 100 GB 磁碟空間用於安裝目錄• 50 GB 磁碟空間用於 MySQL 資料目錄

Unified Manager 可以安裝在具有少量記憶體的系統上，但建議使用 12 GB RAM，以確保有足夠的記憶體來實現最佳效能，並且隨著配置的增長，系統可以容納額外的叢集和儲存物件。您不應在部署 Unified Manager 的虛擬機器上設定任何記憶體限制，也不應啟用任何阻礙軟體利用系統上分配的記憶體的功能（例如，膨脹）。

此外，在安裝第二個 Unified Manager 實例之前，單一 Unified Manager 實例可以監控的節點數量是有限制的。有關更多信息，請參閱《最佳實踐指南》。

["技術報告 4621：Unified Manager 最佳實務指南"](#)

記憶體頁面交換會對系統和管理應用程式的效能產生負面影響。由於整體主機利用率而競爭不可用的 CPU 資源可能會降低效能。

專用要求

安裝 Unified Manager 的實體或虛擬系統應專門用於 Unified Manager，不應與其他應用程式共用。其他應用程式可能會消耗系統資源並大幅降低 Unified Manager 的效能。

備份的空間需求

如果您打算使用 Unified Manager 備份和復原功能，請指派額外的容量，以便「資料」目錄或磁碟有 150 GB 的空間。備份可以寫入本機目標或遠端目標。最佳做法是確定 Unified Manager 主機系統外部至少具有 150 GB 空間的遠端位置。

主機連線需求

安裝 Unified Manager 的實體系統或虛擬系統應以成功的方式進行配置 `ping` 主機本身的主機名稱。如果是 IPv6 配置，您應該驗證 `ping6` 主機名稱是否成功，以確保 Unified Manager 安裝成功。

您可以使用主機名稱（或主機 IP 位址）存取產品 Web UI。如果您在部署期間為網路設定了靜態 IP 位址，那麼您就為網路主機指定了名稱。如果您使用 DHCP 配置網路，則應該從 DNS 取得主機名稱。

如果您打算允許使用者使用短名稱而不是使用完全限定網域名稱 (FQDN) 或 IP 位址存取 Unified Manager，則您的網路設定必須將此短名稱解析為有效的 FQDN。

Windows 軟體和安裝要求

為了在 Windows 上成功安裝 Unified Manager，您應該確保安裝 Unified Manager 的系統符合軟體需求。

作業系統軟體

您可以在下列 Windows 版本上安裝 Unified Manager：

- Microsoft Windows Server 2019 標準版與資料中心版
- Microsoft Windows Server 2022 標準版與資料中心版

Unified Manager 在 64 位元 Windows 作業系統上支援下列語言：

- 英語
- 日本人
- 簡體中文

請參閱互通性矩陣以取得受支援 Windows 版本的完整和最新清單。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)



NetApp 不支援使用第三方工具（例如 Microsoft System Center Configuration Manager (SCCM)）安裝 Unified Manager。

該伺服器應專用於執行 Unified Manager。伺服器上不應安裝任何其他應用程式。由於公司規定，您的 Windows 系統上可能安裝了活動的防毒軟體。您應該在安裝 Unified Manager 之前停用防毒軟體，以防止安裝失敗。

第三方軟體

以下第三方軟體套件與 Unified Manager 捆綁在一起。如果您的系統上未安裝這些第三方軟體包，Unified Manager 會在安裝過程中安裝它們。

- 適用於 Visual Studio 2015 版本 14.26.28720.3 的 Microsoft Visual C++ 可再發行元件套件
- MySQL 社群版 8.4.4
- Python 3.12.4
- OpenJDK 版本 11.0.25
- 7-zip 23.01 或更高版本



從 Unified Manager 9.5 開始，OpenJDK 在 Unified Manager 安裝套件中提供並自動安裝。從 Unified Manager 9.5 開始不再支援 Oracle Java。

如果已預先安裝 MySQL，則應確保：

- 它使用預設連接埠。
- 未安裝範例資料庫。
- 服務名稱是「MYSQL84」。

Unified Manager 部署在 WildFly Web 伺服器上。WildFly 26.1.3 與 Unified Manager 捆綁並配置。



在升級任何第三方軟體之前，您應該關閉正在執行的 Unified Manager 實例。第三方軟體安裝完成後，您可以重新啟動 Unified Manager。

安裝要求

- 應安裝 Microsoft .NET 4.5.2 或更高版本。
- 這 temp 目錄應配置 2 GB 的磁碟空間用於提取安裝檔。若要驗證目錄是否已創建，請在命令列介面上執行以下命令：``echo %temp%`
- 您應該在 Windows 磁碟機中保留 2 GB 的磁碟空間來快取 Unified Manager MSI 檔案。
- 您要安裝 Unified Manager 的 Microsoft Windows Server 應設定完全限定網域名稱 (FQDN)，以便 ping 對主機名稱和 FQDN 的回應成功。
- 您應該停用 Microsoft IIS 全球網路發布服務並確保連接埠 80 和 443 是空閒的。
- 您應該確保在安裝過程中停用「Windows Installer RDS 相容性」的遠端桌面會話主機設定。
- UDP 連接埠 514 應該是空閒的，並且不應被任何其他服務使用。
- 在安裝 Unified Manager 之前，您應該停用系統上的所有防毒軟體。安裝完成後，請確保手動將以下路徑從防毒掃描中排除：
 - Unified Manager 資料目錄，例如，`C:\ProgramData\NetApp\OnCommandAppData\`
 - Unified Manager 安裝目錄，例如，`\C:\Program Files\NetApp\`
 - MySQL 資料目錄，例如，`C:\ProgramData\MySQL\MySQLServerData`

支援的瀏覽器

若要存取 Unified Manager Web UI，請使用支援的瀏覽器。

互通性矩陣列出了受支援的瀏覽器版本。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

對於所有瀏覽器，停用彈出視窗阻止程式可確保軟體功能正常顯示。

如果您打算設定 Unified Manager 進行 SAML 驗證，以便身分提供者 (IdP) 可以對使用者進行驗證，那麼您也應該檢查 IdP 支援的瀏覽器清單。

協定和連接埠要求

所需的連接埠和協定支援 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間的通訊。

與 Unified Manager 伺服器的連接

在典型安裝中，連接到 Unified Manager Web UI 時無需指定連接埠號，因為請務必使用預設連接埠。例如，由於 Unified Manager 始終嘗試在其預設連接埠上執行，因此您可以輸入 `https://<host>` 而不是 `https://<host>:443`。

Unified Manager 伺服器使用特定協定存取下列介面：

介面	協定	港口	描述
Unified Manager Web UI	HTTP	80	用於存取 Unified Manager Web UI；自動重定向到安全連接埠 443。
Unified Manager Web UI 和使用 API 的程式	HTTPS	443	用於安全存取 Unified Manager Web UI 或進行 API 呼叫；API 呼叫只能使用 HTTPS 進行。
維護控制台	SSH/SFTP	22	用於存取維護控制台和檢索支援包。
Linux 命令列	SSH/SFTP	22	用於存取 Red Hat Enterprise Linux 命令列並檢索支援包。
系統日誌	UDP	514	用於從 ONTAP 系統存取基於訂閱的 EMS 訊息並根據這些訊息建立事件。

介面	協定	港口	描述
休息	HTTPS	9443	用於從經過驗證的ONTAP系統存取基於即時 REST API 的 EMS 事件。
MySQL 資料庫	MySQL	3306	用於啟用OnCommand Workflow Automation 和OnCommand API Services 對 Unified Manager 的存取。
AMQP QPID 代理	TCP/IP	56072	用於內部訊息通訊。
AMQP QPID 代理	透過 TCP 的 WebSocket	56080	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。
AMQP QPID 代理	透過 TCP 的 WebSocket	56443	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。透過此連接埠的通訊支援 TLS 或 SSL 提供的加密。



在 Windows 系統上安裝 Unified Manager 時，MySQL 的預設連接埠 3306 僅限於本機。安裝完成後，啟用防火牆以限制對連接埠 MySQL 3306 的存取。這不會影響任何升級方案，因為先前的配置會保留。可以修改此配置，並且可以使用 `Control access to MySQL port 3306` 維護控制台上的選項。有關信息，請參閱["附加選單選項"](#)。可以使用 Unified Manager 維護控制台變更用於 HTTP 和 HTTPS 通訊的連接埠（連接埠 80 和 443）。有關詳細信息，請參閱["配置Active IQ Unified Manager"](#)。

來自 **Unified Manager** 伺服器的連接

您應該配置防火牆以開啟端口，以便 Unified Manager 伺服器與託管儲存系統、伺服器和其他元件之間進行通訊。如果連接埠未打開，則通訊失敗。

根據您的環境，您可以選擇修改 Unified Manager 伺服器用於連接到特定目的地的連接埠和協定。

Unified Manager 伺服器使用下列協定和連接埠連接到託管儲存系統、伺服器和其他元件：

目的地	協定	港口	描述
儲存系統	HTTPS	443/TCP	用於監控和管理儲存系統。
儲存系統	NDMP	10000/TCP	用於某些快照復原操作。

目的地	協定	港口	描述
AutoSupport伺服器	HTTPS	443	用於發送AutoSupport資訊。需要網路存取才能執行此功能。
身份驗證伺服器	LDAP	389	用於發出身份驗證請求以及使用者和群組查找請求。
LDAPS	636	用於安全 LDAP 通訊。	郵件伺服器
SMTP	25	用於發送警報通知電子郵件。	SNMP 陷阱發送器
SNMPv1 或 SNMPv3	162/UDP	用於發送警報通知 SNMP 陷阱。	外部資料提供伺服器
TCP	2003	用於將效能資料傳送至外部資料提供者，例如 Graphite。	NTP 伺服器
NTP	123/UDP	用於將 Unified Manager 伺服器上的時間與外部 NTP 時間伺服器同步。（僅限 VMware 系統）	AMQP QPID 代理
TCP/IP	56072	用於內部訊息通訊。	AMQP QPID 代理
透過 TCP 的 WebSocket	56080	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。	AMQP QPID 代理
透過 TCP 的 WebSocket	56443	用於在此連接埠上偵聽從ONTAP（雲端代理）接收的訊息。透過此連接埠的通訊支援 TLS 或 SSL 提供的加密。	系統日誌

完成工作表

在安裝和設定 Unified Manager 之前，您應該準備好有關您的環境的具體資訊。您可以在工作表中記錄該資訊。

Unified Manager 安裝訊息

安裝 Unified Manager 所需的詳細資訊。

部署軟體的系統	你的價值
主機完全限定域名	
主機 IP 位址	
網路遮罩	
網關 IP 位址	
主 DNS 位址	
輔助 DNS 位址	
搜尋域名	
維護用戶名	
維護用戶密碼	

Unified Manager 設定訊息

安裝後設定 Unified Manager 的詳細資訊。根據您的配置，某些值是可選的。

環境	你的價值
維護使用者電子郵件地址	
SMTP 伺服器主機名稱或 IP 位址	
SMTP 使用者名稱	
SMTP 密碼	
SMTP 連接埠	25 (預設值)
發送警報通知的電子郵件	
身份驗證伺服器主機名稱或 IP 位址	
Active Directory 管理員名稱或 LDAP 綁定可分辨名稱	
Active Directory 密碼或 LDAP 綁定密碼	

環境	你的價值
認證伺服器基礎可分辨名稱	
身分識別提供者 (IdP) URL	
身分提供者 (IdP) 元資料	
SNMP 陷阱目標主機 IP 位址	
SNMP 連接埠	

集群資訊

使用 Unified Manager 管理的儲存系統的詳細資訊。

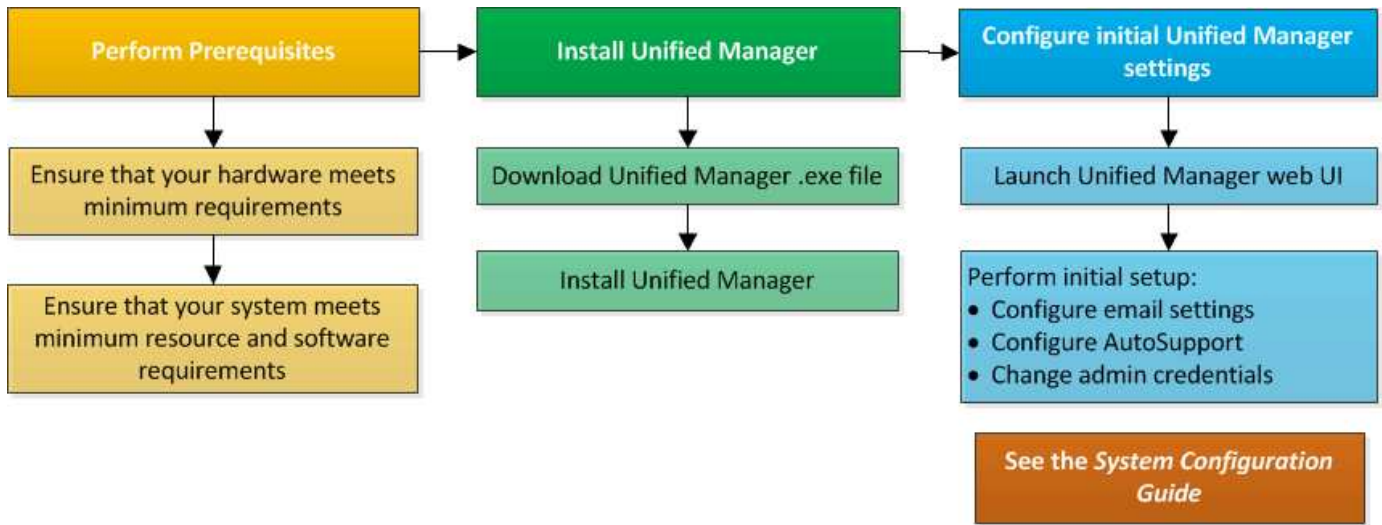
N 的簇 1	你的價值
主機名稱或叢集管理 IP 位址	
ONTAP 管理員使用者名稱  必須為管理員指派“admin”角色。	
ONTAP 管理員密碼	
協定	HTTPS

安裝、升級和刪除 Unified Manager 軟體

您可以安裝 Unified Manager、升級到較新版本或刪除 Unified Manager 應用程式。

安裝過程概述

安裝工作流程描述了您在使用 Unified Manager 之前必須執行的任務。



在 Windows 上安裝 Unified Manager

了解在 Windows 上下載和安裝 Unified Manager 的步驟順序非常重要。

安裝 Unified Manager

您可以安裝 Unified Manager 來監控和排除資料儲存容量、可用性、效能和保護問題。

開始之前

- 您計劃安裝 Unified Manager 的系統應符合系統和軟體需求。

看"[硬體系統需求](#)"。

看"[Windows 軟體和安裝要求](#)"。



從 Unified Manager 9.5 開始，OpenJDK 在安裝套件中提供並自動安裝。從 Unified Manager 9.5 開始不再支援 Oracle Java。

- 您應該具有 Windows 管理員權限。確保您的用戶名不以感嘆號"!"開頭!。 Installation of Unified Manager might fail if the user name of user running the installation begins with "!"。
- 除ASA r2 系統外，所有群集均支援。
- 您應該有一個受支援的 Web 瀏覽器。
- Unified Manager 維護使用者密碼應介於 8 到 20 個字元之間，應包含大寫字母或小寫字母、數字和特殊字元。
- 維護使用者或 MySQL 根使用者的密碼字串中不允許使用以下特殊字元：「! "%、=<>|^()\[\];

允許使用以下特殊字元：~ ! @#\$- ? ° + { }

步驟

1. 使用預設本機管理員帳戶登入 Windows。
2. 登入NetApp支援站點，然後導覽至 Unified Manager 的下載頁面：

"NetApp支援站點"

3. 選擇所需版本的 Unified Manager 並接受最終使用者授權協議 (EULA)。
4. 將 Unified Manager Windows 安裝檔案或 zip 檔案下載到 Windows 系統上的目標目錄。
5. 如果需要，請解壓縮 zip 文件，然後導覽至安裝文件所在的目錄。
6. 右鍵點選並以管理員身分執行 Unified Manager 安裝程式執行檔 (.exe)。

Unified Manager 會偵測缺少或預先安裝的第三方軟體套件並列出它們。如果系統中未安裝所需的第三方軟體包，Unified Manager 會在安裝過程中安裝它們。

7. 按一下“下一步”。
8. 輸入使用者名稱和密碼來建立維護使用者。
9. 在資料庫連線精靈中，輸入 MySQL 根密碼。
10. 按一下「變更」為 Unified Manager 安裝目錄和 MySQL 資料目錄指定新位置。

如果您不變更安裝目錄，Unified Manager 將安裝在預設安裝目錄中。

11. 按一下“下一步”。
12. 在「準備安裝 Shield」精靈中，按一下「安裝」。
13. 安裝完成後，按一下*完成*。
14. 如果您的 Windows 系統上安裝了活動的防毒軟體，請在安裝完成後手動將下列路徑從防毒掃描中排除：
 - Unified Manager 資料目錄
 - Unified Manager 安裝目錄
 - MySQL 資料目錄

安裝過程中會建立多個目錄：

- 安裝目錄

這是您在安裝期間指定的 Unified Manager 的根目錄。例子：C:\Program Files\NetApp\

- MySQL 資料目錄

這是儲存 MySQL 資料庫的目錄，您在安裝期間指定。例子：

C:\ProgramData\MySQL\MySQLServerData\

- Java 目錄

這是 OpenJDK 的安裝目錄。例子：C:\Program Files\NetApp\JDK\

- Unified Manager 應用程式資料目錄 (appDataDir)

這是儲存所有應用程式產生的資料的目錄。這包括日誌、支援包、備份和所有其他附加資料。例子：

C:\ProgramData\NetApp\OnCommandAppData\

您可以存取 Web UI 來執行 Unified Manager 的初始設置，例如["配置Active IQ Unified Manager"](#)。

執行 Unified Manager 的無人值守安裝

您可以使用命令列介面安裝 Unified Manager，無需使用者乾預。透過鍵值對的方式傳遞參數即可完成無人值守安裝。

步驟

1. 使用預設本機管理員帳戶登入 Windows 命令列介面。
2. 導覽至要安裝 Unified Manager 的位置，然後選擇下列選項之一：

選項	指示
如果預先安裝了第三方軟體包	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"</pre> <p>例：</p> <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</pre>
如果未安裝第三方軟體包	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"</pre> <p>例：</p> <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

這 `/qr` 此選項可啟用安靜模式並減少使用者介面。將顯示一個基本使用者介面，其中顯示安裝進度。系統不會提示您輸入。如果未預先安裝 JRE、MySQL 和 7zip 等第三方軟體包，則應使用 `/qr` 選項。若出現以下情況，安裝將會失敗。此選項用於未安裝第三方軟體包的伺服器上。

這 `/qn` 選項啟用沒有使用者介面的安靜模式。安裝期間不顯示任何使用者介面或詳細資訊。您不應該使用 `/qn` 當未安裝第三方軟體包時的選項。

3. 使用下列 URL 登入 Unified Manager Web 使用者介面：

```
https://IP address
```

更改 JBoss 密碼

您可以重設安裝期間設定的特定於實例的 JBoss 密碼。如果您的網站需要此安全功能來覆寫 Unified Manager 安裝設置，您可以選擇重設密碼。此操作也會更改 JBoss 用於存取 MySQL 的密碼。

開始之前

- 您應該擁有安裝 Unified Manager 的系統的 Windows 管理員權限。
- 您應該擁有 MySQL 根使用者的密碼。
- 您應該能夠存取 NetApp 提供的 `password.bat` 目錄中的腳本

```
C:\Program Files\NetApp\essentials\bin。
```

步驟

1. 以管理員使用者身分登入 Unified Manager 主機。
2. 使用 Windows 服務控制台停止下列 Unified Manager 服務：
 - NetApp Active IQ收購服務 (Ocie-au)
 - NetApp Active IQ管理伺服器服務 (Oncommandsvc)
3. 啟動 `password.bat` 腳本開始密碼更改流程：

```
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
```

4. 出現提示時，輸入 MySQL 根使用者密碼。
5. 出現提示時，輸入新的 JBoss 使用者密碼，然後再次輸入以進行確認。

請注意，密碼應介於 8 到 16 個字元之間，並且必須至少包含一個數字、一個大寫字母和一個小寫字母，以及至少一個以下特殊字元：

```
!@%^*-_=[]:<>./~/+
```

6. 腳本完成後，使用 Windows 服務控制台啟動 Unified Manager 服務：
 - NetApp Active IQ管理伺服器服務 (Oncommandsvc)
 - NetApp Active IQ收購服務 (Ocie-au)
7. 所有服務啟動後，您可以登入 Unified Manager UI。

Unified Manager 版本支援的升級路徑

Active IQ Unified Manager 支援每個版本的特定升級路徑。

並非所有版本的 Unified Manager 都可以執行就地升級到更高版本。Unified Manager 升級僅限於 N-2 型號，這表示升級只能在所有平台上的下 2 個版本內進行。例如，您只能從 Unified Manager 9.13 和 9.14 升級到 Unified Manager 9.16。

如果您執行的版本早於支援的版本，則需要先將 Unified Manager 實例升級到支援的版本之一，然後再升級至目前版本。

例如，如果您安裝的版本是 Unified Manager 9.9，並且您想要升級到 Unified Manager 9.14，請遵循一系列升級作業。

升級路徑範例：

1. 升級 9.11 → 9.13
2. 升級 9.13 → 9.14
3. 升級 9.13 → 9.16
4. 升級 9.14 → 9.16

有關升級路徑矩陣的更多信息，請參閱 ["知識庫 \(KB\) 文章"](#)。

升級 Unified Manager

您可以透過在 Windows 平台上下載並執行安裝檔案將 Unified Manager 9.13 或 9.14 升級至 9.16。

開始之前

- 要升級 Unified Manager 的系統應符合系統和軟體需求。

看 ["硬體系統需求"](#)。

看 ["Windows 軟體和安裝要求"](#)。



從 Unified Manager 9.5 開始，OpenJDK 在安裝套件中提供並自動安裝。從 Unified Manager 9.5 開始不再支援 Oracle Java。



在開始升級之前，請確保您的系統上安裝了 Microsoft .NET 4.5.2 或更高版本。

- MySQL 社群版會在 Unified Manager 升級期間自動升級。如果您系統上安裝的 MySQL 版本早於 8.4.4，則 Unified Manager 升級過程會自動將 MySQL 升級到 8.4.4。您無法執行早期版本的 MySQL 到 8.4.4 的獨立昇級。
- 除 ASA r2 系統外，所有群集均支援。
- 您應該具有 Windows 管理員權限。確保您的用戶名不以感嘆號 ""開頭!". Installation of Unified Manager might fail if the user name of user running the installation begins with " ! 「」。

- 您應該擁有有效的憑證才能登入NetApp支援網站。
- 為避免資料遺失，您應該建立 Unified Manager 機器的備份，以防升級期間出現問題。
- 您應該有足夠的磁碟空間來執行升級。

安裝磁碟機上的可用空間應比資料目錄的大小大 2.5 GB。如果可用空間不足，升級將停止並顯示錯誤訊息，指示要新增的空間量。

- 升級過程中，系統可能會提示您確認是否要保留先前的預設設定（即保留效能資料 13 個月）或將其變更為 6 個月。確認後，6個月後的歷史績效數據將被清除。
- 升級之前，您應該關閉 *<InstallDir>\JDK* 和 *MySQL Data Directory* 中所有開啟的檔案或資料夾。
- 如果您的 Windows 系統上安裝了活動的防毒軟體，Unified Manager 升級可能會失敗。在升級 Unified Manager 之前，您應該停用系統上的所有病毒掃描軟體。

在升級過程中，Unified Manager 不可用。在升級 Unified Manager 之前，您應該完成所有正在執行的操作。

如果 Unified Manager 與 OnCommand Workflow Automation 實例配對，且這兩種產品都有新版本的軟體可用，則必須中斷這兩種產品的連接，然後在執行升級後建立新的 Workflow Automation 連接。如果您只對其中一個產品進行升級，則應在升級後登入工作流程自動化並驗證它是否仍在從 Unified Manager 取得資料。

步驟

1. 登入NetApp支援站點，然後導覽至 Unified Manager 的下載頁面：

["NetApp支援站點"](#)。

2. 選擇所需版本的 Unified Manager 並接受最終使用者授權協議 (EULA)。
3. 將 Unified Manager Windows 安裝檔案或 zip 檔案下載到 Windows 系統上的目標目錄。如果需要，請解壓縮 zip 文件，然後導覽至安裝文件所在的目錄。右鍵點選並以管理員身分執行 Unified Manager 安裝程式執行檔 (.exe)。

Unified Manager 會提示您以下訊息：

```
This setup will perform an upgrade of Unified Manager. Do you want to continue?
```

4. 按一下“是”，然後按一下“下一步”。
5. 輸入安裝時設定的MySQL84 root密碼，然後點選*下一步*。
6. 在支援的 Web 瀏覽器的新視窗中啟動 Web UI 並登入以使用升級版的 Unified Manager。
7. 如果您的 Windows 系統上安裝了活動的防毒軟體，請確保在升級完成後手動將以下路徑從防毒掃描中排除：
 - Unified Manager 資料目錄
 - Unified Manager 安裝目錄
 - MySQL 資料目錄



若要執行 Unified Manager 的靜默升級，請執行下列命令：

```
ActiveIQUnifiedManager-<version>.exe /s /v"MYSQL_PASSWORD=<password>  
/qn /l*v <system_drive>:\install.log"
```

升級第三方產品

安裝在 Windows 系統上時，您可以在 Unified Manager 上升級第三方產品，例如 JRE。

開發這些第三方產品的公司會定期報告安全漏洞。您可以按照自己的時間表升級到該軟體的較新版本。

升級 OpenJDK

您可以在安裝了 Unified Manager 的 Windows 伺服器上升級到較新版本的 OpenJDK，以取得安全漏洞的修復。

開始之前

您必須擁有安裝 Unified Manager 的系統的 Windows 管理員權限。

您可以在發行系列中更新 OpenJDK 版本。例如，您可以從 OpenJDK 11.0.16 升級到 OpenJDK 11.0.18，但不能直接從 OpenJDK 11 更新到 OpenJDK 12。

步驟

1. 以管理員使用者身分登入 Unified Manager 主機。
2. 從 OpenJDK 網站下載適當版本的 OpenJDK（64 位元）到目標系統。

例如，下載 `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>。



下載該文件需要 Oracle 帳戶。如果您沒有 Oracle 帳戶，請前往"[Oracle 帳號登入](#)"頁面來創建一個。

3. 使用 Windows 服務控制台停止下列 Unified Manager 服務：
 - NetApp Active IQ收購服務 (Ocie-au)
 - NetApp Active IQ管理伺服器服務 (Oncommandsvc)
4. 展開 `zip` 文件。
5. 從結果複製目錄和文件 `jdk` 目錄（例如，`jdk-11.0.18` 到安裝 Java 的位置。例子：
`C:\Program Files\NetApp\JDK\`
6. 使用 Windows 服務控制台啟動 Unified Manager 服務：
 - NetApp Active IQ管理伺服器服務 (Oncommandsvc)
 - NetApp Active IQ收購服務 (Ocie-au)

卸載第三方產品

升級 Unified Manager 後，您可以解除安裝第三方產品，例如 Python 或 Microsoft Visual

C++ 2013。這是可選的。

解除安裝 Python

步驟

1. 從*控制台*中選擇*程式* > 程式和功能。
2. 從程式列表中選擇 Python。
3. 選擇*卸載此程式*。卸載除 3.12 之外的任何版本的 Python。確保保留 Python 版本 3.12。

解除安裝 Microsoft Visual C++ 2013

步驟

1. 從*控制台*中選擇*程式* > 程式和功能。
2. 從程式清單中選擇 **Microsoft Visual C++ 2013**。
3. 選擇*卸載此程式*。

重新啟動 Unified Manager

更改配置後，您可能需要重新啟動 Unified Manager。

開始之前

您必須具有 Windows 管理員權限。

步驟

1. 使用預設本機管理員帳戶登入 Windows。
2. 停止 Unified Manager 服務：

從...	按以下順序停止服務...
命令列	<ol style="list-style-type: none">a. <code>sc stop ocie-au</code>b. <code>sc stop Oncommandsvc</code>
Microsoft 服務管理員	<ol style="list-style-type: none">a. NetApp Active IQ收購服務 (Ocie-au)b. NetApp Active IQ管理伺服器服務 (Oncommandsvc)

3. 啟動 Unified Manager 服務：

從...	按以下順序啟動服務...
命令列	<ol style="list-style-type: none">a. <code>sc start Oncommandsvc</code>b. <code>sc start ocie-au</code>

從...	按以下順序啟動服務...
Microsoft 服務管理員	a. NetApp Active IQ管理伺服器服務 (Oncommandsvc) b. NetApp Active IQ收購服務 (Ocie-au)

解除安裝 Unified Manager

您可以使用程式和功能精靈來解除安裝 Unified Manager，或從命令列介面執行無人值守卸載。

開始之前

- 您必須具有 Windows 管理員權限。
- 卸載軟體之前，必須從 Unified Manager 伺服器中刪除所有叢集（資料來源）。
- 您應該手動刪除為允許或封鎖 MySQL 連接埠 3306 而建立的防火牆規則。防火牆規則不會被自動刪除。

步驟

1. 選擇下列選項之一來解除安裝 Unified Manager：

- 如果從「程式和功能」精靈中解除安裝 Unified Manager，請執行下列步驟：
 - i. 導航至*控制面板*>*程式和功能*。
 - ii. 選擇Active IQ Unified Manager，然後按一下 解除安裝。
- 如果從命令列卸載 Unified Manager，請執行下列步驟：
 - i. 使用管理員權限登入 Windows 命令列。
 - ii. 導航至Active IQ Unified Manager目錄，然後執行以下命令：

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v
%systemdrive%\UmUnInstall.log
```

如果伺服器上啟用了使用者帳戶控制 (UAC)，且您以網域使用者身分登錄，則必須使用命令列卸載方法。

Unified Manager 已從您的系統中解除安裝。

2. 卸載在 Unified Manager 卸載期間未刪除的以下第三方軟體包和資料：

- 第三方軟體包：JRE、MySQL、Microsoft Visual C++ 2015 Redistributable、Python 和 7zip
- Unified Manager 產生的 MySQL 應用程式數據
- 應用程式日誌和應用程式資料目錄的內容

執行配置和管理任務

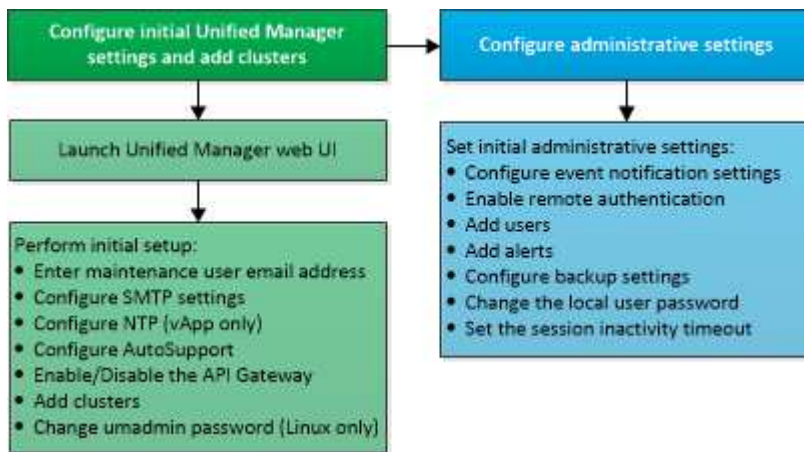
配置Active IQ Unified Manager

安裝Active IQ Unified Manager（以前稱為OnCommand Unified Manager）後，您必須完成初始設定（也稱為首次體驗精靈）才能存取 Web UI。然後，您可以執行其他配置任務，例如新增叢集、配置遠端身份驗證、新增使用者和新增警報。

本手冊中所述的一些步驟是完成 Unified Manager 實例的初始設定所必需的。其他程式是建議的配置設置，這些設置有助於在新實例上進行設置，或在您開始定期監控ONTAP系統之前了解這些設置。

配置序列概述

設定工作流程描述了您在使用 Unified Manager 之前必須執行的任務。



存取 Unified Manager Web UI

安裝 Unified Manager 後，您可以存取 Web UI 設定 Unified Manager，以便開始監控您的ONTAP系統。

開始之前

- 如果這是您第一次造訪 Web UI，則必須以維護使用者（或 Linux 安裝的 umadmin 使用者）身分登入。
- 如果您打算允許使用者使用短名稱而不是使用完全限定網域名稱 (FQDN) 或 IP 位址存取 Unified Manager，則您的網路設定必須將此短名稱解析為有效的 FQDN。
- 如果伺服器使用自簽名數位證書，瀏覽器可能會顯示警告，表示該證書不受信任。您可以承認風險並繼續訪問，或者安裝憑證授權單位 (CA) 簽署的數位憑證進行伺服器驗證。

步驟

1. 使用安裝結束時顯示的 URL 從瀏覽器啟動 Unified Manager Web UI。URL 是 Unified Manager 伺服器的 IP 位址或完全限定網域名稱 (FQDN)。

連結格式如下：`https://URL`。

2. 使用您的維護使用者憑證登入 Unified Manager Web UI。



如果您在一小時內連續三次嘗試登入 Web UI 失敗，您將被鎖定在系統之外，並且需要聯絡您的系統管理員。這僅適用於本地用戶。

執行 **Unified Manager Web UI** 的初始設置

若要使用 Unified Manager，您必須先設定初始設定選項，包括 NTP 伺服器、維護使用者電子郵件地址、SMTP 伺服器主機以及新增ONTAP叢集。

開始之前

您必須已執行以下操作：

- 使用安裝後提供的 URL 啟動 Unified Manager Web UI
- 使用安裝期間建立的維護使用者名稱和密碼（Linux 安裝的 umadmin 使用者）登入

只有在您第一次造訪 Web UI 時才會出現Active IQ Unified ManagerGetting Started 頁面。以下頁面來自 VMware 上的安裝。

Getting Started



Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Email

SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS ⓘ Use SSL ⓘ

Continue

如果您稍後想要變更這些選項中的任何一個，您可以從 Unified Manager 左側導覽窗格中的常規選項中選擇您的選擇。請注意，NTP 設定僅適用於 VMware 安裝，並且可以稍後使用 Unified Manager 維護控制台進行變更。

步驟

1. 在Active IQ Unified Manager初始設定頁面中，輸入維護使用者電子郵件地址、SMTP 伺服器主機名稱和任何其他 SMTP 選項以及 NTP 伺服器（僅限 VMware 安裝）。然後點選“繼續”。



如果您選擇了「使用 STARTTLS」或「使用 SSL」選項，則按一下「繼續」按鈕後將顯示憑證頁面。驗證憑證詳細資訊並接受憑證以繼續進行 Web UI 的初始設定。

2. 在AutoSupport頁面中，按一下 同意並繼續 以啟用從 Unified Manager 到 NetAppActive IQ 的AutoSupport 訊息發送。

如果您需要指定代理程式來提供網際網路存取以傳送AutoSupport內容，或您想要停用AutoSupport，請使用 Web UI 中的 **General** > * AutoSupport* 選項。

3. 在 Red Hat 系統上，將 umadmin 使用者密碼從預設的「admin」字串變更為個人化字串。

4. 在設定 API 閘道頁面中，選擇是否要使用 API 閘道功能，該功能可讓 Unified Manager 管理您計畫使用 ONTAP REST API 監控的 ONTAP 叢集。然後點選“繼續”。

您可以稍後在 Web UI 中從 常規 > 功能設定 > **API 網關** 啟用或停用此設定。有關 API 的更多信息，請參閱["Active IQ Unified Manager REST API 入門"](#)。

5. 新增您希望 Unified Manager 管理的集群，然後按一下「下一步」。對於您計畫管理的每個集群，您必須擁有主機名稱或集群管理 IP 位址 (IPv4 或 IPv6) 以及使用者名稱和密碼憑證 - 使用者必須具有「admin」角色。

此步驟是可選的。您可以稍後在 Web UI 中從 儲存管理 > 叢集設定 新增叢集。

6. 在「摘要」頁面中，驗證所有設定是否正確，然後按一下「完成」。

“入門”頁面關閉並顯示“統一管理器儀表板”頁面。

新增集群

您可以將叢集新增至 Active IQ Unified Manager，以便監控該叢集。這包括獲取叢集資訊的能力，例如叢集的健康狀況、容量、效能和配置，以便您可以發現並解決可能出現的任何問題。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須具有以下資訊：
 - Unified Manager 支援本機 ONTAP 叢集、ONTAP Select 和 Cloud Volumes ONTAP。
 - 主機名稱或叢集管理 IP 位址

主機名稱是 Unified Manager 用於連接叢集的 FQDN 或短名稱。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。如果您使用節點管理 LIF，操作將會失敗。

- 叢集必須運行 ONTAP 9.1 版軟體或更高版本。
- ONTAP 管理員使用者名稱和密碼

此帳戶必須具有 *admin* 角色，並將應用程式存取權限設為 *ontapi*、*console* 和 *http*。

- 使用 HTTPS 協定連接叢集的連接埠號碼（通常為連接埠 443）
- 您擁有所需的證書：

SSL (HTTPS) 憑證：此憑證歸 Unified Manager 所有。全新安裝 Unified Manager 時會產生預設的自簽章 SSL (HTTPS) 憑證。NetApp 建議您將其升級為 CA 簽章憑證以獲得更好的安全性。如果伺服器憑證過期，您應該重新產生它並重新啟動 Unified Manager，以便服務合併新憑證。有關重新產生 SSL 憑證的更多信息，請參閱["產生 HTTPS 安全性憑證"](#)。

EMS 憑證：此憑證歸 Unified Manager 所有。它用於對從 ONTAP 接收的 EMS 通知進行身份驗證。

用於相互 TLS 通訊的憑證：在 Unified Manager 和 ONTAP 之間的相互 TLS 通訊期間使用。根據 ONTAP 版本，為叢集啟用基於憑證的身份驗證。如果執行 ONTAP 版本的叢集低於 9.5，則不會啟用基於憑證的驗證。

如果您正在更新舊版的 Unified Manager，則不會自動為叢集啟用基於憑證的驗證。但是，您可以透過修改和儲存叢集詳細資訊來啟用它。如果憑證過期，您應該重新產生它以包含新憑證。有關查看和重新生成證書的更多信息，請參閱["編輯集群"](#)。



- 您可以從 Web UI 新增集群，並自動啟用基於憑證的身份驗證。
- 您可以透過 Unified Manager CLI 新增集群，預設不會啟用基於憑證的身份驗證。如果您使用 Unified Manager CLI 新增叢集，則需要使用 Unified Manager UI 編輯該叢集。您可以看到["支援的 Unified Manager CLI 命令"](#)使用 Unified Manager CLI 新增叢集。
- 如果為叢集啟用了基於憑證的驗證，並且您從伺服器備份 Unified Manager 並將其還原到主機名稱或 IP 位址已變更的另一個 Unified Manager 伺服器，則叢集的監控可能會失敗。為避免失敗，請編輯並儲存叢集詳細資訊。有關編輯集群詳細信息的更多信息，請參閱["編輯集群"](#)。

+

集群證書：此證書歸 ONTAP 擁有。您無法將憑證已過期的叢集新增至 Unified Manager，如果憑證已過期，則應在新增叢集之前重新產生憑證。有關證書產生的信息，請參閱知識庫 (KB) 文章 ["如何在系統管理員使用者介面中續訂 ONTAP 自簽名憑證"](#)。

- Unified Manager 伺服器上必須有足夠的空間。當資料庫目錄中超過 90% 的空間已被佔用時，您將無法向伺服器新增叢集。

對於 MetroCluster 配置，您必須新增本地集群和遠端集群，並且必須正確配置集群。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在「叢集設定」頁面上，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、使用者名稱、密碼和連接埠號碼。

您可以將叢集管理 IP 位址從 IPv6 變更為 IPv4，或從 IPv4 變更為 IPv6。下一個監控週期完成後，新的 IP 位址將反映在叢集網格和叢集設定頁面中。

4. 點選“提交”。
5. 在授權主機對話方塊中，按一下“檢視憑證”，查看叢集的憑證資訊。
6. 按一下“是”。

儲存叢集詳細資料後，您可以看到叢集的 Mutual TLS 通訊憑證。

如果未啟用基於憑證的驗證，Unified Manager 僅在最初新增叢集時檢查憑證。Unified Manager 不會檢查對 ONTAP 的每個 API 呼叫的憑證。

發現新叢集的所有物件後，Unified Manager 開始收集前 15 天的歷史效能資料。這些統計數據是使用數據連續性收集功能收集的。此功能可在新增叢集後立即為您提供該叢集超過兩週的效能資訊。資料連續性收集週期完成後，預設每五分鐘收集一次即時叢集效能資料。



由於收集 15 天的效能資料需要大量 CPU，因此建議您錯開新叢集的添加，以便資料連續性收集輪詢不會同時在太多叢集上運行。此外，如果您在資料連續性收集期間重新啟動 Unified Manager，則收集將停止，並且您將在效能圖表中看到缺失時間範圍的差距。



如果您收到無法新增叢集的錯誤訊息，請檢查兩個系統上的時鐘是否不同步，以及 Unified Manager HTTPS 憑證的開始日期是否晚於叢集上的日期。您必須確保使用 NTP 或類似服務同步時鐘。

相關資訊

["安裝 CA 簽署並傳回的 HTTPS 憑證"](#)

配置 Unified Manager 以發送警報通知

您可以設定 Unified Manager 來傳送有關您環境中的事件的警報通知。在傳送通知之前，您必須設定其他幾個 Unified Manager 選項。

開始之前

您必須具有應用程式管理員角色。

部署 Unified Manager 並完成初始設定後，您應該考慮設定您的環境以根據收到的事件觸發警報並產生通知電子郵件或 SNMP 陷阱。

步驟

1. ["配置事件通知設定"](#)。

如果您希望在您的環境中發生某些事件時發送警報通知，則必須設定 SMTP 伺服器並提供用於傳送警報通知的電子郵件地址。如果您想使用 SNMP 陷阱，您可以選擇該選項並提供必要的資訊。

2. ["啟用遠端身份驗證"](#)。

如果您希望遠端 LDAP 或 Active Directory 使用者存取 Unified Manager 實例並接收警報通知，則必須啟用遠端驗證。

3. ["新增身份驗證伺服器"](#)。

您可以新增身份驗證伺服器，以便身份驗證伺服器內的遠端使用者可以存取 Unified Manager。

4. ["新增用戶"](#)。

您可以新增幾種不同類型的本機或遠端使用者並指派特定的角色。建立警報時，您會指定一個使用者來接收警報通知。

5. ["添加警報"](#)。

新增了用於發送通知的電子郵件地址、新增了用於接收通知的使用者、配置了網路設定以及配置了環境所需的 SMTP 和 SNMP 選項後，您就可以指派警報了。

配置事件通知設定

您可以設定 Unified Manager 在產生事件或將事件指派給使用者時傳送警報通知。您可以設定用於傳送警報的 SMTP 伺服器，並且可以設定各種通知機制 - 例如，警報通知可以作為電子郵件或 SNMP 陷阱傳送。

開始之前

您必須具有以下資訊：

- 發送警報通知的電子郵件地址

電子郵件地址出現在已發送警報通知的「寄件者」欄位中。如果電子郵件因任何原因無法送達，則該電子郵件地址也將用作無法送達郵件的收件者。

- SMTP 伺服器主機名稱以及存取該伺服器的使用者名稱和密碼
- 將接收 SNMP 陷阱的陷阱目標主機的主機名稱或 IP 位址，以及 SNMP 版本、出站陷阱連接埠、社群和其他所需的 SNMP 設定值

若要指定多個陷阱目標，請用逗號分隔每個主機。在這種情況下，清單中所有主機的所有其他 SNMP 設定（例如版本和出站陷阱連接埠）必須相同。

您必須具有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「常規」>「通知」。
2. 在通知頁面中，配置適當的設定。

筆記：

- 如果寄件者地址預先填寫了地址“ActiveIQUnifiedManager@localhost.com”，則應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。
 - 如果無法解析 SMTP 伺服器的主機名，則可以指定 SMTP 伺服器的 IP 位址（IPv4 或 IPv6）來取代主機名稱。
3. 點選“儲存”。
 4. 如果您選擇了「使用 STARTTLS」或「使用 SSL」選項，則按一下「儲存」按鈕後將顯示憑證頁面。驗證證書詳細資訊並接受證書以保存通知設定。

您可以點擊*查看證書詳情*按鈕來查看證書詳情。如果現有憑證已過期，請取消選取使用 **STARTTLS** 或使用 **SSL** 框，儲存通知設置，然後再次選取使用 **STARTTLS** 或使用 **SSL** 框以查看新憑證。

啟用遠端身份驗證

您可以啟用遠端身份驗證，以便 Unified Manager 伺服器可以與您的身份驗證伺服器通訊。身份驗證伺服器的使用者可以存取 Unified Manager 圖形介面來管理儲存物件和資料。

開始之前

您必須具有應用程式管理員角色。



Unified Manager 伺服器必須直接與驗證伺服器連線。您必須停用任何本機 LDAP 用戶端，例如 SSSD（系統安全服務守護程式）或 NSLCD（名稱服務 LDAP 快取守護程式）。

您可以使用 Open LDAP 或 Active Directory 啟用遠端驗證。如果停用遠端驗證，遠端使用者將無法存取 Unified Manager。

透過 LDAP 和 LDAPS（安全 LDAP）支援遠端身份驗證。Unified Manager 使用 389 作為非安全通訊的預設端口，使用 636 作為安全通訊的預設端口。



用於驗證使用者身分的憑證必須符合 X.509 格式。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 選取“啟用遠端身份驗證...”複選框。
3. 在身份驗證服務欄位中，選擇服務類型並配置身份驗證服務。

對於身份驗證類型...	輸入以下資訊...
活動目錄	<ul style="list-style-type: none">• 認證伺服器管理員名稱採用以下格式之一：<ul style="list-style-type: none">◦ domainname\username◦ username@domainname◦ Bind Distinguished Name（使用適當的 LDAP 符號）• 管理者密碼• 基本可分辨名稱（使用適當的 LDAP 符號）
開啟 LDAP	<ul style="list-style-type: none">• 綁定可分辨名稱（以適當的 LDAP 符號表示）• 綁定密碼• 基本可分辨名稱

如果 Active Directory 使用者的驗證花費很長時間或逾時，則驗證伺服器可能需要很長時間才能回應。停用 Unified Manager 中對嵌套群組的支援可能會減少身份驗證時間。

如果您為身份驗證伺服器選擇「使用安全連線」選項，則 Unified Manager 將使用安全通訊端層 (SSL) 協定與身份驗證伺服器進行通訊。

4. *可選：*新增身份驗證伺服器，並測試身份驗證。
5. 點選“儲存”。

禁用嵌套群組的遠端身份驗證

如果您啟用了遠端驗證，則可以停用巢狀群組驗證，以便只有個人使用者（而不是群組成

員) 可以遠端向 Unified Manager 進行驗證。當您想要提高 Active Directory 驗證回應時間時，可以停用巢狀群組。

開始之前

- 您必須具有應用程式管理員角色。
- 停用嵌套群組僅適用於使用 Active Directory 時。

停用 Unified Manager 中對嵌套群組的支援可能會減少身份驗證時間。如果嵌套群組支援已停用，且如果將遠端群組新增至 Unified Manager，則個別使用者必須是遠端群組的成員才能向 Unified Manager 進行驗證。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 選取「停用巢狀組查找」複選框。
3. 點選“儲存”。

設定身份驗證服務

身份驗證服務可在身份驗證伺服器中對遠端使用者或遠端群組進行身份驗證，然後才允許他們存取 Unified Manager。您可以使用預先定義的驗證服務（例如 Active Directory 或 OpenLDAP）或透過設定您自己的驗證機制來對使用者進行身份驗證。

開始之前

- 您必須啟用遠端身份驗證。
- 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「常規」>「遠端驗證」。
2. 選擇以下身份驗證服務之一：

如果您選擇...	然後這樣做...
活動目錄	<ol style="list-style-type: none">a. 輸入管理員名稱和密碼。b. 指定身份驗證伺服器的基本可分辨名稱。 <p>例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。</p>
OpenLDAP	<ol style="list-style-type: none">a. 輸入綁定可分辨名稱和綁定密碼。b. 指定身份驗證伺服器的基本可分辨名稱。 <p>例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。</p>

如果您選擇...	然後這樣做...
其他的	<p>a. 輸入綁定可分辨名稱和綁定密碼。</p> <p>b. 指定身份驗證伺服器的基本可分辨名稱。</p> <p>例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。</p> <p>c. 指定認證伺服器支援的LDAP協定版本。</p> <p>d. 輸入使用者名稱、群組成員身分、使用者群組和成員屬性。</p>



如果要修改身份驗證服務，則必須刪除任何現有的身份驗證伺服器，然後新增的身份驗證伺服器。

3. 點選“儲存”。

新增身份驗證伺服器

您可以在管理伺服器上新增身份驗證伺服器並啟用遠端身份驗證，以便身份驗證伺服器內的遠端使用者可以存取 Unified Manager。


開始之前

- 必須提供以下資訊：
 - 認證伺服器的主機名稱或IP位址
 - 認證伺服器的連接埠號
- 您必須啟用遠端身份驗證並設定身份驗證服務，以便管理伺服器可以對身份驗證伺服器中的遠端使用者或群組進行身份驗證。
- 您必須具有應用程式管理員角色。

如果您要新增的身份驗證伺服器是高可用性 (HA) 對的一部分（使用相同的資料庫），那麼您也可以新增合作夥伴驗證伺服器。當其中一個身份驗證伺服器無法存取時，這使得管理伺服器能夠與合作夥伴進行通訊。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 啟用或停用*使用安全連線*選項：

如果你想...	然後這樣做...
<p>啟用它</p>	<p>a. 選擇*使用安全連線*選項。</p> <p>b. 在身份驗證伺服器區域，按一下「新增」。</p> <p>c. 在新增認證伺服器對話方塊中，輸入伺服器的認證名稱或IP位址（IPv4或IPv6）。</p> <p>d. 在授權主機對話方塊中，按一下檢視憑證。</p> <p>e. 在「檢視證書」對話方塊中，驗證證書訊息，然後按一下「關閉」。</p> <p>f. 在授權主機對話方塊中，按一下「是」。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> 當您啟用*使用安全連線驗證*選項時，Unified Manager 會與身分驗證伺服器通訊並顯示憑證。Unified Manager 使用 636 作為安全通訊的預設端口，使用連接埠號碼 389 作為非安全通訊的預設連接埠。</p> </div>
<p>禁用它</p>	<p>a. 清除*使用安全連線*選項。</p> <p>b. 在身份驗證伺服器區域，按一下「新增」。</p> <p>c. 在新增驗證伺服器對話方塊中，指定伺服器的主機名稱或 IP 位址（IPv4 或 IPv6）以及連接埠詳細資訊。</p> <p>d. 按一下“新增”。</p>

您新增的身份驗證伺服器將顯示在伺服器區域。

3. 執行測試身份驗證以確認您可以在新增的身份驗證伺服器中對使用者進行身份驗證。

測試身份驗證伺服器的配置

您可以驗證身份驗證伺服器的配置，以確保管理伺服器能夠與它們通訊。您可以透過從身份驗證伺服器搜尋遠端使用者或遠端群組並使用配置的設定對其進行身份驗證來驗證配置。

開始之前

- 您必須啟用遠端身份驗證，並設定身份驗證服務，以便 Unified Manager 伺服器可以對遠端使用者或遠端群組進行身份驗證。
- 您必須新增身份驗證伺服器，以便管理伺服器可以從這些伺服器搜尋遠端使用者或遠端群組並對其進行身份驗證。
- 您必須具有應用程式管理員角色。

如果將身分驗證服務設定為 Active Directory，且您正在驗證屬於身分驗證伺服器主要群組的遠端使用者的驗證

，則身分驗證結果中不會顯示有關主要群組的資訊。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 按一下“測試身份驗證”。
3. 在測試使用者對話方塊中，指定遠端使用者的使用者名稱和密碼或遠端群組的使用者名，然後按一下*測試*。

如果您正在驗證遠端群組，則不得輸入密碼。

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 and 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“Test”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：

步驟

1. 按一下“名稱”，然後在“警報名稱”欄位中輸入“**HealthTest**”。
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. 在“名稱包含”欄位中輸入“**abc**”，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”，在“名稱包含”欄位中輸入“**xyz**”，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. 按一下“操作”，然後在“警報這些使用者”欄位中輸入“**sample@domain.com**”。
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”。

更改本機用戶密碼

您可以修改本機使用者登入密碼，以避免潛在的安全風險。

開始之前

您必須以本機使用者登入。

無法使用這些步驟變更維護使用者和遠端使用者的密碼。若要變更遠端使用者密碼，請聯絡您的密碼管理員。若

要變更維護使用者密碼，請參閱["使用維護控制台"](#)。

步驟

1. 登入 Unified Manager。
2. 從頂部選單列中，點擊使用者圖標，然後點擊*更改密碼*。

如果您是遠端用戶，則不會顯示「更改密碼」選項。

3. 在「更改密碼」對話方塊中，輸入目前密碼和新密碼。
4. 點選“儲存”。

如果 Unified Manager 是在高可用性設定中進行設定的，則必須變更設定的第二個節點上的密碼。兩個實例必須具有相同的密碼。

設定會話不活動逾時

您可以指定 Unified Manager 的不活動逾時值，以便在一定時間不活動後會自動終止。預設情況下，超時設定為 4,320 分鐘（72 小時）。

開始之前

您必須具有應用程式管理員角色。

此設定會影響所有已登入的使用者會話。



如果您啟用了安全性斷言標記語言 (SAML) 驗證，則此選項不可用。

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指定不活動逾時：

如果你想...	然後這樣做...
沒有設定超時，這樣會話就不會自動關閉	在「不活動逾時」面板中，將滑桿按鈕向左移動（關閉），然後按一下「套用」。
設定特定的分鐘數作為超時值	在「不活動逾時」面板中，將滑桿按鈕向右移動（開啟），以分鐘為單位指定不活動逾時值，然後按一下「套用」。

透過 CLI 設定會話逾時

您可以使用 CLI 為 Unified Manager 設定最大會話逾時值，以便會話在一定時間後自動終止。預設情況下，您的會話逾時設定為最大值，即 4,320 分鐘（72 小時）。這表示您的工作階段會在 72 小時後自動結束，即使您已登入並正在使用 Unified Manager。

關於此任務

您必須具有應用程式管理員角色。

會話逾時設定會影響所有已登入的使用者會話。

步驟

1. 透過輸入 `um cli login` 命令。使用有效的使用者名稱和密碼進行身份驗證。
2. 輸入 `um option set max.session.timeout.value=<in mins>` 命令修改會話逾時值。

更改 Unified Manager 主機名

在某些時候，您可能會想要變更已安裝 Unified Manager 的系統的主機名稱。例如，您可能想要重新命名主機，以便更輕鬆地按類型、工作群組或受監控的叢集群組識別 Unified Manager 伺服器。

更改主機名稱所需的步驟有所不同，取決於 Unified Manager 是在 VMware ESXi 伺服器、Red Hat Linux 伺服器還是 Microsoft Windows 伺服器上執行。

更改 Unified Manager 虛擬設備主機名

首次部署 Unified Manager 虛擬設備時，會為網路主機指派名稱。您可以在部署後變更主機名稱。如果變更主機名，也必須重新產生 HTTPS 憑證。

開始之前

您必須以維護使用者身分登入 Unified Manager，或指派應用程式管理員角色才能執行這些任務。

您可以使用主機名稱（或主機 IP 位址）存取 Unified Manager Web UI。如果您在部署期間為網路配置了靜態 IP 位址，那麼您將為網路主機指定名稱。如果您使用 DHCP 配置網路，則主機名稱應從 DNS 中取得。如果 DHCP 或 DNS 設定不正確，則會自動指派主機名稱「Unified Manager」並將其與安全性憑證關聯。

無論主機名稱為何分配，如果您變更主機名，並打算使用新主機名稱存取 Unified Manager Web UI，則必須產生新的安全性憑證。

如果您使用伺服器的 IP 位址而不是主機名稱存取 Web UI，則變更主機名稱時無需產生新憑證。但是，最佳做法是更新證書，以便證書中的主機名稱與實際主機名稱相符。

如果您在 Unified Manager 中變更主機名，則必須在 OnCommand Workflow Automation (WFA) 中手動更新主機名稱。主機名稱不會在 WFA 中自動更新。

直到 Unified Manager 虛擬機器重新啟動後，新憑證才會生效。

步驟

1. [產生 HTTPS 安全性憑證](#)

如果您想要使用新的主機名稱存取 Unified Manager Web UI，則必須重新產生 HTTPS 憑證以將其與新的主機名稱關聯。

2. [重新啟動 Unified Manager 虛擬機](#)

重新產生 HTTPS 憑證後，您必須重新啟動 Unified Manager 虛擬機器。

產生HTTPS安全證書

首次安裝Active IQ Unified Manager時，會安裝預設 HTTPS 憑證。您可以產生一個新的 HTTPS 安全性憑證來取代現有的憑證。

開始之前

您必須具有應用程式管理員角色。

重新產生憑證的原因可能有多種，例如，如果您想要更好的可分辨名稱 (DN) 值，或者您想要更大的金鑰大小，或更長的有效期，或目前憑證已過期。

如果您無法存取 Unified Manager Web UI，則可以使用維護控制台重新產生具有相同值的 HTTPS 憑證。在重新產生憑證時，您可以定義金鑰大小和金鑰的有效期限。如果您使用 `Reset Server Certificate` 選項，則會建立一個有效期為 397 天的新 HTTPS 憑證。此憑證將具有大小為 2048 位元的 RSA 金鑰。

步驟

1. 在左側導覽窗格中，按一下「常規」>「HTTPS 憑證」。
2. 按一下「重新產生 HTTPS 憑證」。

系統彈出「重新產生HTTPS證書」對話框。

3. 根據您想要產生憑證的方式選擇以下選項之一：

如果你想...	這樣做...
使用當前值重新產生證書	按一下「使用目前憑證屬性重新產生」選項。

如果你想...	這樣做...
<p>使用不同的值產生證書</p>	<p>按一下“更新目前憑證屬性”選項。</p> <p>如果您不輸入新值，則通用名稱和備用名稱欄位將使用現有憑證中的值。“通用名稱”應設定為主機的 FQDN。其他欄位不需要值，但您可以輸入值，例如，如果您希望在憑證中填入這些值，則為 EMAIL、COMPANY、DEPARTMENT、City、State 和 Country 輸入這些值。您也可以從可用的金鑰大小（金鑰演算法為「RSA」）和有效期限中進行選擇。</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <ul style="list-style-type: none"> 密鑰大小的允許值為 2048，3072 和 4096。 有效期限最短1天，最長36500天。 <p>儘管允許有效期為 36500 天，但建議您使用不超過 397 天或 13 個月的有效期。因為如果您選擇的有效期超過 397 天，併計劃匯出此憑證的 CSR 並由知名 CA 進行簽名，則 CA 返回給您的簽名憑證的有效期將減少到 397 天。</p> <ul style="list-style-type: none"> 如果您想要從憑證中的備用名稱欄位中刪除本機識別訊息，可以勾選「排除本機識別資訊（例如 localhost）」複選框。選取此核取方塊後，只有您在欄位中輸入的內容才會在備用名稱欄位中使用。當留空時，產生的憑證將根本沒有備用名稱欄位。 </div>

4. 按一下「是」重新產生憑證。
5. 重新啟動 Unified Manager 伺服器，以使新憑證生效。
6. 透過查看HTTPS證書來驗證新的證書資訊。

重新啟動 Unified Manager 虛擬機

您可以從 Unified Manager 的維護控制台重新啟動虛擬機器。產生新的安全性憑證後或虛擬機器出現問題時必須重新啟動。

開始之前

虛擬設備已啟動。

您以維護使用者登入維護控制台。

您也可以使用「重新啟動客戶機」選項從 vSphere 重新啟動虛擬機器。有關詳細信息，請參閱 VMware 文件。

步驟

1. 存取維護控制台。
2. 選擇*系統設定*>*重新啟動虛擬機器*。

在 Linux 系統上變更 Unified Manager 主機名

在某些時候，您可能會想要變更已安裝 Unified Manager 的 Red Hat Enterprise Linux 機器的主機名稱。例如，您可能想要重新命名主機，以便在列出 Linux 機器時更輕鬆地按類型、工作群組或受監控的叢集群組識別 Unified Manager 伺服器。

開始之前

您必須具有安裝 Unified Manager 的 Linux 系統的 root 使用者存取權限。

您可以使用主機名稱（或主機 IP 位址）存取 Unified Manager Web UI。如果您在部署期間為網路配置了靜態 IP 位址，那麼您將為網路主機指定名稱。如果您使用 DHCP 設定網路，則主機名稱應從 DNS 伺服器中取得。

無論主機名稱為何分配，如果您變更主機名稱並打算使用新主機名稱存取 Unified Manager Web UI，則必須產生新的安全性憑證。

如果您使用伺服器的 IP 位址而不是主機名稱存取 Web UI，則變更主機名稱時無需產生新憑證。但是，最佳做法是更新證書，以便證書中的主機名稱與實際主機名稱相符。直到 Linux 機器重新啟動後，新憑證才會生效。

如果您在 Unified Manager 中變更主機名，則必須在 OnCommand Workflow Automation (WFA) 中手動更新主機名稱。主機名稱不會在 WFA 中自動更新。

步驟

1. 以 root 使用者身分登入要修改的 Unified Manager 系統。
2. 輸入以下指令停止 Unified Manager 軟體和相關的 MySQL 軟體：

```
systemctl stop ocieau ocie mysqld
```

3. 使用 Linux 更改主機名 `hostnamectl` 命令：

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. 為伺服器重新產生 HTTPS 憑證：

```
/opt/netapp/essentials/bin/cert.sh create
```

5. 重啟網路服務：

```
systemctl restart NetworkManager.service
```

6. 服務重啟後，驗證新的主機名稱是否能 ping 通自己：

```
ping new_hostname
```

```
ping nuhost
```

此命令應傳回先前為原始主機名稱設定的相同 IP 位址。

7. 完成並驗證主機名稱變更後，輸入以下命令重新啟動 Unified Manager：

```
systemctl start mysqld ocie ocieau
```

啟用和停用基於策略的儲存管理

從 Unified Manager 9.7 開始，您可以在 ONTAP 叢集上設定儲存工作負載（磁碟區和 LUN），並根據指派的效能服務等級管理這些工作負載。此功能類似於在 ONTAP 系統管理員中建立工作負載並附加 QoS 策略，但使用 Unified Manager 應用程式時，您可以設定和管理 Unified Manager 實例正在監控的所有叢集中的工作負載。

您必須具有應用程式管理員角色。

此選項預設為啟用，但如果您不想使用 Unified Manager 設定和管理工作負載，則可以停用它。

啟用後，此選項會在使用者介面中提供許多新項目：

新內容	地點
配置新工作負載的頁面	可從「常見任務」>「配置」取得
建立效能服務等級策略的頁面	可從 設定 > 策略 > 效能服務等級 取得
建立效能儲存效率策略的頁面	可從“設定”>“策略”>“儲存效率”存取
描述目前工作負載效能和工作負載 IOPS 的面板	可從儀表板取得

有關這些頁面和此功能的更多信息，請參閱產品中的線上說明。

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基於政策的儲存管理：

如果你想...	然後這樣做...
禁用基於策略的儲存管理	在*基於策略的儲存管理*面板中，將滑桿按鈕向左移動。
啟用基於策略的儲存管理	在*基於策略的儲存管理*面板中，將滑桿按鈕向右移動。

設定 Unified Manager 備份

您可以透過在主機系統和維護控制台上執行的一組設定步驟來設定 Unified Manager 上的備份功能。

有關配置步驟的信息，請參閱["管理備份和復原作業"](#)。

管理功能設定

透過「功能設定」頁面，您可以啟用和停用Active IQ Unified Manager中的特定功能。這包括根據策略建立和管理儲存物件、啟用 API 閘道和登入橫幅、上傳用於管理警報的腳本、根據不活動時間逾時 Web UI 會話以及停用接收Active IQ平台事件。



只有具有應用程式管理員角色的使用者才能使用「功能設定」頁面。

有關腳本上傳的信息，請參閱["啟用和停用腳本上傳"](#)。

啟用基於策略的儲存管理

*基於策略的儲存管理*選項允許基於服務等級目標 (SLO) 進行儲存管理。預設情況下啟用此選項。

啟動此功能後，您可以在新增至Active IQ Unified Manager實例的ONTAP叢集上設定儲存工作負載，並根據指派的效能服務等級和儲存效率原則管理這些工作負載。

您可以從*常規* > 功能設定 > *基於政策的儲存管理*選擇啟用或停用此功能。啟動此功能後，以下頁面可供操作和監控：

- 配置 (儲存工作負載配置)
- 政策 > 效能服務水準
- 政策 > 儲存效率
- 在叢集設定頁面上按效能服務等級管理的工作負載列
- *儀表板*上的工作負載效能面板

您可以使用這些畫面來建立效能服務等級和儲存效率策略，並配置儲存工作負載。您也可以監控符合指定效能服務等級的儲存工作負載以及不符合規定的儲存工作負載。工作負載效能和工作負載 IOPS 面板還可讓您根據資料中心內叢集所配置的儲存工作負載來評估叢集的總容量、可用容量和已使用容量及效能 (IOPS)。

啟動此功能後，您可以執行 Unified Manager REST API 來從 功能表列 > 說明按鈕 > **API** 文件 > 儲存提供者 類別執行其中一些功能。或者，您可以輸入主機名稱或 IP 位址以及存取 REST API 頁面的 URL，格式為 `https://<hostname>/docs/api/`

有關 API 的更多信息，請參閱["Active IQ Unified Manager REST API 入門"](#)。

啟用 API 網關

API 閘道功能可讓Active IQ Unified Manager作為單一控制平面，您可以從中管理多個ONTAP叢集，而無需單獨登入它們。

您可以從首次登入 Unified Manager 時出現的設定頁面啟用此功能。或者，您可以從*常規* > 功能設定 > *API 網關*啟用或停用此功能。

Unified Manager REST API 與ONTAP REST API 不同，並且並非所有ONTAP REST API 的功能都可以透過使用 Unified Manager REST API 來實現。但是，如果您有特定的業務需求，需要存取ONTAP API 來管理未向 Unified Manager 公開的特定功能，則可以啟用 API 閘道功能並執行ONTAP API。網關充當代理，透過維護與ONTAP API 相同的格式的標頭和正文請求來傳輸 API 請求。您可以使用 Unified Manager 憑證並執行特定的 API 來存取和管理ONTAP叢集，而無需傳遞單獨的叢集憑證。Unified Manager 作為單一管理點，在由 Unified Manager 實例管理的ONTAP叢集中執行 API。API 傳回的回應與直接從ONTAP執行的對應ONTAP REST API 傳回的回應相同。

啟用此功能後，您可以從 功能表列 > 說明按鈕 > **API** 文件 > 網關 類別執行 Unified Manager REST API。或者，您可以輸入主機名稱或 IP 位址以及 URL 來存取 REST API 頁面，格式如下 <https://<hostname>/docs/api/>

有關 API 的更多信息，請參閱"[Active IQ Unified Manager REST API 入門](#)"。

指定不活動逾時

您可以指定Active IQ Unified Manager的不活動逾時值。在指定時間不活動後，應用程式將自動登出。預設情況下啟用此選項。

您可以從*常規* > 功能設定 > 不活動逾時*停用此功能或修改時間。一旦啟動此功能，您應該在 ***LOGOUT AFTER*** 欄位中指定不活動的時間限制（以分鐘為單位），之後系統將自動登出。預設值為 4320 分鐘（72 小時）。



如果您啟用了安全性斷言標記語言 (SAML) 驗證，則此選項不可用。

啟用Active IQ入口網站事件

您可以指定是否要啟用或停用Active IQ入口網站事件。此設定允許Active IQ入口網站發現並顯示有關係統配置、佈線等的其他事件。預設情況下啟用此選項。

啟用此功能後，Active IQ Unified Manager將顯示Active IQ網站發現的事件。這些事件是透過針對所有受監控的儲存系統產生的AutoSupport訊息執行一組規則而建立的。這些事件與其他 Unified Manager 事件不同，它們識別與系統配置、佈線、最佳實踐和可用性問題相關的事件或風險。

您可以從 常規 > 功能設定 > 活動**Active IQ**入口網站事件*選擇啟用或停用此功能。在沒有外部網路存取的網站中，您必須從*儲存管理 > 事件設定 > *上傳規則*手動上傳規則。

此功能預設為啟用。停用此功能將阻止在 Unified Manager 上發現或顯示Active IQ事件。停用此功能後，啟用此功能可允許 Unified Manager 在該叢集時區的預先定義時間 00:15 接收叢集上的Active IQ事件。

啟用和停用安全設定以實現合規性

透過使用「功能設定」頁面的「安全儀表板」面板上的「自訂」按鈕，您可以啟用或停用 Unified Manager 上的合規性監控的安全性參數。

從此頁面啟用或停用的設定控制 Unified Manager 上叢集和儲存虛擬機器的整體合規性狀態。根據選擇，對應的列將顯示在叢集清單頁面的*安全性：所有叢集*視圖和儲存虛擬機器清單頁面的*安全性：所有儲存虛擬機器*視圖中。



只有具有管理員角色的使用者才能編輯這些設定。

您的ONTAP叢集、儲存虛擬機器和磁碟區的安全標準將根據"[NetApp ONTAP 9 安全強化指南](#)"。儀表板上的安全面板和安全性頁面顯示叢集、儲存虛擬機器和磁碟區的預設安全合規狀態。也會產生安全事件並針對存在安全違規的叢集和儲存虛擬機器啟用管理操作。

自訂安全設定

若要根據您的ONTAP環境自訂合規性監控設置，請依照下列步驟操作：

步驟

1. 點選*常規>功能設定>安全儀表板>自訂*。出現「自訂安全儀表板設定」彈出視窗。



您啟用或停用的安全性合規性參數會直接影響叢集和儲存虛擬機器畫面上的預設安全性視圖、報表和排程報告。如果您在修改安全參數之前從這些畫面上傳了 Excel 報告，則下載的 Excel 報告可能有錯誤。

2. 若要啟用或停用ONTAP叢集的自訂設置，請在 叢集 下選擇所需的常規設定。有關自訂叢集合規性的選項的信息，請參閱"[集群合規性類別](#)"。
3. 若要啟用或停用儲存虛擬機器的自訂設置，請在「儲存虛擬機器」下選擇所需的常規設定。有關自訂儲存虛擬機器合規性的選項的信息，請參閱"[儲存虛擬機器合規性類別](#)"。

自訂AutoSupport和身份驗證設置

在 * AutoSupport設定* 部分，您可以指定是否使用 HTTPS 傳送從ONTAP傳送AutoSupport訊息。

從「驗證設定」部分，您可以啟用 Unified Manager 警報來向預設ONTAP管理員使用者發出警報。

啟用和停用腳本上傳

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。如果您的組織出於安全原因不想允許此活動，您可以停用此功能。

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「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腳本：

如果你想...	然後這樣做...
停用腳本	在*腳本上傳*面板中，將滑桿按鈕向左移動。
啟用腳本	在*腳本上傳*面板中，將滑桿按鈕向右移動。

新增登入橫幅

新增登入橫幅使您的組織能夠顯示任何訊息，例如，誰被允許存取系統以及登入和登出期間的使用條款和條件。

任何使用者（例如儲存操作員或管理員）都可以在登入、登出和會話逾時期間查看此登入橫幅彈出視窗。

使用維護控制台

您可以使用維護控制台設定網路設定、設定和管理安裝了 Unified Manager 的系統，以及執行其他維護任務以協助您預防和排除可能出現的問題。

維護控制台提供哪些功能

Unified Manager 維護控制台可讓您維護 Unified Manager 系統上的設定並進行任何必要的變更以防止問題發生。

根據安裝 Unified Manager 的作業系統，維護控制台提供以下功能：

- 排除虛擬設備的任何問題，尤其是在 Unified Manager Web 介面不可用的情況下
- 升級到較新版本的 Unified Manager
- 產生支援包以發送給技術支持
- 設定網路設定
- 修改維護用戶密碼
- 連接到外部數據提供者以發送效能統計數據
- 更改性能數據收集內部
- 從先前備份的版本還原 Unified Manager 資料庫和設定。

維護用戶做什麼

維護使用者是在 Red Hat Enterprise Linux 系統上安裝 Unified Manager 期間建立的。維護用戶名是“umadmin”用戶。維護使用者在 Web UI 中具有應用程式管理員角色，並且該使用者可以建立後續使用者並為他們指派角色。

維護使用者或 umadmin 使用者也可以存取 Unified Manager 維護控制台。

診斷使用者功能

診斷存取的目的是使技術支援能夠幫助您進行故障排除，並且您只能在技術支援的指導下使用它。

診斷使用者可以在技術支援的指導下執行作業系統級命令，以進行故障排除。

存取維護控制台

如果 Unified Manager 使用者介面未執行，或者您需要執行使用者介面中不可用的功能，則可以存取維護控制台來管理 Unified Manager 系統。

開始之前

您必須已安裝並設定 Unified Manager。

15 分鐘不活動後，維護控制台將註銷您。



在 VMware 上安裝時，如果您已經透過 VMware 控制台以維護使用者身分登錄，則無法同時使用安全外殼登入。

步

1. 請依照下列步驟存取維護控制台：

在此作業系統上...	請依照以下步驟操作...
VMware	<ol style="list-style-type: none">使用安全性外殼連接到 Unified Manager 虛擬設備的 IP 位址或完全限定網域名稱。使用您的維護使用者名稱和密碼登入維護控制台。
Linux	<ol style="list-style-type: none">使用安全性外殼連接到 Unified Manager 系統的 IP 位址或完全限定網域名稱。使用維護使用者 (umadmin) 名稱和密碼登入系統。輸入命令 <code>`maintenance_console`</code> 然後按 Enter 鍵。
視窗	<ol style="list-style-type: none">使用管理員憑證登入 Unified Manager 系統。以 Windows 管理員身分啟動 PowerShell。輸入命令 <code>`maintenance_console`</code> 然後按 Enter 鍵。

顯示 Unified Manager 維護控制台選單。

使用 vSphere VM 控制台存取維護控制台

如果 Unified Manager 使用者介面未執行，或者您需要執行使用者介面中不可用的功能，則可以存取維護控制台來重新設定虛擬設備。

開始之前

- 您必須是維護使用者。
- 必須開啟虛擬設備才能存取維護控制台。

步驟

1. 在 vSphere Client 中，找到 Unified Manager 虛擬設備。
2. 按一下「控制台」標籤。
3. 按一下控制台視窗內部即可登入。
4. 使用您的使用者名稱和密碼登入維護控制台。

15 分鐘不活動後，維護控制台將註銷您。

維護控制台選單

維護控制台由不同的選單組成，可讓您維護和管理 Unified Manager 伺服器的特殊功能和設定設定。

根據安裝 Unified Manager 的作業系統，維護控制台包含下列選單：

- 升級 Unified Manager (僅限 VMware)
- 網路配置 (僅限 VMware)
- 系統配置 (僅限 VMware)
 - a. 支持/診斷
 - b. 重置伺服器憑證
 - c. 外部資料提供者
 - d. 備份還原
 - e. 效能輪詢間隔配置
 - f. 禁用 SAML 身份驗證
 - g. 查看/更改應用程式端口
 - h. 偵錯日誌配置
 - i. 控制對 MySQL 連接埠 3306 的訪問
 - j. 出口

您從清單中選擇數字來存取特定的選單選項。例如，對於備份和恢復，您選擇_4_。

網路設定選單

網路配置選單可讓您管理網路設定。當 Unified Manager 使用者介面不可用時，您應該使用此功能表。



如果 Unified Manager 安裝在 Red Hat Enterprise Linux 或 Microsoft Windows 上，則此功能表不可用。

有以下選單選項可供選擇。

- 顯示 IP 位址設定

顯示虛擬設備的目前網路設置，包括 IP 位址、網路、廣播位址、網路遮罩、網關和 DNS 伺服器。

- 更改 IP 位址設定

使您能夠更改虛擬設備的任何網路設置，包括 IP 位址、網路遮罩、網關或 DNS 伺服器。如果您使用維護控制台將網路設定從 DHCP 切換到靜態網路，則無法編輯主機名稱。您必須選擇“提交更改”才能使更改生效。

- 顯示網域搜尋設定

顯示用於解析主機名稱的網域搜尋清單。

- 更改網域搜尋設定

使您能夠變更解析主機名稱時要搜尋的網域名稱。您必須選擇“提交更改”才能使更改生效。

- 顯示靜態路由

顯示目前靜態網路路由。

- 更改靜態路由

使您能夠新增或刪除靜態網路路由。您必須選擇“提交更改”才能使更改生效。

- 新增路線

使您能夠新增靜態路由。

- 刪除路線

使您能夠刪除靜態路由。

- 後退

帶您返回*主選單*。

- 出口

退出維護控制台。

- 停用網路介面

停用任何可用的網路介面。如果只有一個網路介面可用，則無法停用它。您必須選擇“提交更改”才能使更改生效。

- 啟用網路介面

啟用可用的網路介面。您必須選擇“提交更改”才能使更改生效。

- 提交更改

應用對虛擬設備的網路設定所做的任何變更。您必須選擇此選項才能實施所做的任何更改，否則不會發生更改。

- **Ping** 主機

對目標主機執行 ping 操作以確認 IP 位址變更或 DNS 配置。

- 恢復預設值

將所有設定重設為出廠預設值。您必須選擇“提交更改”才能使更改生效。

- 後退

帶您返回*主選單*。

- 出口

退出維護控制台。

系統配置選單

系統配置選單提供各種選項，例如查看伺服器狀態以及重新啟動和關閉虛擬機，使您能夠管理虛擬設備。



當 Unified Manager 安裝在 Linux 或 Microsoft Windows 系統上時，此功能表中只有「從 Unified Manager 備份還原」選項可用。

有以下選單選項可供選擇：

- 顯示伺服器狀態

顯示目前伺服器狀態。狀態選項包括“正在運行”和“未運行”。

如果伺服器沒有運行，您可能需要聯絡技術支援。

- 重啟虛擬機器

重新啟動虛擬機，停止所有服務。重啟後，虛擬機器和服務重新啟動。

- 關閉虛擬機器

關閉虛擬機，停止所有服務。

您只能從虛擬機器控制台選擇此選項。

- 更改<登入使用者>的使用者密碼

更改目前登入使用者的密碼，該使用者只能是維護使用者。

- 增加資料磁碟大小

增加虛擬機器中資料磁碟（磁碟 3）的大小。

- *增加交換磁碟大小

增加虛擬機器中交換磁碟（磁碟 2）的大小。

- 更改時區

將時區變更為您的位置。

- 更改 **NTP** 伺服器

變更 NTP 伺服器設置，例如 IP 位址或完全限定網域名稱 (FQDN)。

- 更改 **NTP** 服務

在 `ntp` 和 `systemd-timesyncd` 服務。

- 從統一管理器備份還原

從先前備份的版本還原 Unified Manager 資料庫和設定。

- 重置伺服器憑證

重置伺服器安全性憑證。

- 更改主機名稱

變更安裝虛擬設備的主機的名稱。

- 後退

退出系統配置選單並返回主選單。

- 出口

退出維護控制台選單。

支援和診斷選單

透過「支援和診斷」選單，您可以產生支援包，然後將其發送給技術支援以獲得故障排除幫助。

有以下選單選項可用：

- 產生輕量級支援包

使您能夠產生僅包含 30 天的日誌和設定資料庫記錄的輕量級支援包 - 它不包括效能資料、擷取記錄檔和伺服器堆轉儲。

- 產生支援包

使您能夠在診斷使用者的主目錄中建立包含診斷資訊的完整支援包（7-Zip 檔案）。如果您的系統已連接到互聯網，您也可以將支援包上傳到NetApp。

該檔案包括由AutoSupport訊息產生的資訊、Unified Manager 資料庫的內容、有關 Unified Manager 伺服器內部的詳細資料以及AutoSupport訊息或輕量級支援套件中通常不包含的詳細等級日誌。

附加選單選項

以下功能表選項可讓您在 Unified Manager 伺服器上執行各種管理任務。

有以下選單選項可供選擇：

- 重置伺服器憑證

重新產生 HTTPS 伺服器憑證。

您可以透過點選 常規 > **HTTPS** 憑證 > 重新產生 **HTTPS** 憑證 在 Unified Manager GUI 中重新產生伺服器憑證。

- 停用 **SAML** 驗證

停用 SAML 驗證，以便身分提供者 (IdP) 不再為存取 Unified Manager GUI 的使用者提供登入驗證。當 IdP 伺服器或 SAML 設定問題阻止使用者存取 Unified Manager GUI 時，通常會使用此控制台選項。

- 外部資料提供者

提供將 Unified Manager 連接到外部資料提供者的選項。建立連接後，效能數據將發送到外部伺服器，以便儲存效能專家可以使用第三方軟體繪製效能指標圖表。將顯示以下選項：

- 顯示伺服器配置 - 顯示外部資料提供者的目前連線和設定。
- 新增/修改伺服器連線 - 使您能夠為外部資料提供者輸入新的連線設置，或變更現有設定。
- 修改伺服器配置 - 使您能夠為外部資料提供者輸入新的配置設置，或變更現有設定。
- 刪除伺服器連線 - 刪除與外部資料提供者的連線。

刪除連線後，Unified Manager 將失去與外部伺服器的連線。

- 備份還原

有關信息，請參閱以下主題"[管理備份和復原作業](#)"。

- 效能輪詢間隔配置

提供一個選項來設定 Unified Manager 從叢集收集效能統計資料的頻率。預設收集間隔為5分鐘。

如果您發現大型叢集的收集沒有按時完成，則可以將此間隔變更為 10 或 15 分鐘。

- 查看/更改應用程式連接埠

如果出於安全考慮，提供一個選項來更改 Unified Manager 用於 HTTP 和 HTTPS 協定的預設連接埠。HTTP 的預設連接埠為 80，HTTPS 的預設連接埠為 443。

- 控制對 **MySQL** 連接埠 **3306** 的存取

控制主機對預設 MySQL 連接埠 3306 的存取。基於安全性原因，在 Linux、Windows 和 VMware vSphere 系統上全新安裝 Unified Manager 期間，透過此連接埠的存取僅限於本機。此選項使您能夠在本地主機和遠端主機之間切換此端口的可見性，也就是說，如果僅在您的環境中為本地主機啟用了該端口，那麼您也可以使該端口對遠端主機可用。或者，當為所有主機啟用時，您可以將此連接埠的存取權限制為僅限本機主機。如果之前在遠端主機上啟用了訪問，則在升級場景中將保留該配置。切換連接埠可見性後，您應該檢查 Windows 系統上的防火牆設置，如果設定配置為限制對 MySQL 連接埠 3306 的訪問，則應停用防火牆設置。

- 出口

退出維護控制台選單。

在 **Windows** 上變更維護使用者密碼

您可以在需要時變更 Unified Manager 維護使用者密碼。

步驟

1. 在 Unified Manager Web UI 登入頁面上，按一下「忘記密碼」。

將顯示一個頁面，提示您輸入要重設密碼的使用者的姓名。

2. 輸入使用者名稱並點擊*提交*。

一封包含重設密碼連結的電子郵件將傳送至為該使用者名稱定義的電子郵件地址。

3. 點擊電子郵件中的*重設密碼連結*並定義新密碼。
4. 返回 Web UI 並使用新密碼登入 Unified Manager。

在 **Linux** 系統上變更 **umadmin** 密碼

出於安全原因，您必須在完成安裝程序後立即變更 Unified Manager umadmin 使用者的預設密碼。如果需要，您可以隨時再次變更密碼。

開始之前

- Unified Manager 必須安裝在 Red Hat Enterprise Linux Linux 系統上。
- 您必須擁有安裝了 Unified Manager 的 Linux 系統的 root 使用者憑證。

步驟

1. 以 root 使用者身分登入執行 Unified Manager 的 Linux 系統。
2. 更改 umadmin 密碼：


```
passwd umadmin
```

系統提示您輸入 umadmin 使用者的新密碼。

更改 Unified Manager 用於 HTTP 和 HTTPS 協定的端口

如果出於安全性考慮，可以在安裝後變更 Unified Manager 用於 HTTP 和 HTTPS 協定的預設連接埠。HTTP 的預設連接埠為 80，HTTPS 的預設連接埠為 443。

開始之前

您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。



使用 Mozilla Firefox 或 Google Chrome 瀏覽器時，某些連接埠被認為是不安全的。在為 HTTP 和 HTTPS 流量指派新的連接埠號碼之前，請先檢查您的瀏覽器。選擇不安全的連接埠可能會導致系統無法存取，這需要您聯絡客戶支援尋求解決方案。

變更連接埠後，Unified Manager 實例會自動重新啟動，因此請確保這是一個短時間關閉系統的好時機。

1. 使用 SSH 以維護使用者身分登入 Unified Manager 主機。

將顯示 Unified Manager 維護控制台提示。

2. 鍵入標示 檢視/變更應用程式連接埠 的選單選項的編號，然後按 Enter。
3. 如果出現提示，請再次輸入維護使用者密碼。
4. 鍵入 HTTP 和 HTTPS 連接埠的新連接埠號，然後按 Enter。

將連接埠號留空將為協定分配預設連接埠。

系統會提示您是否要立即變更連接埠並重新啟動 Unified Manager。

5. 鍵入 **y** 以變更連接埠並重新啟動 Unified Manager。
6. 退出維護控制台。

完成此變更後，使用者必須在 URL 中包含新的連接埠號碼才能存取 Unified Manager Web UI，例如 + <https://host.company.com:1234+>或 [https://\[2001:db8:0:1\]:2123](https://[2001:db8:0:1]:2123)。

新增網路介面

如果需要分離網路流量，可以新增新的網路介面。

開始之前

您必須已使用 vSphere 將網路介面新增至虛擬設備。

虛擬設備必須已開啟電源。



如果 Unified Manager 安裝在 Red Hat Enterprise Linux 或 Microsoft Windows 上，則無法執行此操作。

步驟

1. 在 vSphere 控制台主選單中，選擇 系統配置 > 重新啟動作業系統。

重新啟動後，維護控制台可以偵測到新新增的網路介面。

2. 存取維護控制台。
3. 選擇*網路設定* > 啟用網路介面。
4. 選擇新的網路介面並按 **Enter**。

選擇 **eth1** 並按 **Enter**。

5. 輸入 **y** 以啟用網路介面。
6. 輸入網路設定。

如果使用靜態介面或未偵測到 DHCP，系統將提示您輸入網路設定。

進入網路設定後，自動返回*網路設定*選單。

7. 選擇*提交更改*。

您必須提交變更才能新增網路介面。

向 Unified Manager 資料庫目錄新增磁碟空間

Unified Manager 資料庫目錄包含從ONTAP系統收集的所有健康和效能資料。某些情況下可能需要您增加資料庫目錄的大小。

例如，如果 Unified Manager 從大量叢集（每個叢集都有許多節點）收集數據，則資料庫目錄可能會已滿。當資料庫目錄已滿 90% 時，您將收到警告事件；當資料庫目錄已滿 95% 時，您將收到嚴重事件。



當目錄達到 95% 滿度後，將不再從群集收集其他資料。

根據 Unified Manager 是在 VMware ESXi 伺服器、Red Hat 伺服器還是 Microsoft Windows 伺服器上執行，為資料目錄新增容量所需的步驟會有所不同。

為Linux主機的資料目錄新增空間

如果您分配的磁碟空間不足 `/opt/netapp/data` 目錄以支援 Unified Manager，當您最初設定 Linux 主機然後安裝 Unified Manager 時，您可以在安裝後透過增加 `/opt/netapp/data` 目錄。

開始之前

您必須具有安裝了 Unified Manager 的 Red Hat Enterprise Linux 機器的 root 使用者存取權。

我們建議您在增加資料目錄的大小之前備份 Unified Manager 資料庫。

步驟

1. 以 root 使用者身分登入要新增磁碟空間的 Linux 機器。
2. 以所示順序停止 Unified Manager 服務和相關的 MySQL 軟體：

```
systemctl stop ocieau ocie mysqld
```

3. 建立臨時備份資料夾（例如， /backup-data ）具有足夠的磁碟空間來包含當前 /opt/netapp/data 目錄。
4. 複製現有 /opt/netapp/data 目錄到備份資料目錄：

```
cp -arp /opt/netapp/data/* /backup-data
```

5. 如果啟用了 SE Linux：

- a. 取得現有資料夾的 SE Linux 類型 /opt/netapp/data 資料夾：

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

系統傳回類似如下的確認訊息：

```
echo $se_type  
mysqld_db_t
```

- a. 執行 chcon 指令設定備份目錄的 SE Linux 類型：

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 刪除 /opt/netapp/data 目錄：

- a. cd /opt/netapp/data
- b. rm -rf *

7. 擴大規模 /opt/netapp/data 透過 LVM 指令或新增額外的磁碟將目錄大小增加到至少 150 GB。



如果您已經創建 /opt/netapp/data 從磁碟，那麼您不應該嘗試安裝 /opt/netapp/data 作為 NFS 或 CIFS 共享。因為在這種情況下，如果您嘗試擴展磁碟空間，則一些 LVM 命令，例如 'resize' 和 'extend' 可能無法如預期工作。

8. 確認 /opt/netapp/data 目錄擁有者（mysql）和群組（root）保持不變：

```
ls -ltr /opt/netapp/ | grep data
```

系統傳回類似如下的確認訊息：

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. 如果啟用了 SE Linux，請確認 /opt/netapp/data 目錄仍然設定為 mysqld_db_t：

- a. touch /opt/netapp/data/abc

```
b. ls -Z /opt/netapp/data/abc
```

系統傳回類似如下的確認訊息：

```
-rw-r--r--. root root unconfined_u:object_r:mysql_d_db_t:s0  
/opt/netapp/data/abc
```

10. 刪除檔案 abc，以便這個無關的檔案將來不會導致資料庫錯誤。

11. 將備份資料中的內容複製回擴充的 `/opt/netapp/data` 目錄：

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. 如果啟用了 SE Linux，請執行以下命令：

```
chcon -R --type=mysql_d_db_t /opt/netapp/data
```

13. 啟動 MySQL 服務：

```
systemctl start mysqld
```

14. MySQL服務啟動後，依照所示順序啟動ocie和ocieau服務：

```
systemctl start ocie ocieau
```

15. 所有服務啟動後，刪除備份資料夾 /backup-data：

```
rm -rf /backup-data
```

為VMware虛擬機器資料盤新增空間

如果需要增加 Unified Manager 資料庫的資料磁碟空間量，則可以在安裝後使用 Unified Manager 維護控制台增加磁碟空間來增加容量。

開始之前

- 您必須具有 vSphere Client 的存取權限。
- 虛擬機器一定不能有任何本地儲存的快照。
- 您必須擁有維護使用者憑證。

我們建議您在增加虛擬磁碟的大小之前備份虛擬機器。

步驟

1. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後在資料中新增更多磁碟容量 disk 3。有關詳細信息，請參閱 VMware 文件。

在極少數情況下，Unified Manager 部署使用「硬碟 2」而不是「硬碟 3」作為資料磁碟。如果您的部署中出現這種情況，請增加較大磁碟的空間。資料磁碟的空間總是比其他磁碟大。

2. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後選擇「控制台」標籤。
3. 按一下控制台窗口，然後使用您的使用者名稱和密碼登入維護控制台。
4. 在主選單中，輸入*系統配置*選項的編號。
5. 在系統設定選單中，輸入「增加資料磁碟大小」選項的數字。

為 Microsoft Windows 伺服器的邏輯磁碟機新增空間

如果需要增加 Unified Manager 資料庫的磁碟空間量，您可以為安裝 Unified Manager 的邏輯磁碟機新增容量。

開始之前

您必須具有 Windows 管理員權限。

我們建議您在新增磁碟空間之前備份 Unified Manager 資料庫。

步驟

1. 以管理員身分登入要新增磁碟空間的 Windows 伺服器。
2. 按照與您想要使用的方法相對應的步驟來增加更多空間：

選項	描述
在實體伺服器上，為安裝 Unified Manager 伺服器的邏輯磁碟機新增容量。	請依照 Microsoft 主題中的步驟操作： "擴充基本捲"
在實體伺服器上，新增硬碟。	請依照 Microsoft 主題中的步驟操作： "新增硬碟驅動器"
在虛擬機器上，增加磁碟分割的大小。	請按照 VMware 主題中的步驟操作： "增加磁碟分割區的大小"

管理用戶訪問

您可以建立角色並指派功能來控制使用者對 Active IQ Unified Manager 的存取。您可以識別具有存取 Unified Manager 中選取物件所需權限的使用者。只有擁有這些角色和功能的使用者才能管理 Unified Manager 中的物件。

新增用戶

您可以使用「使用者」頁面新增本機使用者或資料庫使用者。您也可以新增屬於身份驗證伺服器的遠端使用者或群組。您可以為這些使用者指派角色，並且根據角色的權限，使用者可以使用 Unified Manager 管理儲存物件和數據，或查看資料庫中的資料。

開始之前

- 您必須具有應用程式管理員角色。
- 若要新增遠端使用者或群組，您必須啟用遠端身份驗證並設定身份驗證伺服器。
- 如果您打算設定 SAML 驗證，以便身分提供者 (IdP) 對存取圖形介面的使用者進行身份驗證，請確保這些使用者被定義為「遠端」使用者。

啟用 SAML 身份驗證時，「本機」或「維護」類型的使用者無法存取 UI。

如果您從 Windows Active Directory 新增一個群組，則所有直接成員和巢狀子群組都可以向 Unified Manager 進行驗證，除非巢狀子群組已停用。如果您從 OpenLDAP 或其他驗證服務新增一個群組，則只有該群組的直接成員才能向 Unified Manager 進行驗證。

步驟

1. 在左側導覽窗格中，按一下「常規」>「使用者」。
2. 在「使用者」頁面上，按一下「新增」。
3. 在新增使用者對話方塊中，選擇要新增的使用者類型，然後輸入所需的資訊。

輸入所需的使用者資訊時，您必須指定該使用者唯一的電子郵件地址。您必須避免指定由多個使用者共用的電子郵件地址。

4. 按一下“新增”。

建立資料庫用戶

若要支援工作流程自動化和 Unified Manager 之間的連接，或存取資料庫視圖，您必須先在 Unified Manager Web UI 中建立具有整合模式或報表模式角色的資料庫使用者。

開始之前

您必須具有應用程式管理員角色。

資料庫使用者提供與工作流程自動化的整合以及對特定於報告的資料庫視圖的存取。資料庫使用者無權存取 Unified Manager Web UI 或維護控制台，也無法執行 API 呼叫。

步驟

1. 在左側導覽窗格中，按一下「常規」>「使用者」。
2. 在「使用者」頁面中，按一下「新增」。
3. 在新增使用者對話方塊中，在*類型*下拉清單中選擇*資料庫使用者*。
4. 輸入資料庫使用者的名稱和密碼。
5. 在*角色*下拉清單中，選擇適當的角色。

如果您是...	選擇此角色
將 Union Manager 與工作流程自動化連接起來	整合模式
存取報告和其他資料庫視圖	報告架構

6. 按一下“新增”。

編輯用戶設定

您可以編輯每個使用者指定的使用者設置，例如電子郵件地址和角色。例如，您可能想要變更儲存操作員使用者的角色，並為該使用者指派儲存管理員權限。

開始之前

您必須具有應用程式管理員角色。

修改指派給使用者的角色時，發生下列任一操作時都會套用變更：

- 使用者登出並重新登入 Unified Manager。
- 會話逾時已達 24 小時。

步驟

1. 在左側導覽窗格中，按一下「常規」>「使用者」。
2. 在「用戶」頁面中，選擇要編輯設定的用戶，然後按一下「編輯」。
3. 在「編輯使用者」對話方塊中，編輯為使用者指定的適當設定。
4. 點選“儲存”。

查看用戶

您可以使用「使用者」頁面查看使用 Unified Manager 管理儲存物件和資料的使用者清單。您可以查看有關使用者的詳細信息，例如使用者名稱、使用者類型、電子郵件地址以及指派給使用者的角色。

開始之前

您必須具有應用程式管理員角色。

步

1. 在左側導覽窗格中，按一下「常規」>「使用者」。

刪除使用者或群組

您可以從管理伺服器資料庫中刪除一個或多個用戶，以防止特定用戶存取 Unified Manager。您也可以刪除群組，以便群組中的所有使用者都無法再存取管理伺服器。

開始之前

- 刪除遠端群組時，您必須重新指派已指派給遠端群組使用者的事件。
如果您刪除本機用戶或遠端用戶，則指派給這些用戶的事件將自動取消指派。
- 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「常規」>「使用者」。
2. 在「使用者」頁面中，選擇要刪除的使用者或群組，然後按一下「刪除」。
3. 點選“是”確認刪除。

什麼是 RBAC

RBAC（基於角色的存取控制）可以控制誰有權存取Active IQ Unified Manager伺服器中的各種功能和資源。

基於角色的存取控制的作用

基於角色的存取控制 (RBAC) 使管理員能夠透過定義角色來管理使用者群組。如果您需要限制選定管理員對特定功能的訪問，則必須為他們設定管理員帳戶。如果您想要限制管理員可以查看的資訊和可以執行的操作，您必須將角色套用到您建立的管理員帳戶。

管理伺服器使用RBAC進行使用者登入和角色權限。如果您沒有更改管理伺服器的管理用戶存取的預設設置，則無需登入即可查看它們。

當您啟動需要特定權限的操作時，管理伺服器會提示您登入。例如，要建立管理員帳戶，您必須使用應用程式管理員帳戶存取權限登入。

使用者類型的定義

使用者類型指定使用者持有的帳戶類型，包括遠端使用者、遠端群組、本機使用者、資料庫使用者和維護使用者。每種類型都有自己的角色，由具有管理員角色的使用者分配。

Unified Manager 使用者類型如下：

- 維護使用者

在 Unified Manager 的初始設定期間建立。然後，維護使用者建立其他使用者並指派角色。維護使用者也是唯一有權存取維護控制台的使用者。當 Unified Manager 安裝在 Red Hat Enterprise Linux 系統上時，維護使用者的使用者名稱為「umadmin」。

- 本地用戶

存取 Unified Manager UI 並根據維護使用者或具有應用程式管理員角色的使用者授予的角色執行功能。

- 遠端組

使用儲存在驗證伺服器上的憑證存取 Unified Manager UI 的一組使用者。該帳戶的名稱應與身份驗證伺服器上儲存的群組的名稱相符。遠端群組內的所有使用者都可以使用各自的使用者憑證存取 Unified Manager UI。遠端群組可以根據指派的角色執行功能。

- 遠端使用者

使用儲存在驗證伺服器上的憑證存取 Unified Manager UI。遠端使用者根據維護使用者或具有應用程式管理員角色的使用者賦予的角色執行功能。

- 資料庫使用者

對 Unified Manager 資料庫中的資料具有唯讀存取權限，但無法存取 Unified Manager Web 介面或維護控制台，也無法執行 API 呼叫。

使用者角色的定義

維護使用者或應用程式管理員為每個使用者指派一個角色。每個角色都包含一定的權限。您可以在 Unified Manager 中執行的活動範圍取決於您被指派的角色以及該角色所包含的權限。

Unified Manager 包含以下預先定義使用者角色：

- 操作員

查看儲存系統資訊和 Unified Manager 收集的其他數據，包括歷史記錄和容量趨勢。此角色使儲存操作員能夠查看、指派、確認、解決事件並新增註釋。

- 存儲管理員

在 Unified Manager 中設定儲存管理操作。此角色使儲存管理員能夠配置閾值並建立警報和其他特定於儲存管理的選項和策略。

- 應用程式管理員

配置與儲存管理無關的設定。此角色可以管理使用者、安全性憑證、資料庫存取和管理選項，包括身份驗證、SMTP、網路和AutoSupport。



當 Unified Manager 安裝在 Linux 系統上時，具有應用程式管理員角色的初始使用者將自動命名為「umadmin」。

- 整合模式

此角色允許對 Unified Manager 資料庫視圖進行唯讀訪問，以便將 Unified Manager 與OnCommand Workflow Automation (WFA) 整合。

- 報告架構

此角色允許直接從 Unified Manager 資料庫對報表和其他資料庫視圖進行唯讀存取。可以查看的資料庫包括：

- netapp_model_view
- netapp_效能
- 奧庫姆
- ocum_報告
- ocum_report_birt
- 操作
- 規模監控器

Unified Manager 使用者角色和功能

根據您指派的使用者角色，您可以決定可以在 Unified Manager 中執行哪些操作。

下表顯示了每個使用者角色可以執行的功能：

功能	操作員	儲存管理員	應用程式管理員	整合模式	報告架構
查看儲存系統資訊	•	•	•	•	•
查看其他數據，例如歷史記錄和容量趨勢	•	•	•	•	•
查看、分配和解決事件	•	•	•		
檢視儲存服務對象，例如 SVM 關聯和資源池	•	•	•		
查看閾值策略	•	•	•		
管理儲存服務對象，例如 SVM 關聯和資源池		•	•		
定義警報		•	•		
管理儲存管理選項		•	•		
管理儲存管理策略		•	•		
管理用戶			•		
管理管理選項			•		
定義閾值策略			•		
管理資料庫訪問			•		
管理與 WFA 的整合並提供對資料庫視圖的訪問				•	

功能	操作員	儲存管理員	應用程式管理員	整合模式	報告架構
安排和保存報告		•	•		
從管理操作執行「修復」操作		•	•		
提供對資料庫視圖的唯讀存取權限					•

管理 SAML 身份驗證設定

設定遠端驗證設定後，您可以啟用安全性斷言標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前由安全性身分提供者 (IdP) 進行驗證。

請注意，啟用 SAML 身份驗證後，只有遠端使用者才能存取 Unified Manager 圖形使用者介面。本機用戶和維護用戶將無法存取 UI。此配置不會影響存取維護控制台的使用者。

身份提供者要求

當設定 Unified Manager 使用身分提供者 (IdP) 為所有遠端使用者執行 SAML 驗證時，您需要了解一些必要的設定設置，以便成功連線到 Unified Manager。

您必須將 Unified Manager URI 和元資料輸入到 IdP 伺服器中。您可以從 Unified Manager SAML 驗證頁面複製此資訊。Unified Manager 被視為安全斷言標記語言 (SAML) 標準中的服務提供者 (SP)。

支援的加密標準

- 高級加密標準 (AES)：AES-128 和 AES-256
- 安全雜湊演算法 (SHA)：SHA-1 和 SHA-256

經過驗證的身份提供者

- 口令
- Active Directory 聯合驗證服務 (ADFS)

ADFS 設定要求

- 您必須依照下列順序定義三個宣告規則，Unified Manager 需要這些規則來解析此依賴方信任項目的 ADFS SAML 回應。

聲明規則	價值
SAM 帳戶名稱	姓名 ID

聲明規則	價值
SAM 帳戶名稱	urn:oid:0.9.2342.19200300.100.1.1
令牌組——非限定名稱	urn : oid : 1.3.6.1.4.1.5923.1.5.1.1

- 您必須將身份驗證方法設定為「表單驗證」，否則使用者在退出 Unified Manager 時可能會收到錯誤。請依照以下步驟操作：
 - a. 開啟 ADFS 管理控制台。
 - b. 點選左側樹狀視圖上的身份驗證策略資料夾。
 - c. 在右側的操作下，按一下編輯全域主要驗證策略。
 - d. 將 Intranet 驗證方法設定為「表單驗證」而不是預設的「Windows 驗證」。
- 在某些情況下，當 Unified Manager 安全性憑證由 CA 簽署時，透過 IdP 登入會被拒絕。有兩種解決方法可以解決此問題：
 - 依照連結中的說明，停用 ADFS 伺服器上與鍊式 CA 憑證關聯的信賴方的撤銷檢查：

["停用每個依賴方信任的撤銷檢查"](#)
 - 讓 CA 伺服器駐留在 ADFS 伺服器內以簽署 Unified Manager 伺服器憑證要求。

其他配置要求

- Unified Manager 時鐘偏差設定為 5 分鐘，因此 IdP 伺服器和 Unified Manager 伺服器之間的時間差不能超過 5 分鐘，否則驗證會失敗。

啟用 SAML 身份驗證

您可以啟用安全性斷言標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前先透過安全性身分提供者 (IdP) 進行驗證。

開始之前

- 您必須已配置遠端身份驗證並驗證其是否成功。
- 您必須至少建立一個具有應用程式管理員角色的遠端使用者或遠端群組。
- 身分提供者 (IdP) 必須受 Unified Manager 支持，並且必須進行設定。
- 您必須擁有 IdP URL 和元資料。
- 您必須有權存取 IdP 伺服器。

從 Unified Manager 啟用 SAML 驗證後，使用者無法存取圖形使用者介面，直到使用 Unified Manager 伺服器主機資訊設定 IdP。因此，您必須準備好在開始設定程序之前完成連接的兩個部分。可以在設定 Unified Manager 之前或之後設定 IdP。

啟用 SAML 身份驗證後，只有遠端使用者才能存取 Unified Manager 圖形使用者介面。本機用戶和維護用戶將無法存取 UI。此配置不會影響存取維護控制台、Unified Manager 命令或 ZAPI 的使用者。



完成此頁面上的 SAML 設定後，Unified Manager 將自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML 驗證**」。
2. 選取「啟用 SAML 身份驗證」複選框。

顯示配置 IdP 連線所需的欄位。

3. 輸入將 Unified Manager 伺服器連接到 IdP 伺服器所需的 IdP URI 和 IdP 元資料。

如果可以從 Unified Manager 伺服器直接存取 IdP 伺服器，則可以在輸入 IdP URI 後按一下取得 **IdP** 元資料按鈕以自動填入 IdP 元資料欄位。

4. 複製 Unified Manager 主機元資料 URI，或將主機元資料儲存到 XML 文字檔案。

現在您可以使用此資訊來設定 IdP 伺服器。

5. 點選“儲存”。

將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

6. 點選*確認並登出*，Unified Manager 將重新啟動。

下次授權遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 IdP 登入頁面而不是 Unified Manager 登入頁面中輸入其憑證。

如果尚未完成，請造訪您的 IdP 並輸入 Unified Manager 伺服器 URI 和元資料以完成設定。



當使用 ADFS 作為身分提供者時，Unified Manager GUI 不遵守 ADFS 逾時，並將繼續運作，直到達到 Unified Manager 會話逾時。您可以透過點擊 常規 > 功能設定 > 不活動逾時 來變更 GUI 會話逾時。

更改用於 **SAML** 身份驗證的身分提供者

您可以變更 Unified Manager 用於對遠端使用者進行身份驗證的身分提供者 (IdP)。

開始之前

- 您必須擁有 IdP URL 和元資料。
- 您必須有權存取 IdP。

可以在設定 Unified Manager 之前或之後設定新的 IdP。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML 驗證**」。
2. 輸入新的 IdP URI 以及將 Unified Manager 伺服器連接到 IdP 所需的 IdP 元資料。

如果可以直接從 Unified Manager 伺服器存取 IdP，則可以在輸入 IdP URL 後按一下取得 **IdP** 元資料 按鈕以自動填入 IdP 元資料欄位。

3. 複製 Unified Manager 元資料 URI，或將元資料儲存到 XML 文字檔案。

4. 按一下“儲存配置”。

將顯示一個訊息框來確認您是否要變更配置。

5. 按一下“確定”。

存取新的 IdP 並輸入 Unified Manager 伺服器 URI 和元資料以完成設定。

下次授權的遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在新的 IdP 登入頁面而不是舊的 IdP 登入頁面中輸入其憑證。

Unified Manager 安全性憑證變更後更新 SAML 驗證設定

對 Unified Manager 伺服器上安裝的 HTTPS 安全性憑證的任何變更都會要求您更新 SAML 驗證設定。如果您重新命名主機系統、為主機系統指派新的 IP 位址或手動變更系統的安全性證書，則證書會更新。

變更安全性憑證並重新啟動 Unified Manager 伺服器後，SAML 驗證將無法運作，使用者將無法存取 Unified Manager 圖形介面。您必須更新 IdP 伺服器和 Unified Manager 伺服器上的 SAML 驗證設定才能重新啟用對使用者介面的存取。

步驟

1. 登入維護控制台。

2. 在*主選單*中，輸入*停用 SAML 驗證*選項的號碼。

將顯示一則訊息，確認您要停用 SAML 驗證並重新啟動 Unified Manager。

3. 使用更新的 FQDN 或 IP 位址啟動 Unified Manager 使用者介面，將更新後的伺服器憑證接受到瀏覽器中，然後使用維護使用者憑證登入。

4. 在*設定/驗證*頁面中，選擇*SAML 驗證*標籤並設定 IdP 連線。

5. 複製 Unified Manager 主機元資料 URI，或將主機元資料儲存到 XML 文字檔案。

6. 點選“儲存”。

將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

7. 點選*確認並登出*，Unified Manager 將重新啟動。

8. 存取您的 IdP 伺服器並輸入 Unified Manager 伺服器 URI 和元資料以完成設定。

身分提供者	設定步驟
ADFS	<ol style="list-style-type: none"> 刪除 ADFS 管理 GUI 中現有的依賴方信任條目。 使用 `saml_sp_metadata.xml` 來自更新的 Unified Manager 伺服器。 定義 Unified Manager 解析此依賴方信任條目的 ADFS SAML 回應所需的三個聲明規則。 重新啟動 ADFS Windows 服務。
口令	<ol style="list-style-type: none"> 將 Unified Manager 伺服器的新 FQDN 更新到 `attribute-filter.xml` 和 `relying-party.xml` 文件。 重新啟動 Apache Tomcat Web 伺服器並等待連接埠 8005 上線。

9. 登入 Unified Manager 並透過您的 IdP 驗證 SAML 身份驗證是否如預期運作。

禁用 SAML 身份驗證

當您想要在遠端使用者登入 Unified Manager Web UI 之前停止透過安全性身分提供者 (IdP) 對其進行驗證時，可以停用 SAML 驗證。當停用 SAML 驗證時，設定的目錄服務提供者（例如 Active Directory 或 LDAP）將執行登入驗證。

停用 SAML 身份驗證後，除了配置的遠端使用者之外，本機使用者和維護使用者也將能夠存取圖形使用者介面。

如果您無法存取圖形使用者介面，您也可以使用 Unified Manager 維護控制台停用 SAML 驗證。



停用 SAML 驗證後，Unified Manager 會自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML 驗證**」。
2. 取消選取*啟用 SAML 驗證*複選框。
3. 點選“儲存”。

將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

4. 點選*確認並登出*，Unified Manager 將重新啟動。

下次遠端使用者嘗試造訪 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而不是 IdP 登入頁面輸入其憑證。

存取您的 IdP 並刪除 Unified Manager 伺服器 URI 和元資料。

從維護控制台停用 SAML 驗證

當無法存取 Unified Manager GUI 時，您可能需要從維護控制台停用 SAML 驗證。如果配置錯誤或無法存取 IdP，則可能會發生這種情況。

開始之前

您必須以維護使用者身分存取維護控制台。

當停用 SAML 驗證時，設定的目錄服務提供者（例如 Active Directory 或 LDAP）將執行登入驗證。除了配置的遠端使用者之外，本機使用者和維護使用者也能夠存取圖形使用者介面。

您也可以從 UI 中的設定/身份驗證頁面停用 SAML 身份驗證。



停用 SAML 驗證後，Unified Manager 會自動重新啟動。

步驟

1. 登入維護控制台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的號碼。

將顯示一則訊息，確認您要停用 SAML 驗證並重新啟動 Unified Manager。

3. 鍵入 **y**，然後按 Enter，Unified Manager 將重新啟動。

下次遠端使用者嘗試造訪 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而不是 IdP 登入頁面輸入其憑證。

如果需要，請造訪您的 IdP 並刪除 Unified Manager 伺服器 URL 和元資料。

SAML 身份驗證頁面

您可以使用 SAML 驗證頁面設定 Unified Manager，以便透過安全身分提供者 (IdP) 使用 SAML 對遠端使用者進行驗證，然後他們才能登入 Unified Manager Web UI。

- 您必須具有應用程式管理員角色才能建立或修改 SAML 設定。
- 您必須已設定遠端身份驗證。
- 您必須至少配置一個遠端使用者或遠端群組。

設定遠端驗證和遠端使用者後，您可以勾選啟用 SAML 驗證核取方塊以使用安全性身分提供者啟用身分驗證。

• IdP URI

從 Unified Manager 伺服器存取 IdP 的 URI。下面列出了範例 URI。

ADFS 範例 URI：

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Shibboleth 範例 URI：

`https://centos7.ntap2016.local/idp/shibboleth`

- **IdP 元資料**

XML 格式的 IdP 元資料。

如果可以從 Unified Manager 伺服器存取 IdP URL，則可以按一下「取得 IdP 元資料」按鈕來填入此欄位。

- **主機系統 (FQDN)**

安裝期間定義的 Unified Manager 主機系統的 FQDN。如果需要的話，您可以更改該值。

- **主機 URI**

從 IdP 存取 Unified Manager 主機系統的 URI。

- **主機元資料**

XML 格式的主機系統元資料。

管理身份驗證

您可以在 Unified Manager 伺服器上使用 LDAP 或 Active Directory 啟用身份驗證，並將其設定為與您的伺服器協同工作以對遠端使用者進行身份驗證。

若要啟用遠端身分驗證、設定身分驗證服務和新增身分驗證伺服器，請參閱上一節「設定 Unified Manager 以傳送警報通知」。

編輯身份驗證伺服器

您可以變更 Unified Manager 伺服器用於與身分驗證伺服器通訊的連接埠。

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「常規」>「遠端驗證」。
2. 勾選“停用巢狀組查找”方塊。
3. 在「驗證伺服器」區域中，選擇要編輯的驗證伺服器，然後按一下「編輯」。
4. 在「編輯身份驗證伺服器」對話方塊中，編輯連接埠詳細資訊。
5. 點選“儲存”。

刪除身份驗證伺服器

如果您想要封鎖 Unified Manager 伺服器與身份驗證伺服器通信，您可以刪除該身份驗證伺服器。例如，如果您想要變更管理伺服器正在與之通訊的身份驗證伺服器，您可以刪除

該驗證伺服器並新增新的身份驗證伺服器。

開始之前

您必須具有應用程式管理員角色。

當您刪除身份驗證伺服器時，該驗證伺服器的遠端使用者或群組將無法再存取 Unified Manager。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 選擇一個或多個要刪除的身份驗證伺服器，然後按一下「刪除」。
3. 按一下“是”確認刪除請求。

如果啟用了「使用安全連線」選項，則與驗證伺服器關聯的憑證將與驗證伺服器一起刪除。

使用 Active Directory 或 OpenLDAP 進行驗證

您可以在管理伺服器上啟用遠端身份驗證，並將管理伺服器設定為與您的身份驗證伺服器通信，以便身份驗證伺服器內的使用者可以存取 Unified Manager。

您可以使用下列預先定義身分驗證服務之一，也可以指定您自己的身分驗證服務：

- 微軟活動目錄



您不能使用 Microsoft 輕量級目錄服務。

- OpenLDAP

您可以選擇所需的身份驗證服務並新增適當的身份驗證伺服器，以使身份驗證伺服器中的遠端使用者能夠存取 Unified Manager。遠端使用者或群組的憑證由身份驗證伺服器維護。管理伺服器使用輕量級目錄存取協定 (LDAP) 對配置的驗證伺服器內的遠端使用者進行驗證。

對於在 Unified Manager 中建立的本機用戶，管理伺服器維護自己的用戶名稱和密碼資料庫。管理伺服器執行身份驗證，且不使用 Active Directory 或 OpenLDAP 進行身份驗證。

審計日誌

您可以使用稽核日誌偵測稽核日誌是否已外洩。使用者執行的所有活動都受到監控並記錄在稽核日誌中。審核針對Active IQ Unified Manager的所有使用者介面和公開的 API 功能進行。

您可以使用*稽核日誌：檔案檢視*來檢視和存取Active IQ Unified Manager中可用的所有稽核日誌檔案。審計日誌：文件視圖中的文件根據其建立日期列出。此視圖顯示從安裝或升級到系統中現在捕獲的所有審計日誌的資訊。每當您在 Unified Manager 中執行操作時，資訊都會更新並可在日誌中取得。使用「檔案完整性狀態」屬性擷取每個日誌檔案的狀態，該屬性受到主動監控以偵測日誌檔案的篡改或刪除。當系統中有稽核日誌時，稽核日誌可以具有下列狀態之一：

狀態	描述
積極的	目前正在記錄日誌的檔案。
普通的	系統中處於非活動狀態、壓縮並儲存的檔案。
被竄改	該文件已被手動編輯過的使用者破壞。
手動刪除	已被授權使用者刪除的檔案。
滾動刪除	根據滾動配置策略，由於滾動而被刪除的檔案。
意外刪除	由於未知原因而被刪除的檔案。

審計日誌頁面包括以下命令按鈕：

- 配置
- 刪除
- 下載

使用 **DELETE** 按鈕可以刪除稽核日誌檢視中所列的任何稽核日誌。您可以刪除審計日誌，並可選擇提供刪除檔案的原因，這有助於將來確定有效的刪除。REASON 欄位列出了原因以及執行刪除操作的使用者的姓名。



刪除日誌檔案將導致檔案從系統中刪除，但資料庫表中的條目不會被刪除。

您可以使用稽核日誌部分中的 **DOWNLOAD** 按鈕從Active IQ Unified Manager下載稽核日誌並匯出稽核日誌檔案。標記為“正常”或“篡改”的檔案以壓縮檔案形式下載`.gzip`格式。

審計日誌檔案定期歸檔並保存到資料庫以供參考。在存檔之前，審計日誌經過數位簽章以維護安全性和完整性。

產生完整的AutoSupport套件時，支援包將包括存檔和活動審計日誌檔案。但是，當產生輕量級支援包時，它僅包含活動審計日誌。不包括存檔的稽核日誌。

配置審計日誌

您可以使用稽核日誌部分中的「設定」按鈕來設定稽核日誌檔案的捲動策略，並為稽核日誌啟用遠端日誌記錄。

您可以根據要在系統中儲存的資料量和頻率設定*MAX FILE SIZE*和*AUDIT LOG RETENTION DAYS*中的值。欄位 **TOTAL AUDIT LOG SIZE** 中的值是系統中存在的稽核日誌資料的總大小。捲動原則由欄位 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 中的值決定。當稽核日誌備份的大小達到*TOTAL AUDIT LOG SIZE*中配置的值時，將刪除第一個已存檔的檔案。這意味著最舊的檔案被刪除。但文件條目仍然在資料庫中可用，並被標記為“Rollover Delete”。**AUDIT LOG RETENTION DAYS** 值表示稽核日誌檔案保留的天數。任何比此欄位中設定的值更舊的檔案都會被翻轉。

步驟

1. 點選*審計日誌*>>*配置*。

2. 在 **MAX FILE SIZE**、**TOTAL AUDIT LOG SIZE** 和 **AUDIT LOG RETENTION DAYS** 中輸入數值。

如果您想啟用遠端日誌記錄，那麼您應該選擇*啟用遠端日誌記錄*。 /// 2025-6-11，OTHERDOC-133

啟用稽核日誌的遠端記錄

您可以在「設定稽核日誌」對話方塊中選取「啟用遠端日誌記錄」核取方塊來啟用遠端稽核日誌記錄。您可以使用此功能將稽核日誌傳輸到遠端 Syslog 伺服器。這將使您能夠在空間受限的情況下管理稽核日誌。

稽核日誌的遠端記錄提供了防篡改備份，以防Active IQ Unified Manager伺服器上的稽核日誌檔案被篡改。

步驟

1. 在*設定稽核日誌*對話方塊中，選取*啟用遠端日誌記錄*複選框。

顯示用於配置遠端日誌記錄的附加欄位。

2. 輸入您想要連接的遠端伺服器的 **HOSTNAME** 和 **PORT**。

3. 在*伺服器 CA 憑證*欄位中，按一下*瀏覽*以選擇目標伺服器的公共憑證。

證書應上傳至 .pem 格式。此憑證應從目標 Syslog 伺服器取得，且不應過期。憑證應包含所選的「主機名稱」作為 `SubjectAltName (SAN)` 屬性。

4. 輸入以下欄位的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

這些欄位的值應以毫秒為單位。

5. 在 **FORMAT** 和 **PROTOCOL** 欄位中選擇所需的 Syslog 格式和 TLS 協定版本。

6. 如果目標 Syslog 伺服器需要基於憑證的驗證，請勾選「啟用用戶端驗證」複選框。

在儲存審計日誌配置之前，您需要下載用戶端身份驗證憑證並將其上傳到 Syslog 伺服器，否則連線將失敗。根據 Syslog 伺服器的類型，您可能需要建立用戶端身份驗證憑證的雜湊值。

範例：syslog-ng 需要使用下列命令建立憑證的 <hash> openssl x509 -noout -hash -in cert.pem，然後您應該將客戶端身份驗證憑證符號連結到以 <hash> .0 命名的檔案。

7. 按一下「儲存」以設定與伺服器的連線並啟用遠端日誌記錄。

您將被重新導向到稽核日誌頁面。



*連線逾時*值會影響配置。如果配置回應的時間比定義值長，則可能會因連線錯誤而導致配置失敗。若要建立成功的連接，請增加*連接逾時*值，然後再次嘗試配置。

遠端身份驗證頁面

您可以使用遠端身份驗證頁面設定 Unified Manager 與您的身份驗證伺服器通信，以對嘗試登入 Unified Manager Web UI 的遠端使用者進行身份驗證。

您必須具有應用程式管理員或儲存管理員角色。

選取啟用遠端身份驗證複選框後，您可以使用身份驗證伺服器啟用遠端身份驗證。

- 認證服務

使您能夠設定管理伺服器以在目錄服務提供者（例如 Active Directory、OpenLDAP）中對使用者進行驗證，或指定您自己的驗證機制。只有當您啟用了遠端身份驗證時，您才可以指定身份驗證服務。

- 活動目錄

- 管理員姓名

指定認證伺服器的管理員名稱。

- 密碼

指定存取認證伺服器的密碼。

- 基本可分辨名稱

指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

- 禁用嵌套組查找

指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

- 使用安全連接

指定用於與身份驗證伺服器通訊的身份驗證服務。

- OpenLDAP

- 綁定可分辨名稱

指定與基本可分辨名稱一起使用的綁定可分辨名稱，以在身份驗證伺服器中尋找遠端使用者。

- 綁定密碼

指定存取認證伺服器的密碼。

- 基本可分辨名稱

指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

- 使用安全連接

指定使用安全 LDAP 與 LDAP 驗證伺服器進行通訊。

- 其他的

- 綁定可分辨名稱

指定綁定可分辨名稱，該名稱與基本可分辨名稱一起使用，以在您的身份驗證伺服器中尋找遠端使用者。

- 綁定密碼

指定存取認證伺服器的密碼。

- 基本可分辨名稱

指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

- 協議版本

指定您的驗證伺服器支援的輕量級目錄存取協定 (LDAP) 版本。您可以指定是否必須自動偵測協定版本或將版本設定為 2 或 3。

- 使用者名稱屬性

指定驗證伺服器中的屬性名稱，該屬性包含要由管理伺服器進行驗證的使用者登入名稱。

- 群組成員身分屬性

指定一個值，該值根據使用者的身份驗證伺服器中指定的屬性和值為遠端使用者指派管理伺服器群組成員身分。

- UGID

如果遠端使用者作為身分驗證伺服器中 GroupOfUniqueNames 物件的成員，則此選項可讓您根據該 GroupOfUniqueNames 物件中的指定屬性將管理伺服器群組成員身分指派給遠端使用者。

- 禁用嵌套組查找

指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

- 成員

指定身份驗證伺服器用於儲存有關群組的各個成員的資訊的屬性名稱。

- 使用者物件類別

指定遠端認證伺服器中使用者的物件類別。

- 群組物件類別

指定遠端認證伺服器中所有群組的物件類別。



您為 `_Member_`、`User Object Class` 和 `Group Object Class` 屬性輸入的值應與在 Active Directory、OpenLDAP 和 LDAP 配置中新增的值相同。否則，身份驗證可能會失敗。

- 使用安全連接

指定用於與身份驗證伺服器通訊的身份驗證服務。



如果要修改身份驗證服務，請確保刪除所有現有的身份驗證伺服器並新增新的身份驗證伺服器。

身份驗證伺服器區域

身份驗證伺服器區域顯示管理伺服器與之通訊以尋找和驗證遠端使用者的身份驗證伺服器。遠端使用者或群組的憑證由身份驗證伺服器維護。

- 命令按鈕

使您能夠新增、編輯或刪除身份驗證伺服器。

- 添加

使您能夠新增身份驗證伺服器。

如果您要新增的身份驗證伺服器是高可用性對的一部分（使用相同的資料庫），那麼您也可以新增合作夥伴驗證伺服器。當其中一個身份驗證伺服器無法存取時，這使得管理伺服器能夠與合作夥伴進行通訊。

- 編輯

使您能夠編輯選定身份驗證伺服器的設定。

- 刪除

刪除選定的認證伺服器。

- 姓名或 IP 位址

顯示用於在管理伺服器上驗證使用者的驗證伺服器的主機名稱或 IP 位址。

- 港口

顯示認證伺服器的連接埠號碼。

- 測試認證

此按鈕透過驗證遠端使用者或群組來驗證您的身份驗證伺服器的配置。

測試時，如果僅指定用戶名，管理伺服器會在認證伺服器中搜尋遠端用戶，但不會對用戶進行認證。如果您同時指定使用者名稱和密碼，管理伺服器將搜尋並驗證遠端使用者。

如果遠端身份驗證已停用，則您無法測試身份驗證。

管理安全證書

您可以在 Unified Manager 伺服器中設定 HTTPS，以透過安全連線監控和管理您的叢集。

查看HTTPS安全證書

您可以將 HTTPS 憑證詳細資訊與瀏覽器中檢索到的憑證進行比較，以確保瀏覽器與 Unified Manager 的加密連線不會被攔截。

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。

檢視憑證可讓您驗證重新產生的憑證的內容，或檢視可以從中存取 Unified Manager 的主題備用名稱 (SAN)。

步

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS 憑證**」。

HTTPS憑證顯示在頁面頂部

如果您需要查看比 HTTPS 憑證頁面上顯示的更多有關安全憑證的詳細信息，您可以在瀏覽器中查看連接憑證。

下載 HTTPS 憑證簽署請求

您可以下載目前 HTTPS 安全性憑證的認證簽章要求，以便將該檔案提供給憑證授權單位進行簽署。CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

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「常規」>「**HTTPS 憑證**」。
2. 按一下「下載 HTTPS 憑證簽署請求」。
3. 儲存 ``<hostname>.csr`` 文件。

您可以將該文件提供給證書頒發機構進行簽名，然後安裝已簽署的證書。

安裝 CA 簽署並傳回的 HTTPS 憑證

您可以在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。您上傳並安裝的檔案必須是現有自簽名憑證的簽章版本。CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

*開始之前

您必須完成以下操作：

- 下載憑證簽署請求文件並由憑證授權單位簽名
- 以 PEM 格式儲存憑證鏈
- 包含鏈中的所有證書，從 Unified Manager 伺服器證書到根簽名證書，包括任何存在的中間證書

您必須具有應用程式管理員角色。



如果建立 CSR 的憑證有效期超過 397 天，則 CA 會在簽署並傳回憑證之前將有效期縮短至 397 天

步驟

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS 憑證**」。
2. 按一下「安裝 HTTPS 憑證」。
3. 在顯示的對話方塊中，按一下「選擇檔案...」以找到要上傳的檔案。
4. 選擇文件，然後按一下*安裝*來安裝該文件。

有關信息，請參閱["安裝使用外部工具產生的 HTTPS 憑證"](#)。

證書鏈範例

以下範例顯示了憑證鏈檔案的可能外觀：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

安裝使用外部工具產生的 **HTTPS 憑證**

您可以安裝自簽名或 CA 簽署的證書，並使用外部工具（如 OpenSSL、BoringSSL、LetsEncrypt）產生。

您應該將私鑰與憑證鏈一起加載，因為這些憑證是外部產生的公鑰-私鑰對。允許的金鑰對演算法是“RSA”和“EC”。在「常規」部分下的「HTTPS 憑證」頁面中提供了「安裝 **HTTPS 憑證**」選項。您上傳的文件應採用以下輸入格式。

1. 屬於 Active IQ Unified Manager 主機的伺服器的私鑰

2. 與私鑰匹配的伺服器憑證
3. 反向直到根的 CA 證書，用於簽署上述證書

載入帶有 **EC** 金鑰對的憑證的格式

允許的曲線是“prime256v1”和“secp384r1”。具有外部產生的 EC 對的憑證樣本：

```
-----BEGIN EC PRIVATE KEY-----  
<EC private key of Server>  
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----  
<Server certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #1 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #2 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root signing certificate>  
-----END CERTIFICATE-----
```

使用 **RSA** 金鑰對載入憑證的格式

屬於主機憑證的 RSA 金鑰對允許的金鑰大小為 2048、3072 和 4096。具有外部產生的 **RSA** 金鑰對的憑證：

```
-----BEGIN RSA PRIVATE KEY-----  
<RSA private key of Server>  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
<Server certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #1 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #2 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root signing certificate>  
-----END CERTIFICATE-----
```

上傳憑證後，您應該重新啟動Active IQ Unified Manager實例以使變更生效。

上傳外部產生的憑證時進行檢查

系統在上傳使用外部工具產生的憑證時執行檢查。如果任何檢查失敗，則證書被拒絕。還包括產品內 CSR 產生的憑證和使用外部工具產生的憑證的驗證。

- 輸入中的私鑰根據輸入中的主機憑證進行驗證。
- 主機憑證中的通用名稱 (CN) 與主機的 FQDN 進行檢查。
- 主機憑證的通用名稱 (CN) 不能為空或空白，且不能設定為localhost。
- 證書的有效期限起始日期不應為日後日期，且證書的有效期限到期日不應為過去日期。
- 如果存在中級 CA 或 CA，則憑證的有效期限開始日期不應在未來，有效期到期日不應在過去。



輸入中的私鑰不應該被加密。如果有任何私鑰被加密，那麼系統就會拒絕它們。

範例 1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----  
<Encrypted private key>  
-----END ENCRYPTED PRIVATE KEY-----
```

範例 2

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
<content here>  
-----END RSA PRIVATE KEY-----
```

範例 3

```
-----BEGIN EC PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
<content here>  
-----END EC PRIVATE KEY-----
```

如果憑證安裝失敗，請參閱知識庫 (KB) 文章

：[https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate\[\"ActiveIQ Unified Manager 無法安裝外部產生的憑證\"\]](https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate[\)

證書管理的頁面描述

您可以使用 HTTPS 憑證頁面查看目前的安全性憑證並產生新的 HTTPS 憑證。

HTTPS 憑證頁面

HTTPS 憑證頁面可讓您查看目前安全性憑證、下載憑證簽署要求、產生新的自簽名 HTTPS 憑證或安裝新的 HTTPS 憑證。

如果您尚未產生新的自簽名 HTTPS 證書，則此頁面上顯示的證書是安裝期間產生的證書。

命令按鈕

命令按鈕使您能夠執行以下操作：

- 下載 **HTTPS 憑證簽署請求**

下載目前安裝的 HTTPS 憑證的認證請求。您的瀏覽器會提示您儲存 <hostname>.csr 文件，以便您可以將該文件提供給憑證授權單位進行簽署。

- 安裝 **HTTPS 憑證**

使您能夠在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。重新啟動管理伺服器後，新憑證將生效。

- 重新產生 **HTTPS 憑證**

使您能夠產生新的自簽名 HTTPS 證書，以取代目前的安全性證書。重新啟動 Unified Manager 後，新憑證將生效。

重新產生 HTTPS 憑證對話框

「重新產生 HTTPS 憑證」對話方塊可讓您自訂安全訊息，然後使用該資訊產生新的 HTTPS 憑證。

當前證書資訊出現在此頁面上。

「使用目前憑證屬性重新產生」和「更新目前憑證屬性」選擇可讓您使用目前資訊重新產生憑證或使用新資訊產生憑證。

- 通用名稱

必需的。您希望保護的完全限定網域名稱 (FQDN)。

在 Unified Manager 高可用性設定中，使用虛擬 IP 位址。

- 電子郵件

選修的。用於聯絡您組織的電子郵件地址；通常是憑證管理員或 IT 部門的電子郵件地址。

- 公司

選修的。通常是您公司的註冊名稱。

- 部門

選修的。貴公司部門的名稱。

- 城市

選修的。貴公司所在的城市。

- 狀態

選修的。貴公司所在的州或省位置（不縮寫）。

- 國家

選修的。貴公司所在的國家。這通常是該國家的兩個字母的 ISO 代碼。

- 其他名稱

必需的。除了現有的本地主機或其他網路位址之外，還可用於存取此伺服器的附加非主要網域名稱。用逗號分隔每個備用名稱。

如果您想要從憑證中的備用名稱欄位中刪除本機識別訊息，請勾選「排除本機識別資訊（例如 localhost）」複選框。選取此核取方塊後，只有您在欄位中輸入的內容才會在備用名稱欄位中使用。當留空時，產生的憑證將根本沒有備用名稱欄位。

- 金鑰大小（金鑰演算法：**RSA**）

金鑰演算法設定為RSA。您可以從下列密鑰大小中選擇一個：2048、3072 或 4096 位元。預設密鑰大小設定為 2048 位元。

- 有效期限

預設有效期為397天。如果您從先前的版本升級，您可能會看到先前的憑證有效性保持不變。

有關詳細信息，請參閱 ["產生 HTTPS 憑證"](#)。

監視和管理存儲

Active IQ Unified Manager簡介

Active IQ Unified Manager（以前稱為OnCommand Unified Manager）可讓您從單一介面監控和管理ONTAP儲存系統的運作狀況和效能。

Unified Manager 提供以下功能：

- 發現、監控和通知安裝了ONTAP軟體的系統。
- 儀表板顯示環境的容量、安全性和性能健康狀況。
- 增強的警報、事件和閾值基礎設施。
- 顯示繪製工作負載活動隨時間變化的詳細圖表；包括 IOPS（操作）、MBps（吞吐量）、延遲（回應時間）、利用率、效能容量和快取比率。
- 識別過度使用叢集組件的工作負載以及效能受到活動增加影響的工作負載。
- 提供可執行的建議糾正措施來解決某些事件和事件，並為某些事件提供「修復」按鈕，以便您可以立即解決問題。
- 與OnCommand Workflow Automation整合以執行自動保護工作流程。
- 能夠直接從 Unified Manager 建立新的工作負載（例如 LUN 或檔案共用），並指派效能服務等級來定義使用該工作負載存取應用程式的使用者的效能和儲存目標。

Active IQ Unified Manager健康監控簡介

Active IQ Unified Manager（以前稱為OnCommand Unified Manager）可協助您透過集中式使用者介面監控執行ONTAP軟體的大量系統。Unified Manager 伺服器基礎架構提供可擴充性、可支援性以及增強的監控和通知功能。

Unified Manager 的主要功能包括監控、警報、管理叢集的可用性和容量、管理保護功能以及捆綁診斷資料並將其傳送給技術支援。

您可以使用 Unified Manager 來監控您的叢集。當叢集中出現問題時，Unified Manager 會透過事件通知您此類問題的詳細資訊。有些事件還會為您提供可以採取的補救措施來糾正問題。您可以設定事件警報，以便在出現問題時透過電子郵件和 SNMP 陷阱通知您。

您可以使用 Unified Manager 透過將儲存物件與註解關聯來管理環境中的儲存物件。您可以建立自訂註釋，並透過規則將叢集、儲存虛擬機器 (SVM) 和磁碟區與註釋動態關聯。

您也可以使用容量和運行狀況圖表中提供的資訊來為各個叢集物件規劃叢集物件的儲存需求。

物理和邏輯容量

Unified Manager 利用用於ONTAP儲存物件的實體和邏輯空間的概念。

- 物理容量：物理空間是指磁碟區中使用的實體儲存區塊。由於儲存效率功能（例如重複資料刪除和壓縮）減少了數據，因此「物理已使用容量」通常小於邏輯已使用容量。

- **邏輯容量：**邏輯空間是指磁碟區中的可用空間（邏輯區塊）。邏輯空間是指理論上如何使用空間，不考慮重複資料刪除或壓縮的結果。「使用的邏輯空間」是使用的實體空間加上已配置的儲存效率功能（例如重複資料刪除和壓縮）所節省的空间。這個測量值通常看起來大於物理使用容量，因為這沒有反映資料壓縮和物理空間的其他減少。因此，總邏輯容量可能高於配置的空间。

容量測量單位

Unified Manager 根據 1024 (2¹⁰) 位元組的二進位單位計算儲存容量。在 ONTAP 9.10.0 及更早版本中，這些單位顯示為 KB、MB、GB、TB 和 PB。從 ONTAP 9.10.1 開始，它們在 Unified Manager 中顯示為 KiB、MiB、GiB、TiB 和 PiB。



對於 ONTAP 的所有版本，吞吐量使用的單位仍然是每秒千位元組 (Kbps)、每秒兆位元組 (Mbps)、每秒千兆位元組 (Gbps) 或每秒太字節 (Tbps) 等等。

Unified Manager for ONTAP 9.10.0 及更早版本中顯示的容量單位	Unified Manager for ONTAP 9.10.1 中顯示的容量單位	計算	以位元組為單位的值
知識庫	基布	1024	1024 位元組
MB	資訊局	1024 * 1024	1,048,576 字節
英國	吉布	1024 * 1024 * 1024	1,073,741,824 字節
結核病	硼化鈦	1024 * 1024 * 1024 * 1024	1,099,511,627,776 字節

Active IQ Unified Manager 效能監控簡介

Active IQ Unified Manager（以前稱為 OnCommand Unified Manager）為執行 NetApp ONTAP 軟體的系統提供效能監控功能和事件根本原因分析。

Unified Manager 可協助您辨識過度使用叢集元件並降低叢集上其他工作負載效能的工作負載。透過定義效能閾值策略，您還可以指定某些效能計數器的最大值，以便在超過閾值時產生事件。Unified Manager 會向您發出有關這些效能事件的警報，以便您採取糾正措施，並使效能恢復到正常運作水準。您可以在 Unified Manager UI 中檢視和分析事件。

Unified Manager 監控兩種類型工作負載的效能：

- 使用者定義的工作負載

這些工作負載包括您在叢集中建立的 FlexVol 磁碟區和 FlexGroup 磁碟區。

- 系統定義的工作負載

這些工作負載由內部系統活動組成。

使用 Unified Manager REST API

Active IQ Unified Manager 為您提供 REST API 來查看有關監控和管理儲存環境的資訊。API 還允許根據策略配置和管理儲存物件。

您也可以使用 Unified Manager 支援的 API 閘道在所有 ONTAP 管理的叢集上執行 ONTAP API。

有關 Unified Manager REST API 的信息，請參閱["Active IQ Unified Manager REST API 入門"](#)。

Unified Manager 伺服器的功能

Unified Manager 伺服器基礎架構由資料收集單元、資料庫和應用程式伺服器組成。它提供發現、監控、基於角色的存取控制 (RBAC)、稽核和日誌記錄等基礎設施服務。

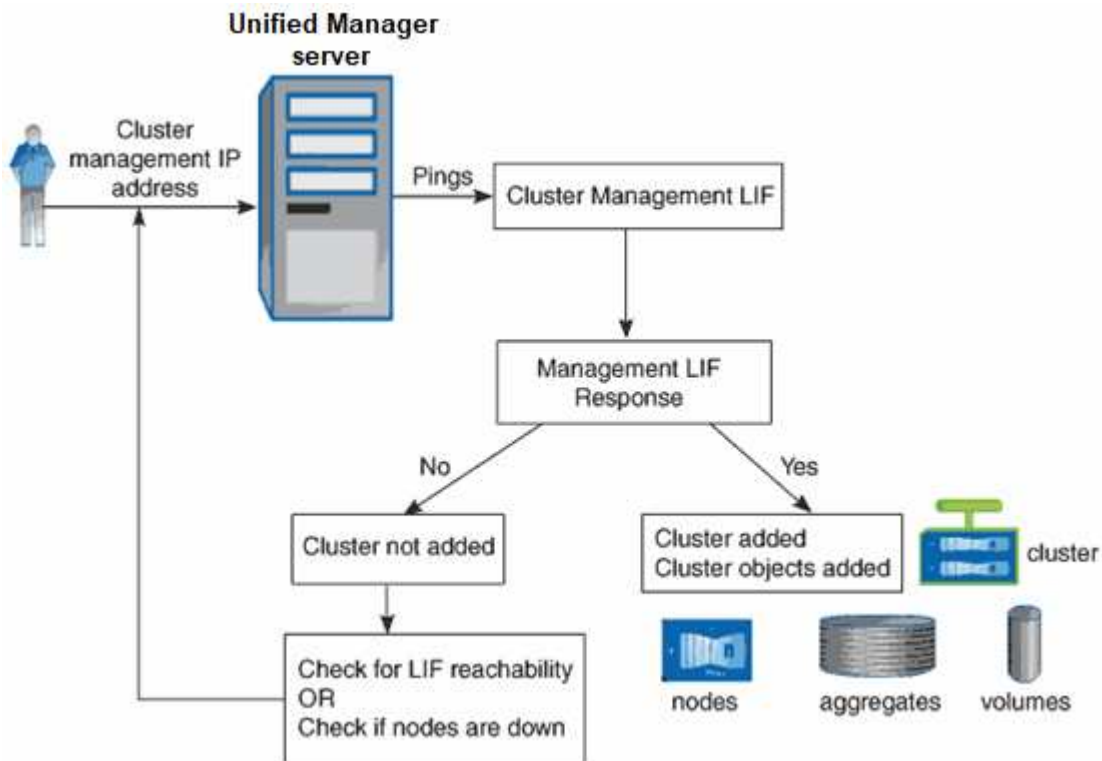
Unified Manager 收集叢集信息，將資料儲存在資料庫中，並分析資料以查看是否存在任何叢集問題。

發現過程如何運作

將叢集新增至 Unified Manager 後，伺服器會發現叢集物件並將其新增至其資料庫。了解發現過程的工作原理有助於您管理組織的集群及其物件。

預設監控間隔為 15 分鐘：如果您已將叢集新增至 Unified Manager 伺服器，則需要 15 分鐘才能在 Unified Manager UI 中顯示叢集詳細資訊。

下圖說明了 Active IQ Unified Manager 中的發現過程：



了解使用者介面

Unified Manager 使用者介面主要由一個儀表板組成，該儀表板提供所監控物件的概覽視圖。使用者介面還提供查看所有集群物件的權限。

您可以選擇首選視圖並根據需要使用操作按鈕。您的螢幕設定會儲存在工作區中，以便在啟動 Unified Manager 時可以使用您需要的所有功能。但是，當您從一個視圖導航到另一個視圖，然後導航回來時，視圖可能會不一樣。

典型的視窗佈局

了解典型的視窗佈局有助於您有效地導覽和使用Active IQ Unified Manager。大多數 Unified Manager 視窗類似於兩種常規佈局之一：物件清單或詳細資訊。建議的顯示設定至少為 1280 x 1024 像素。

並非每個視窗都包含下圖中的每個元素。

物件清單視窗佈局

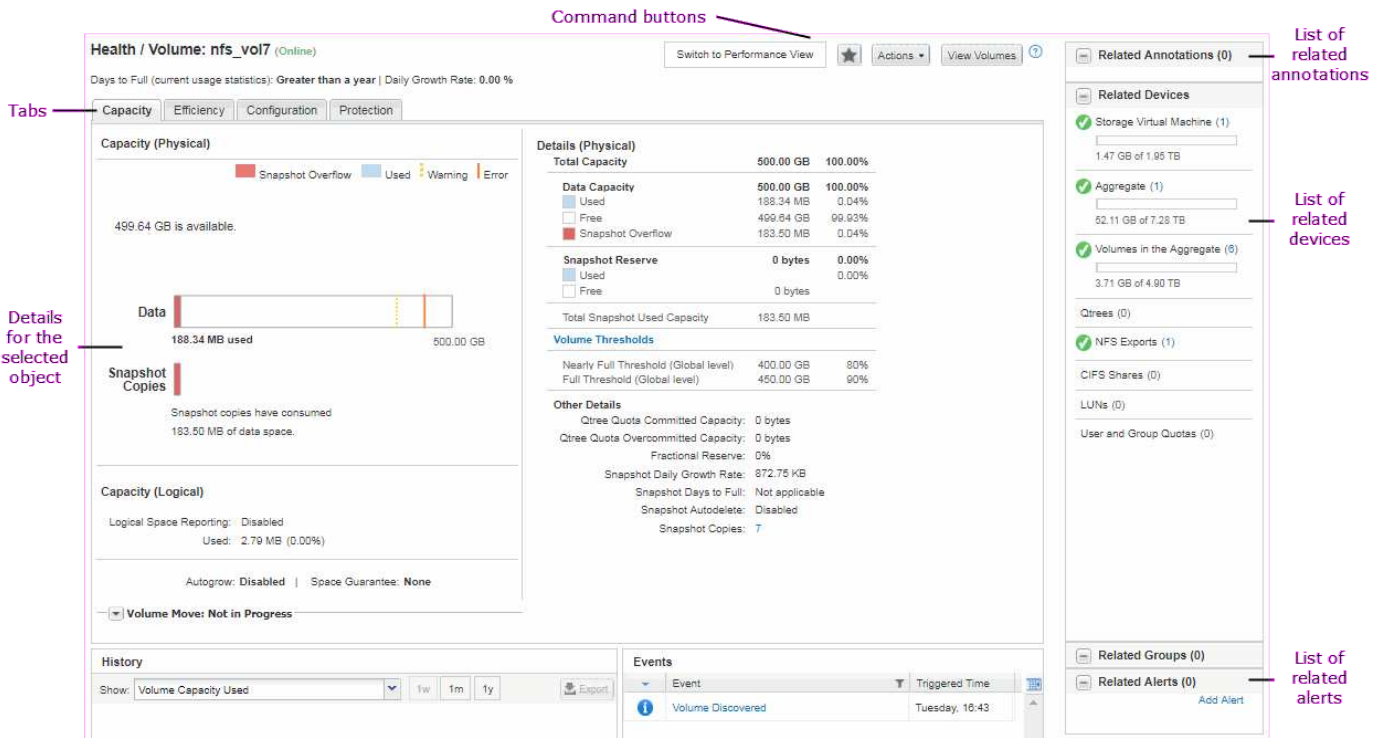
The screenshot displays the 'Aggregates' view in the Active IQ Unified Manager. The interface is annotated with labels for various components:

- Navigation expand/collapse**: Located at the top left of the navigation panel.
- Menu bar**: The top horizontal bar containing the 'Active IQ Unified Manager' logo and search bar.
- Page help**: A question mark icon in the top right corner.
- View selector**: A dropdown menu above the table header.
- Object list**: The main table displaying aggregate data.
- Page search**: A search input field within the table header.
- Filter tool**: A filter icon in the table header.
- Global search**: A search bar in the top menu bar.
- Schedule report**: A button in the top right area.
- Notification bell**: A bell icon in the top right area.
- System help**: A question mark icon in the top right area.
- User profile / logout**: A user profile icon in the top right area.
- Feedback**: A feedback icon in the top right area.
- Export report**: A button in the top right area.
- Column selector**: A dropdown menu in the top right area.

	Status	Aggregate	Node	Type	Total Data Capacity	Committed Capacity	Used Data Capacity	Avg
<input type="checkbox"/>	●	aggr2	ocum-infinity-01	SSD	10.7 TB	251 TB	8.03 TB	2.71
<input type="checkbox"/>	●	aggr1	ocum-infinity-01	SSD	3.45 TB	129 TB	1.28 TB	2.17
<input type="checkbox"/>	●	aggr3	ocum-infinity-02	SSD	1.87 TB	8.3 TB	1.41 TB	5.75
<input type="checkbox"/>	●	aggr4	ocum-infinity-02	SSD	2.63 TB	14.3 TB	1.33 TB	1.37
<input type="checkbox"/>	●	aggr1	ocum-infinity-01	SSD	2.06 TB	10.2 TB	1.8 TB	1.06
<input type="checkbox"/>	●	aggr_donor_touch	ocum-infinity-02	SSD	3.07 TB	8.87 TB	257 GB	2.82
<input type="checkbox"/>	●	aggr2	ocum-infinity-02	SSD	7.78 TB	136 TB	6.06 TB	3.71

Showing all 26 aggregates

物件詳細資料視窗佈局




視窗佈局自訂

Active IQ Unified Manager可讓您自訂儲存空間和網路物件頁面上資訊的佈局。透過自訂窗口，您可以控制哪些資料可查看以及資料的顯示方式。

- 排序

您可以按下列標題來變更列條目的排序順序。按下列標題時，排序箭頭 (▲ 和 ▼) 出現在該列。

- 過濾

您可以點選過濾器圖示 () 套用篩選器來自訂儲存和網路物件頁面上的資訊顯示，以便只顯示符合所提供條件的項目。您可以從「篩選器」窗格套用篩選器。

篩選器窗格可讓您根據所選的選項篩選大多數列。例如，在「健康狀況：所有磁碟區」檢視中，您可以使用「篩選器」窗格，透過選擇「狀態下」下的對應篩選器選項來顯示所有處於離線狀態的磁碟區。

任何清單中與容量相關的列始終以適當的單位顯示容量數據，並四捨五入到小數點後兩位。這也適用於過濾容量列。例如，如果使用「運行狀況：所有聚合」視圖中「總數據容量」列中的過濾器來過濾大於 20.45 GB 的數據，則實際容量 20.454 GB 將顯示為 20.45 GB。同樣，如果過濾小於 20.45 GB 的數據，則實際容量 20.449 GB 將顯示為 20.45 GB。

如果使用「運行狀況：所有聚合」視圖中「可用資料 %」列中的篩選器來過濾大於 20.45% 的數據，則實際容量 20.454% 將顯示為 20.45%。同樣的，如果過濾小於 20.45% 的數據，那麼實際容量 20.449% 就會顯示為 20.45%。

- 隱藏或顯示列

您可以按下列顯示圖示 (顯示/隱藏) 來選擇要顯示的列。一旦選擇了適當的列，您就可以使用滑鼠拖曳它們來重新排序。

- 搜尋中

您可以使用搜尋框搜尋某些物件屬性，以協助最佳化庫存頁面中的項目清單。例如，您可以輸入「雲」來優化磁碟區清單頁面中的磁碟區列表，以查看其中包含單字「雲」的所有磁碟區。

- 匯出資料



您可以點擊“報告”按鈕（或“匯出”按鈕將資料匯出為逗號分隔的值 `(.csv)` 文件，`.pdf)` 文件或 Microsoft Excel `(.xlsx)` 文件並使用匯出的數據來建立報告。

使用 Unified Manager 協助

協助包含有關Active IQ Unified Manager中包含的所有功能的資訊。您可以使用目錄、索引或搜尋工具來尋找有關功能及其使用方法的資訊。

每個標籤和 Unified Manager 使用者介面的選單列中均提供協助。

幫助中的搜尋工具不適用於部分單字。

- 若要了解特定欄位或參數，請按一下 。
- 要查看所有幫助內容，請點擊*  * > 功能表列中的 幫助/文件。

您可以透過展開導覽窗格中目錄的任意部分來找到更詳細的資訊。

- 若要搜尋說明內容，請按一下導覽窗格中的“搜尋”選項卡，鍵入要尋找的單字或一系列單字，然後按一下“開始！”
- 若要列印說明主題，請按一下印表機圖示。

為您最喜歡的幫助主題添加書籤

在「幫助收藏夾」標籤中，您可以為經常使用的幫助主題添加書籤。幫助書籤可讓您快速存取您喜歡的主題。

步驟

1. 導覽至您想要新增為收藏夾的說明主題。
2. 按一下“收藏夾”，然後按一下“新增”。

搜尋儲存對象

若要快速存取特定對象，您可以使用功能表列頂部的「搜尋所有儲存對象」欄位。這種對所有物件進行全域搜尋的方法使您能夠按類型快速定位特定物件。搜尋結果按儲存物件類型排序，您可以使用下拉式選單按物件進一步過濾它們。

開始之前

- 您必須具有以下角色之一才能執行此任務：操作員、應用程式管理員或儲存管理員。
- 有效搜尋必須至少包含三個字元。

當使用下拉式選單值「全部」時，全域搜尋顯示在所有物件類別中找到的結果總數；每個物件類別最多 25 個搜尋結果。您可以從下拉式選單中選擇特定的物件類型，以優化特定物件類型內的搜尋。在這種情況下，傳回的清單不限於前 25 個物件。

您可以搜尋的物件類型包括：

- 叢集
- 節點
- 儲存虛擬機
- 聚合
- 卷
- 配額樹
- 中小企業股份
- NFS 分享
- 使用者或群組配額
- LUN
- NVMe 命名空間
- 發起者群組
- 發起者
- 一致性組

輸入工作負載名稱將傳回對應磁碟區或 LUN 類別下的工作負載清單。

您可以按一下搜尋結果中的任何物件來導覽至該物件的健康詳細資料頁面。如果某個物件沒有直接的健康頁面，則會顯示其父對象的健康頁面。例如，搜尋特定 LUN 時，將顯示該 LUN 所在的 SVM 詳細資訊頁面。

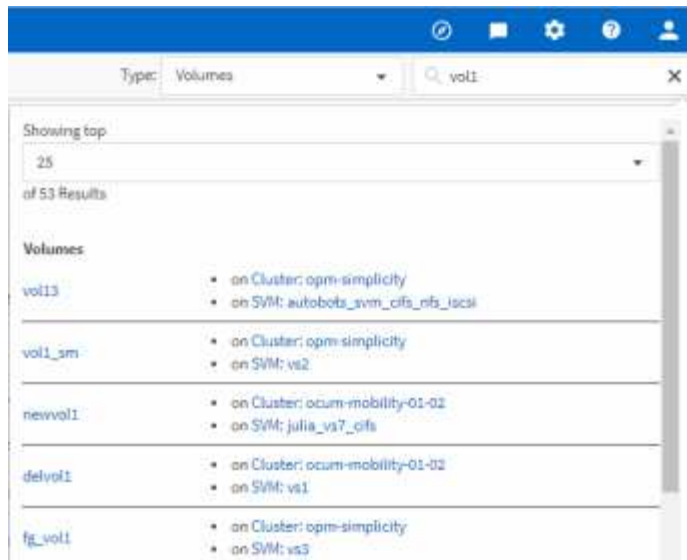


無法在全域搜尋列中搜尋連接埠和 LIF。

步驟

1. 從選單中選擇一種物件類型，以最佳化僅針對單一物件類型的搜尋結果。
2. 在*搜尋所有儲存物件*欄位中輸入物件名稱的至少三個字元。

在此範例中，下拉方塊選擇了磁碟區物件類型。在*搜尋所有儲存物件*欄位中輸入「vol1」將顯示名稱中包含這些字元的所有磁碟區的清單。



將儲存資料匯出為報告

您可以以多種輸出格式匯出儲存數據，然後使用匯出的數據來建立報表。例如，如果有 10 個尚未解決的關鍵事件，您可以從事件管理庫存頁面匯出資料以建立報告，然後將報告傳送給可以解決問題的管理員。

您可以將資料匯出到`.csv`文件，`.xlsx`文件，或`.pdf`從*儲存*和*網路*庫存頁面取得文件並使用匯出的資料來建立報表。產品中還有其他位置僅`.csv`或者`.pdf`可以產生文件。

步驟

1. 執行下列操作之一：

如果您想匯出...	這樣做...
儲存物件清單詳細信息	點擊左側導覽功能表中的“儲存”或“網路”，然後選擇儲存物件。選擇系統提供的視圖之一，或您建立的任何自訂視圖。
QoS 策略群組詳細信息	點選左側導覽選單中的「儲存」>「QoS 策略群組」。
儲存容量和保護歷史記錄詳細信息	按一下“儲存”>“聚合”或“儲存”>“磁碟區”，然後選擇單一聚合或磁碟區。
活動詳情	點選左側導覽功能表中的“事件管理”。
儲存物件 Top 10 效能詳情	按一下“儲存”>“叢集”>“效能：所有叢集”，然後選擇一個叢集並選擇“最佳表現者”標籤。然後選擇一個儲存物件和效能計數器。

2. 按一下「報告」按鈕（或某些 UI 頁面中的「匯出」按鈕）。

3. 按一下*下載 CSV*、下載 **PDF** 或 下載 **Excel** 以確認匯出請求。

從「最佳表現者」標籤中，您可以選擇下載您正在查看的單一群集或資料中心中所有群集的統計報告。

文件已下載。

4. 在適當的應用程式中開啟該文件。

相關資訊

["健康/集群清單頁面"](#)

["安排報告"](#)

過濾庫存頁面內容

您可以在 Unified Manager 中過濾庫存頁面數據，以便根據特定條件快速定位數據。您可以使用篩選功能來縮小 Unified Manager 頁面的內容範圍，以僅顯示您感興趣的結果。這提供了一種非常有效的方法，可以僅顯示您感興趣的數據。

使用*過濾*根據您的喜好自訂網格視圖。可用的篩選選項是基於網格中查看的物件類型。如果目前套用了過濾器，則已套用的過濾器的數量將顯示在過濾器按鈕的右側。

支援三種類型的過濾參數。

範圍	驗證
字串（文字）	運算子包括*包含*、以...開頭、以...結尾*和*不包含*。
數位	運算子包括*大於*、小於、在最後*和*之間。
枚舉（文本）	運算子是 is 和 is not 。

每個篩選器都需要列、運算子和值欄位；可用的篩選器反映目前頁面上可篩選的列。您最多可以套用四個濾鏡。過濾結果基於組合過濾參數。過濾結果適用於過濾搜尋中的所有頁面，而不僅僅是目前顯示的頁面。

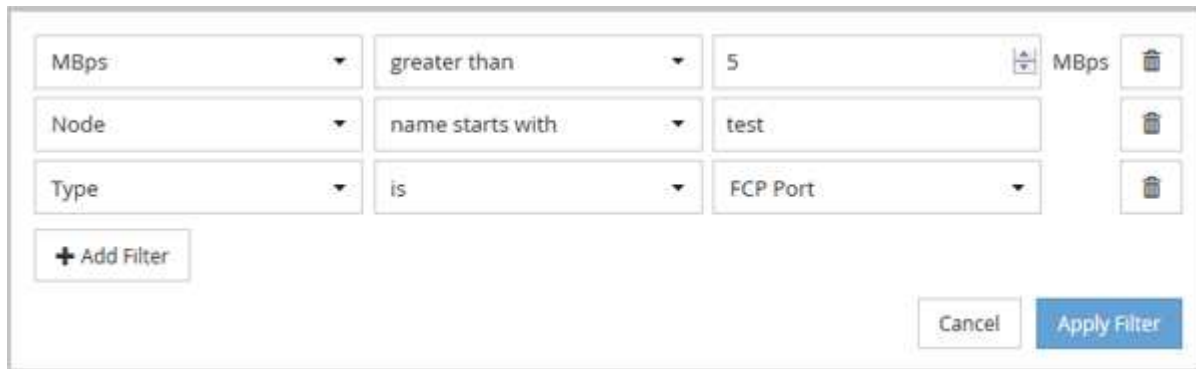
您可以使用過濾面板新增過濾器。

1. 在頁面頂部，按一下“過濾器”按鈕。顯示過濾面板。
2. 點擊左側下拉清單並選擇一個物件；例如，“Cluster”或效能計數器。
3. 按一下中心下拉列表，然後選擇要使用的運算子。
4. 在最後一個清單中，選擇或輸入一個值以完成該物件的篩選。
5. 若要新增另一個過濾器，請按一下「+新增過濾器」。顯示附加的過濾欄位。使用前面步驟中所述的程序完成此過濾器。請注意，新增第四個過濾器後，*+新增過濾器*按鈕不再顯示。
6. 按一下“套用過濾器”。過濾選項應用於網格，過濾器的數量顯示在過濾器按鈕的右側。
7. 使用過濾面板透過點擊要刪除的過濾器右側的垃圾桶圖示來刪除單個過濾器。

8. 若要刪除所有過濾器，請按一下過濾面板底部的“重設”。

過濾範例

該圖顯示了帶有三個過濾器的過濾面板。當您擁有的過濾器少於四個時，將顯示“+新增過濾器”按鈕。



MBps	greater than	5	MBps	🗑️
Node	name starts with	test		🗑️
Type	is	FCP Port		🗑️

+ Add Filter

Cancel Apply Filter

點擊“套用過濾器”後，“過濾”面板將關閉，套用過濾器，並顯示已套用的過濾器數量（  3 ）。


從通知鈴查看活動事件

通知鈴聲（）提供了一種快速查看 Unified Manager 正在追蹤的最重要的活動事件的方法。

活動事件清單提供了一種查看所有叢集上嚴重、錯誤、警告和升級事件總數的方法。此清單包括前 7 天的事件，但不包括資訊事件。您可以點擊連結來顯示您最感興趣的事件清單。

請注意，當叢集不可存取時，Unified Manager 會在此頁面中顯示此資訊。您可以透過點擊「詳細資料」按鈕查看有關無法存取的叢集的詳細資訊。此操作將開啟事件詳細資訊頁面。規模監控問題（例如管理站空間或 RAM 不足）也會顯示在此頁面上。

步驟

1. 在功能表列中，按一下 。
2. 要查看任何活動事件的詳細信息，請單擊事件文字鏈接，例如“2 容量”或“4 性能”。

從儀表板監控和管理集群

儀表板提供受監控 ONTAP 系統目前運作狀況的累積概覽資訊。儀表板提供“面板”，使您能夠評估正在監控的叢集的整體容量、效能和安全健康狀況。

此外，您可以直接從 Unified Manager 使用者介面修復某些 ONTAP 問題，而不必使用 ONTAP System Manager 或 ONTAP CLI。

在儀表板頂部，您可以選擇面板是否顯示所有受監控叢集的資訊或單一叢集的資訊。您可以先查看所有叢集的狀態，然後在想要查看詳細資訊時深入到單一叢集。



根據您的配置，下面列出的某些面板可能不會出現在頁面上。

面板	描述
管理措施	當 Unified Manager 可以診斷並確定問題的單一解決方案時，這些解決方案將顯示在此面板中，並帶有 修復 按鈕。
容量	顯示本地層和雲層的總容量和已使用容量，以及本地容量達到上限的天數。
性能容量	顯示每個群集的效能容量值以及達到效能容量上限的天數。
工作負載 IOPS	顯示目前在特定 IOPS 範圍內運作的工作負載總數。
工作負載效能	顯示分配給每個定義的效能服務等級的符合和不符合的工作負載總數。
安全	顯示合規或不合規的群集數量、合規或不合規的 SVM 數量以及加密或未加密的磁碟區數量。
保護	顯示受 SVM-DR 關係保護的儲存虛擬機器的數量、受 SnapMirror 關係保護的磁碟區的數量、受 Snapshot 保護的磁碟區的數量以及受 MetroCluster 保護的叢集的數量。
使用概述	顯示依最高 IOPS、最高吞吐量 (MBps) 或最高已以實體容量排序的叢集。

儀表板頁面

儀表板頁面有“面板”，顯示您正在監控的叢集的高級容量、效能和安全健康狀況。此頁面還提供了一個管理操作面板，其中列出了 Unified Manager 可以採取的修復措施來解決某些事件。

大多數面板還顯示該類別中的活躍事件數，以及過去 24 小時內新增的事件數。此資訊可協助您確定需要進一步分析哪些叢集以解決事件。點擊事件將顯示熱門事件，並提供指向事件管理庫存頁面的鏈接，該頁面經過篩選以顯示該類別中的活動事件。

在儀表板頂部，您可以選擇面板是否顯示所有受監控集群（「所有集群」）或單一集群的資訊。您可以先查看所有叢集的狀態，然後在想要查看詳細資訊時深入到單一叢集。



下面列出的一些面板將根據您的配置出現在儀表板上。

管理操作面板

Unified Manager 可以徹底診斷某些問題並提供單一解決方案。當可用時，這些解析度將顯示在此面板中，並帶有“修復”或“修復全部”按鈕。您可以從 Unified Manager 立即修復這些問題，而不必使用 ONTAP System

Manager 或 ONTAP CLI。要查看所有問題，請點擊查看["直接從 Unified Manager 修復 ONTAP 問題"](#)了解更多。

容量面板

在查看所有叢集時，此面板顯示每個叢集的實體已使用容量（應用儲存效率節省後）和實體可用容量（不包括潛在的儲存效率節省）、磁碟預計滿載的天數以及基於配置的 ONTAP 儲存效率設定的資料縮減率（不含 Snapshot 副本）。它還列出了任何已配置雲層的已使用容量。點擊條形圖將轉到該叢集的聚合庫存頁面。按一下「剩餘容量天數」文字將顯示一則訊息，標識剩餘容量天數最少的聚合；按一下聚合名稱以查看更多詳細資訊。

查看單一叢集時，此面板顯示按本機層和雲層上的每個磁碟類型排序的資料聚合的實體已使用容量和實體可用容量。按一下磁碟類型的長條圖將前往使用該磁碟類型的磁碟區的磁碟區清單頁面。

性能容量面板

查看所有群集時，此面板顯示每個群集的效能容量值（前 1 小時的平均值）以及效能容量達到上限的天數（基於每日成長率）。點擊長條圖將轉到該叢集的節點清單頁面。請注意，節點清單頁面顯示過去 72 小時的平均效能容量。按一下「剩餘效能容量天數」文字將顯示一則訊息，標識剩餘效能容量天數最少的節點；按一下節點名稱以查看更多詳細資訊。

查看單一叢集時，此面板顯示叢集效能容量使用百分比、總 IOPS 和總吞吐量（MB/s）值，以及預計這三個指標達到其上限的天數。

工作負載 IOPS 面板

查看單一叢集時，此面板顯示目前在特定 IOPS 範圍內執行的工作負載總數，並在將遊標停留在圖表上時指示每種磁碟類型的數量。

工作負載效能面板

此面板顯示指派給每個效能服務等級 (PSL) 策略的符合和不符合的工作負載總數。它還顯示未分配 PSL 的工作負載數量。按一下長條圖可前往「工作負載」頁面中指派給該策略的符合工作負載。點擊條形圖後面的數字即可查看分配給該策略的符合和不符合的工作負載。

安全面板

根據您目前的視圖，安全面板顯示所有叢集或單一叢集的進階安全狀態。此面板顯示：

- 過去 24 小時內收到的安全事件清單。點擊事件，在事件詳情頁面查看事件詳情
- 集群安全狀態（合規和不合規集群的數量）
- 儲存虛擬機器安全狀態（合規和不合規儲存虛擬機器的數量）
- 卷加密狀態（已加密或未加密的磁碟區的數量）
- 捲反勒索軟體狀態（啟用或停用反勒索軟體的捲數）

您可以點選合規與不合規叢集、儲存虛擬機器、加密與非加密磁碟區、捲防勒索狀態長條圖，進入對應頁面，查看已篩選叢集、儲存虛擬機器、磁碟區的安全詳情。

合規性基於 ["NetApp ONTAP 9 安全強化指南"](#)。按下面板頂部的右箭頭可在「安全性」頁面上查看所有叢集的安全性詳細資訊。有關信息，請參閱["查看叢集和儲存虛擬機器的詳細安全狀態"](#)。

資料保護面板

此面板顯示資料中心內單一或所有群集的資料保護摘要。它顯示ONTAP中過去 24 小時內發生的資料保護事件、MetroCluster事件和活動事件的總數。點擊每個事件的連結即可進入事件詳細資訊頁面。您可以點擊「查看全部」連結以查看事件管理庫存頁面中的所有活動保護事件。面板顯示：

- 受 Snapshot 副本保護的叢集或資料中心內所有叢集中的磁碟區數。
- 受SnapMirror關係保護的叢集或資料中心內所有叢集中的磁碟區數。對於SnapMirror關係，將考慮來源叢集中的磁碟區數。
- 透過 IP 或 FC 受MetroCluster配置保護的資料中心中的叢集數量或所有叢集。
- 根據滯後狀態，具有SnapMirror恢復點目標 (RPO) 滯後的捲關係的數量。

您可以將滑鼠懸停在螢幕上以查看相應的計數和圖例。您可以點擊面板頂部的右箭頭來查看資料保護頁面上的單一或所有叢集的詳細資訊。您也可以點擊：

- 未受保護的捲和受 Snapshot 副本保護的捲的條形圖，可前往「捲」頁面並查看詳細資訊。
- 受MetroCluster配置保護或未受保護的叢集的長條圖，可前往「叢集」頁面並查看詳細資訊。
- 所有關係的長條圖都會轉到「關係」頁面，其中會根據來源集群過濾詳細資訊。

有關詳細信息，請參閱 ["查看卷宗保護狀態"](#)。

使用情況概覽面板

在查看所有叢集時，您可以選擇按最高 IOPS、最高吞吐量（MB/s）或最高已用實體容量排序以查看叢集。

查看單一叢集時，您可以選擇以最高 IOPS、最高吞吐量（MB/s）或最高使用邏輯容量排序來查看工作負載。

相關資訊

["使用 Unified Manager 自動修復修復問題"](#)

["顯示有關性能事件的信息"](#)

["使用效能容量和可用 IOPS 資訊管理效能"](#)

["音量/健康詳情頁面"](#)

["效能事件分析和通知"](#)

["事件嚴重性類型描述"](#)

["性能事件的來源"](#)

["管理叢集安全目標"](#)

["從效能叢集登入頁面監控叢集效能"](#)

["使用「效能清單」頁面監控效能"](#)

直接從 Unified Manager 管理ONTAP問題或功能

您可以直接從 Unified Manager 使用者介面修復某些ONTAP問題或管理某些ONTAP功能，而不必使用ONTAP System Manager 或ONTAP CLI。「管理操作」選項為觸發 Unified Manager 事件的許多ONTAP問題提供了修復。

您可以透過選擇左側導覽窗格上的「管理操作」選項直接從「管理操作」頁面修正問題。您還可以從儀表板上的管理操作面板、事件詳細資訊頁面和左側導覽功能表上的工作負載分析選擇中獲得管理操作。

Unified Manager 可以徹底診斷某些問題並提供單一解決方案。對於某些ONTAP功能（例如反勒索軟體監控），Unified Manager 會執行內部檢查並建議採取特定措施。當可用時，這些解決方案將顯示在管理作業中，並帶有*修復*按鈕。點擊“修復”按鈕即可修復該問題。您必須具有應用程式管理員或儲存管理員角色。

Unified Manager 向叢集發送ONTAP命令以進行要求的修復。修復完成後，該事件將被廢棄。

某些管理操作可讓您使用「修復全部」按鈕修復多個儲存物件上的相同問題。例如，可能有 5 個磁碟區發生「磁碟區空間已滿」事件，可以透過按一下「啟用磁碟區自動成長」的 修復全部 管理操作來解決。只需單擊一下，即可修復 5 個磁碟區上的此問題。

有關可以使用自動修復功能管理的ONTAP問題和功能的信息，請參閱["Unified Manager 可以修復哪些問題"](#)。

當我看到“修復”或“修復全部”按鈕時，我有哪些選項

管理操作頁面為您提供了「修復」或「修復全部」按鈕，用於修復 Unified Manager 透過事件通知的問題。

我們建議您根據需要點擊按鈕來解決問題。但是，如果您不確定是否要按照 Unified Manager 的建議解決問題，則可以執行下列操作：

你想讓我做什麼？	行動
讓 Unified Manager 修復所有已識別物件上的問題。	點選“修復全部”按鈕。
此時不要修復任何已識別物件的問題，並隱藏此管理操作，直到再次引發該事件。	按一下向下箭頭，然後按一下「全部關閉」。
僅修復部分已識別物件的問題。	按一下管理操作的名稱以展開清單並顯示所有單獨的*修復*操作。然後按照修復或解除單一管理操作的步驟進行操作。

你想讓我做什麼？	行動
讓 Unified Manager 修復該問題。	點選“修復”按鈕。
此時請勿修復該問題並隱藏此管理操作，直到事件再次發生。	按一下向下箭頭，然後按一下“關閉”。

你想讓我做什麼？	行動
顯示此事件的詳細信息，以便您更好地了解問題。	<ul style="list-style-type: none"> • 點擊“修復”按鈕並查看將在出現的對話方塊中套用的修復。 • 按一下向下箭頭，然後按一下「檢視事件詳情」以顯示事件詳情頁面。 <p>如果您想修復該問題，請在任一結果頁面中按一下「修復它」。</p>
顯示此存儲對象的詳細信息，以便您更好地了解問題。	按一下儲存物件的名稱可在「效能資源管理器」或「運作狀況詳細資料」頁面中顯示詳細資料。

在某些情況下，修復會反映在接下來的 15 分鐘配置輪詢中。在其他情況下，可能需要花費數小時來驗證配置變更並讓事件過時。

若要查看已完成或正在進行的管理操作列表，請按一下篩選器圖示並選擇*已完成*或*進行中*。

修復所有操作都以串行方式運行，因此當您查看*進行中*面板時，某些物件的狀態為*進行中*，而其他物件的狀態為*已安排*；這表示它們仍在等待實施。


查看您選擇修復的管理操作的狀態

您可以在「管理操作」頁面中查看您選擇修復的所有管理操作的狀態。在 Unified Manager 將 ONTAP 指令傳送到叢集後，大多數操作都會很快顯示為*已完成*。但是，某些操作（例如移動磁碟區）可能需要更長時間。

管理操作頁面上有三個可用的篩選器：

- *已完成*顯示成功完成的管理操作和失敗的管理操作。*失敗*的操作提供了失敗的原因，以便您可以手動解決問題。
- *進行中*顯示正在實施的管理行動以及計畫實施的管理行動。
- *建議*顯示所有受監控群集目前處於活動狀態的所有管理操作。

步驟

1. 按一下左側導覽窗格上的「管理操作」。或者，點擊  在*儀表板*上的*管理操作*面板頂部，選擇您想要查看的視圖。
將顯示「管理操作」頁面。
2. 您可以點擊「描述」欄位中管理操作旁邊的插入符號圖示來查看有關該問題以及用於修復該問題的命令的詳細資訊。
3. 若要查看任何*失敗*的操作，請在*已完成*視圖中的*狀態*列上進行排序。您可以使用*濾鏡*工具來達到相同的目的。
4. 如果您想查看有關失敗的管理操作的更多信息，或者您決定要修復建議的管理操作，您可以在單擊管理操作旁邊的插入符號圖示後，從展開區域中單擊“查看事件詳細信息”。該頁面上有一個「修復」按鈕。

Unified Manager 可以修復哪些問題

透過使用Active IQ Unified Manager的自動修復功能，您可以選擇透過 Unified Manager 有效地解決某些ONTAP問題或管理某些ONTAP功能（例如反勒索軟體監控）。

下表介紹了這些ONTAP問題或功能，您可以透過 Unified Manager Web UI 上的 修復它 或 修復全部 按鈕直接管理這些問題或功能。

事件名稱和描述	管理行動	“修復”操作
<p>捲空間已滿</p> <p>該卷的空間幾乎用盡，並且已突破容量滿閾值。此閾值預設為磁碟區大小的 90%。</p>	啟用卷自動增長	Unified Manager 確定此磁碟區未設定磁碟區自動成長，因此啟用此功能，以便磁碟區在需要時容量會增加。
<p>Inode 已滿</p> <p>此磁碟區的 inode 已用完，無法接受任何新檔案。</p>	增加磁碟區上的 inode 數量	將磁碟區上的 inode 數量增加 2%。
<p>偵測到儲存層策略不匹配</p> <p>該磁碟區具有大量非活動數據，且目前分層策略設定為「僅快照」或「無」。</p>	啟用自動雲端分層	由於磁碟區已經駐留在FabricPool上，它將分層策略變更為“自動”，以便將非活動資料移至成本較低的雲層。
<p>偵測到儲存層不匹配</p> <p>該磁碟區具有大量非活動數據，但它不駐留在支援雲端的儲存層 (FabricPool) 上。</p>	更改磁碟區的儲存層	將磁碟區移至支援雲端的儲存層，並將分層策略設為「自動」將非活動資料移至雲端。
<p>已禁用審計日誌</p> <p>儲存虛擬機器未啟用稽核日誌</p>	為儲存虛擬機器啟用審核日誌記錄	<p>在儲存虛擬機器上啟用稽核日誌記錄。</p> <p>請注意，儲存虛擬機器必須已經配置了本機或遠端稽核日誌位置。</p>
<p>登入橫幅已停用</p> <p>應啟用叢集的登入橫幅，透過明確存取限制來提高安全性。</p>	設定集群的登入橫幅	將叢集登入橫幅設定為「存取限制為授權使用者」。
<p>登入橫幅已停用</p> <p>應啟用儲存虛擬機器的登入橫幅，透過明確存取限制來提高安全性。</p>	為儲存虛擬機器設定登入橫幅	將儲存虛擬機器登入橫幅設定為「僅限授權使用者存取」。

事件名稱和描述	管理行動	“修復”操作
SSH 使用不安全的密碼 帶有後綴“-cbc”的密碼被認為是不安全的。	從叢集中刪除不安全的密碼	從叢集中刪除不安全的密碼 - 例如 aes192-cbc 和 aes128-cbc。
SSH 使用不安全的密碼 帶有後綴“-cbc”的密碼被認為是不安全的。	從儲存虛擬機器中刪除不安全的密碼	從儲存虛擬機器中刪除不安全的密碼 - 例如 aes192-cbc 和 aes128-cbc。
AutoSupport HTTPS 傳輸已停用 用於向技術支援發送AutoSupport訊息的傳輸協定應該加密。	將 HTTPS 設定為AutoSupport訊息的傳輸協定	將 HTTPS 設定為叢集上AutoSupport訊息的傳輸協定。
叢集負載不平衡閾值已突破 表示叢集中節點之間的負載不平衡。當節點間效能容量使用差異超過 30% 時，產生此事件。	平衡叢集工作負載	Unified Manager 確定從一個節點移動到另一個節點的最佳磁碟區以減少不平衡，然後移動該磁碟區。
集群容量不平衡閾值被突破 表示叢集中聚合之間的容量不平衡。當聚合之間的已使用容量差異超過 70% 時，會產生此事件。	平衡叢集容量	Unified Manager 確定從一個聚合移動到另一個聚合的最佳磁碟區以減少不平衡，然後移動該磁碟區。
已使用效能容量閾值已突破 表示如果不透過一個或多個高度活躍的工作負載來降低利用率，則節點上的負載可能會被過度利用。當節點效能容量使用值超過100%且持續12小時以上時，產生此事件。	限制節點的高負載	Unified Manager 識別具有最高 IOPS 的捲，並使用歷史預期和峰值 IOPS 等級應用 QoS 策略來減少節點上的負載。
動態事件警告閾值已突破 表示由於某些工作負載的負載異常高，該節點已經處於過載狀態。	減少節點過載	Unified Manager 識別具有最高 IOPS 的捲，並使用歷史預期和峰值 IOPS 等級應用 QoS 策略來減少節點上的負載。
無法進行收購 故障轉移目前已停用，因此在中斷或重新啟動期間對節點資源的存取將會遺失，直到節點再次可用為止。	啟用節點故障轉移	Unified Manager 會傳送適當的命令以在叢集中的所有節點上啟用故障轉移。

事件名稱和描述	管理行動	“修復”操作
<p>選項 Cf.takeover.on_panic 配置為關閉</p> <p>nodeshell 選項「cf.takeover.on_panic」設定為*off*，這可能會導致 HA 配置的系統出現問題。</p>	啟用恐慌接管	Unified Manager 向叢集發送適當的命令以將此設定變更為 on 。
<p>停用 nodeshell 選項 snapmirror.enable</p> <p>舊的 nodeshell 選項「snapmirror.enable」設定為 on，這可能會在升級到ONTAP 9.3 或更高版本後在啟動期間導致問題。</p>	將 snapmirror.enable 選項設定為關閉	Unified Manager 向叢集發送適當的命令以將此設定變更為 off 。
<p>已啟用 Telnet</p> <p>表示存在潛在的安全問題，因為 Telnet 不安全並且以未加密的方式傳遞資料。</p>	禁用 Telnet	Unified Manager 向叢集發送適當的命令以停用 Telnet。
<p>配置儲存 VM 反勒索軟體學習</p> <p>定期檢查具有反勒索軟體監控許可證的群集。驗證儲存虛擬機器在這樣的叢集中是否僅支援 NFS 或 SMB 磁碟區。</p>	將儲存虛擬機器放入 `learning` 反勒索軟體監控模式	Unified Manager 將反勒索軟體監控設定為 `learning` 透過叢集管理控制台查看儲存虛擬機器的狀態。儲存虛擬機器上建立的所有新磁碟區上的反勒索軟體監控都會自動轉入學習模式。透過此功能，ONTAP 可以了解磁碟區上的活動模式並偵測因潛在惡意攻擊而導致的異常。
<p>配置批量反勒索軟體學習</p> <p>定期檢查具有反勒索軟體監控許可證的群集。驗證磁碟區在這樣的叢集中是否僅支援 NFS 或 SMB 服務。</p>	將捲放入 `learning` 反勒索軟體監控模式	Unified Manager 將反勒索軟體監控設定為 `learning` 透過叢集管理控制台查看磁碟區的狀態。透過此功能，ONTAP 可以了解磁碟區上的活動模式並偵測因潛在惡意攻擊而導致的異常。
<p>啟用批量反勒索軟體</p> <p>定期檢查具有反勒索軟體監控許可證的群集。檢測卷是否在 `learning` 反勒索軟體監控模式超過 45 天，並確定將其置於主動模式的前景。</p>	將捲放入 `active` 反勒索軟體監控模式	Unified Manager 將反勒索軟體監控設定為 `active` 透過叢集管理控制台查看磁碟區上的狀態。透過此功能，ONTAP 可以了解磁碟區上的活動模式並偵測因潛在惡意攻擊而導致的異常，並為資料保護措施建立警報。

事件名稱和描述	管理行動	“修復”操作
<p>禁用批量反勒索軟體</p> <p>定期檢查具有反勒索軟體監控許可證的群集。在磁碟區進行主動反勒索軟體監控期間偵測重複通知（例如，30 天內多次返回潛在勒索軟體攻擊的警告）。</p>	禁用磁碟區上的反勒索軟體監控	Unified Manager 透過叢集管理控制台停用磁碟區上的反勒索軟體監控。

透過腳本覆蓋管理操作

您可以建立自訂腳本並將其與警報關聯，以針對特定事件採取特定操作，而不是選擇「管理操作」頁面或 Unified Manager 儀表板上可用的預設管理操作。

如果您想要針對某種事件類型採取特定操作，並選擇不將其作為 Unified Manager 提供的管理操作功能的一部分進行修復，則可以為特定操作配置自訂腳本。然後，您可以將腳本與該事件類型的警報關聯起來，並單獨處理此類事件。在這種情況下，管理操作頁面或 Unified Manager 儀表板上不會針對該特定事件類型產生管理操作。

管理集群

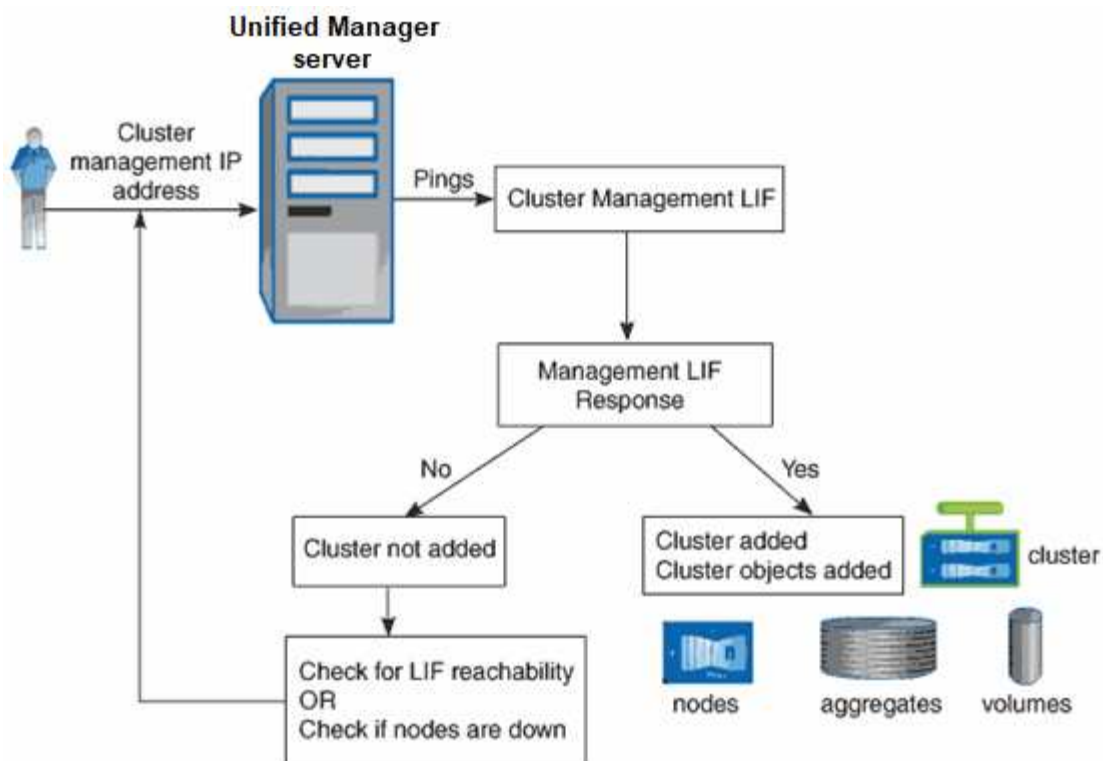
您可以使用 Unified Manager 監控、新增、編輯和刪除叢集來管理 ONTAP 叢集。

集群發現過程的工作原理

將叢集新增至 Unified Manager 後，伺服器會發現叢集物件並將其新增至其資料庫。了解發現過程的工作原理有助於您管理組織的集群及其物件。

收集群集配置資訊的監控間隔為 15 分鐘。例如，新增叢集後，需要 15 分鐘才能在 Unified Manager UI 中顯示叢集物件。對叢集進行變更時，此時間範圍也是如此。例如，如果您在叢集中的 SVM 中新增兩個新磁碟區，您將在下一個輪詢間隔（最長可達 15 分鐘）後在 UI 中看到這些新物件。

下圖說明了發現過程：



發現新叢集的所有物件後，Unified Manager 開始收集前 15 天的歷史效能資料。這些統計數據是使用數據連續性收集功能收集的。此功能可在新增叢集後立即為您提供該叢集超過兩週的效能資訊。資料連續性收集週期完成後，預設每五分鐘收集一次即時叢集效能資料。



由於收集 15 天的效能資料需要大量 CPU，因此建議您錯開新叢集的添加，以便資料連續性收集輪詢不會同時在太多叢集上運行。

查看監控叢集列表

您可以使用「集群設定」頁面來查看集群的清單。您可以查看有關集群的詳細信息，例如其名稱或 IP 位址和通訊狀態。

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」>「叢集設定」。

將顯示儲存環境中由 Unified Manager 管理的所有叢集。群集清單按收集狀態嚴重性等級列排序。您可以按下列標題來按不同列對叢集進行排序。

新增集群

您可以將叢集新增至 Active IQ Unified Manager，以便監控該叢集。這包括獲取叢集資訊的能力，例如叢集的健康狀況、容量、效能和配置，以便您可以發現並解決可能出現的任何問題。

開始之前

- 您必須具有應用程式管理員角色或儲存管理員角色。
- 您必須具有以下資訊：
 - Unified Manager 支援本機ONTAP叢集、ONTAP Select和Cloud Volumes ONTAP。
 - 您必須擁有叢集的主機名稱或叢集管理 IP 位址 (IPv4 或 IPv6)。

使用主機名稱時，它必須解析為叢集管理 LIF 的叢集管理 IP 位址。如果使用節點管理 LIF，操作將會失敗。

- 您必須擁有使用者名稱和密碼才能存取叢集。

此帳戶必須具有 *admin* 角色，並將應用程式存取權限設為 *ontapi*、*console* 和 *http*。

- 您必須知道使用 HTTPS 協定連接到叢集的連接埠號碼 (通常為連接埠 443)。
- 叢集必須運行ONTAP 9.9 版軟體或更高版本。
- Unified Manager 伺服器上必須有足夠的空間。當已消耗的空間超過 90% 時，您將無法為伺服器新增叢集。
- 您擁有所需的證書：

SSL (HTTPS) 憑證：此憑證歸 Unified Manager 所有。全新安裝 Unified Manager 時會產生預設的自簽章 SSL (HTTPS) 憑證。NetApp建議您將其升級為 CA 簽章憑證以獲得更好的安全性。如果伺服器憑證過期，您應該重新產生它並重新啟動 Unified Manager，以便服務合併新憑證。有關重新產生 SSL 憑證的更多信息，請參閱["產生 HTTPS 安全性憑證"](#)。

EMS 憑證：此憑證歸 Unified Manager 所有。它用於對從ONTAP接收的 EMS 通知進行身份驗證。

用於相互 **TLS** 通訊的憑證：在 Unified Manager 和ONTAP之間的相互 TLS 通訊期間使用。根據ONTAP 版本，為叢集啟用基於憑證的身份驗證。如果執行ONTAP版本的叢集低於 9.5，則不會啟用基於憑證的驗證。

如果您正在更新舊版的 Unified Manager，則不會自動為叢集啟用基於憑證的驗證。但是，您可以透過修改和儲存叢集詳細資訊來啟用它。如果憑證過期，您應該重新產生它以包含新憑證。有關查看和重新生成證書的更多信息，請參閱["編輯集群"](#)。



- 您可以從 Web UI 新增集群，並自動啟用基於憑證的身份驗證。
- 您可以透過 Unified Manager CLI 新增集群，預設不會啟用基於憑證的身份驗證。如果您使用 Unified Manager CLI 新增叢集，則需要使用 Unified Manager UI 編輯該叢集。您可以看到["支援的 Unified Manager CLI 命令"](#)使用 Unified Manager CLI 新增叢集。
- 如果為叢集啟用了基於憑證的驗證，並且您從伺服器備份 Unified Manager 並將其還原到主機名稱或 IP 位址已變更的另一個 Unified Manager 伺服器，則叢集的監控可能會失敗。為避免失敗，請編輯並儲存叢集詳細資訊。有關編輯集群詳細信息的更多信息，請參閱["編輯集群"](#)。
- 在叢集級別，Active IQ介面為身份驗證方法「cert」新增了兩個新的使用者群組條目。

+

集群證書：此證書歸ONTAP擁有。您無法將憑證已過期的叢集新增至 Unified Manager，如果憑證已過期，則應在新增叢集之前重新產生憑證。有關證書產生的信息，請參閱知識庫 (KB) 文章 ["如何在系統管理員使用"](#)

者介面中續訂ONTAP自簽名憑證"。

- Unified Manager 的單一實例可以支援特定數量的節點。如果您需要監控超出支援節點數的環境，則必須安裝額外的 Unified Manager 實例來監控某些叢集。若要查看支援的節點數列表，請參閱 "[Unified Manager 最佳實務指南](#)"。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在「叢集設定」頁面上，按一下「新增」。
3. 在新增叢集對話方塊中，根據需要指定值，然後按一下*提交*。
4. 在授權主機對話方塊中，按一下“檢視憑證”，查看叢集的憑證資訊。
5. 按一下“是”。

儲存叢集詳細資料後，您可以看到叢集的 Mutual TLS 通訊憑證。

如果未啟用基於憑證的驗證，Unified Manager 僅在最初新增叢集時檢查憑證。Unified Manager 不會檢查對ONTAP的每個 API 呼叫的憑證。

發現新叢集的所有物件後，Unified Manager 開始收集前 15 天的歷史效能資料。這些統計數據是使用數據連續性收集功能收集的。此功能可在新增叢集後立即為您提供該叢集超過兩週的效能資訊。資料連續性收集週期完成後，預設每五分鐘收集一次即時叢集效能資料。



- 收集 15 天的效能資料需要大量 CPU。NetApp建議您錯開新叢集的新增，以便資料連續性收集輪詢不會同時在太多叢集上執行。此外，如果您在資料連續性收集期間重新啟動 Unified Manager，則收集將停止，並且您將在效能圖表中看到缺失時間範圍的間隙。
- 當新增版本 9.14.1 或更高版本的ONTAP叢集時，通訊將透過雲端代理功能進行。ONTAP會自動建立具有唯讀權限的內部服務帳戶使用者（例如，clus-agent-xxxx）。如果出現以下情況，Unified Manager 將停止從這些叢集收集數據 `clus-agent` 用戶已刪除。

如果您收到無法新增叢集的錯誤訊息，請檢查是否有以下問題：



- 如果兩個系統上的時鐘不同步，且 Unified Manager HTTPS 憑證的開始日期晚於叢集上的日期。您必須確保使用 NTP 或類似服務同步時鐘。
- 如果叢集已達到 EMS 通知目標的最大數量，則無法新增 Unified Manager 位址。預設情況下，叢集上只能定義 20 個 EMS 通知目的地。

相關資訊

["新增用戶"](#)

["查看集群列表和詳細信息"](#)

["安裝 CA 簽署並傳回的 HTTPS 憑證"](#)

編輯集群

您可以使用編輯叢集對話方塊修改現有叢集的設置，例如主機名稱或 IP 位址、使用者名

稱、密碼和連接埠。

開始之前

您必須具有應用程式管理員角色或儲存管理員角色。



從 Unified Manager 9.7 開始，只能使用 HTTPS 新增叢集。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在「集群設定」頁面上，選擇要編輯的集群，然後按一下「編輯」。
3. 在「編輯集群」對話方塊中，根據需要修改值。+ 如果您修改了新增至 Unified Manager 的叢集的詳細信息，則可以基於ONTAP版本查看 Mutual TLS 通訊的憑證詳細資訊。有關ONTAP版本的更多信息，請參閱["用於相互 TLS 通訊的證書"](#)。+ 您可以點選*證書詳情*查看證書詳情。如果憑證已過期，請按一下「重新產生」按鈕以合併新憑證。
4. 點選“提交”。
5. 在授權主機對話方塊中，按一下“檢視憑證”，查看叢集的憑證資訊。
6. 按一下“是”。

相關資訊

["新增用戶"](#)

["查看集群列表和詳細信息"](#)

刪除叢集

您可以使用叢集設定頁面從 Unified Manager 中刪除叢集。例如，如果叢集發現失敗，或者您想要退役儲存系統時，您可以刪除叢集。

開始之前

您必須具有應用程式管理員角色或儲存管理員角色。

此任務將從 Unified Manager 中刪除選取的叢集。叢集被刪除後，它將不再受到監控。在已刪除的叢集中註冊的 Unified Manager 實例也將從叢集中取消註冊。

刪除叢集也會從 Unified Manager 中刪除其所有儲存物件、歷史資料、儲存服務以及所有相關事件。這些變更將在下一個資料收集週期後反映在庫存頁面和詳細資料頁面上。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在「集群設定」頁面上，選擇要刪除的集群，然後按一下「刪除」。
3. 在「刪除資料來源」訊息對話方塊中，按一下「刪除」以確認刪除要求。

相關資訊

["新增用戶"](#)

["查看集群列表和詳細信息"](#)

重新發現集群

您可以從「集群設定」頁面手動重新發現集群，以獲取有關集群的健康狀況、監控狀態和效能狀態的最新資訊。

當您想要更新叢集（例如，在空間不足時增加聚合的大小）並且希望 Unified Manager 發現您所做的變更時，您可以手動重新發現叢集。

當 Unified Manager 與 OnCommand Workflow Automation (WFA) 配對時，該配對會觸發重新取得 WFA 快取的資料。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「叢集設定」。
2. 在「叢集設定」頁面上，按一下「重新發現」。

Unified Manager 重新發現選定的叢集並顯示最新的運作狀況和效能狀態。

相關資訊

["查看集群列表和詳細信息"](#)

監控 VMware 虛擬基礎架構

Active IQ Unified Manager 提供對虛擬基礎架構中虛擬機器 (VM) 的可見性，並支援監控和排除虛擬環境中的儲存和效能問題。您可以使用此功能來確定儲存環境中的任何延遲問題，或確定 vCenter Server 上報告的效能事件。

ONTAP 上的典型虛擬基礎架構部署具有分佈在運算、網路和儲存層的各種元件。VM 應用程式中的任何效能滯後都可能是由於各個層上的各個元件所面臨的延遲組合所造成的。此功能對於需要分析虛擬環境中的效能問題並了解問題發生在哪個元件中的儲存和 vCenter Server 管理員和 IT 通才非常有用。

現在您可以從 VMware 部分的 vCenter 選單存取 vCenter Server。列出的每個虛擬機的預覽視圖在拓撲視圖中都有 **VCENTER SERVER** 鏈接，可在新瀏覽器中啟動 vCenter Server。您也可以使用*擴充拓樸*按鈕啟動 vCenter Server，然後按一下*在 vCenter 中檢視*按鈕檢視 vCenter Server 中的資料儲存體。

Unified Manager 以拓撲視圖的形式呈現虛擬環境的底層子系統，以確定計算節點、網路或儲存中是否出現了延遲問題。該視圖還突出顯示了導致效能滯後的具體對象，以便採取補救措施並解決根本問題。

部署在 ONTAP 儲存上的虛擬基礎架構包括以下物件：

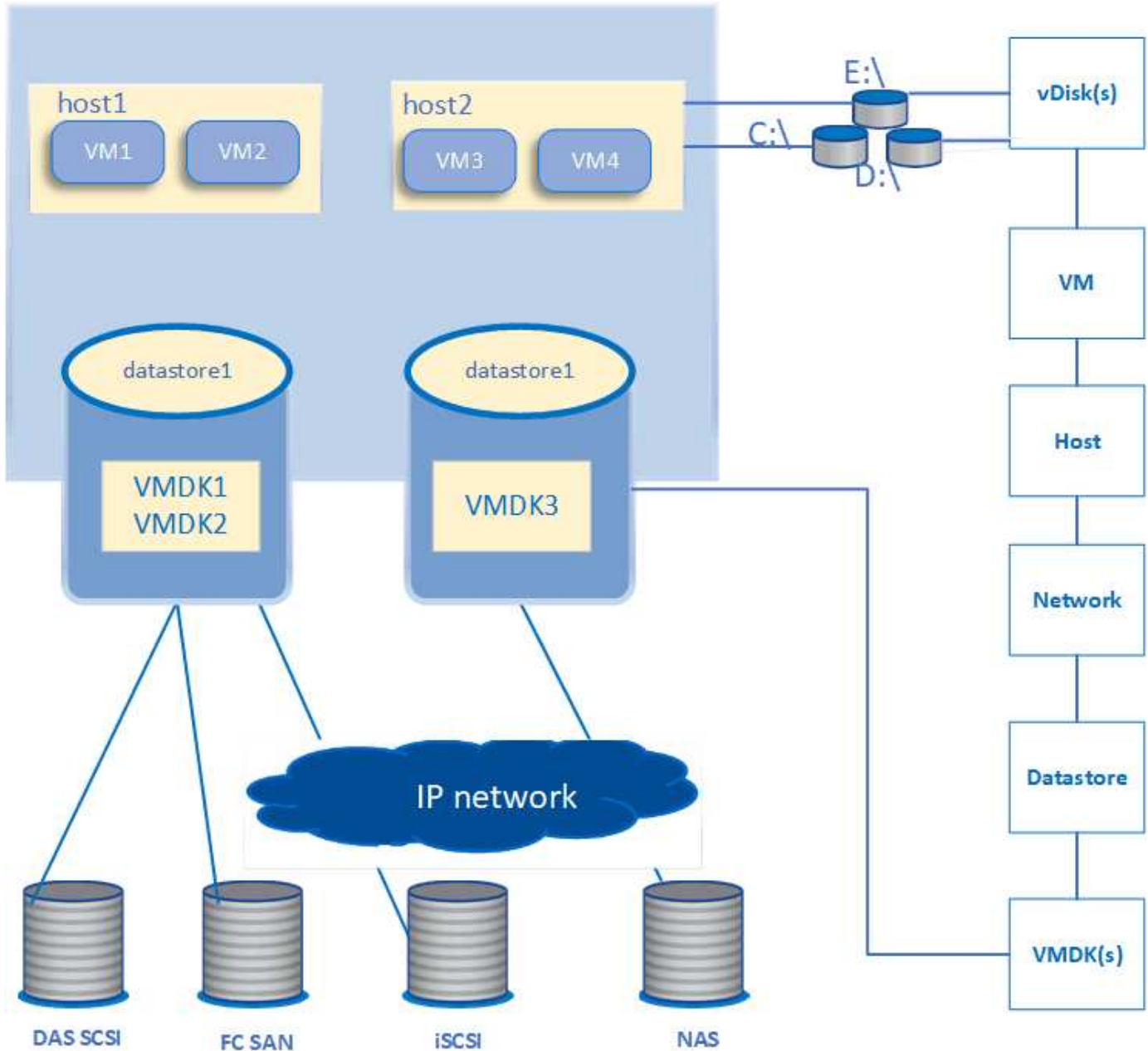
- vCenter Server：用於管理虛擬環境中的 VMware VM、ESXi 主機和所有相關元件的集中控制平面。有關 vCenter Server 的更多信息，請參閱 VMware 文件。
- 主機：執行 ESXi (VMware 的虛擬化軟體) 並託管 VM 的實體或虛擬系統。
- 資料儲存：資料儲存是連接到 ESXi 主機的虛擬儲存物件。資料儲存庫是 ONTAP 的可管理儲存實體，例如 LUN 或磁碟區，用作 VM 檔案（例如日誌檔案、腳本、設定檔和虛擬磁碟）的儲存庫。它們透過 SAN 或 IP 網路連接與環境中的主機連接。對應到 vCenter Server 的 ONTAP 以外的資料儲存庫不受 Unified Manager

支援或顯示。

- VM：VMware 虛擬機器。
- 虛擬磁碟：屬於虛擬機器的資料儲存區上的副檔名為 VMDK 的虛擬磁碟。虛擬磁碟中的資料儲存在對應的 VMDK 上。
- VMDK：資料儲存上的虛擬機器磁碟，為虛擬磁碟提供儲存空間。對於每個虛擬磁碟，都有一個對應的 VMDK。

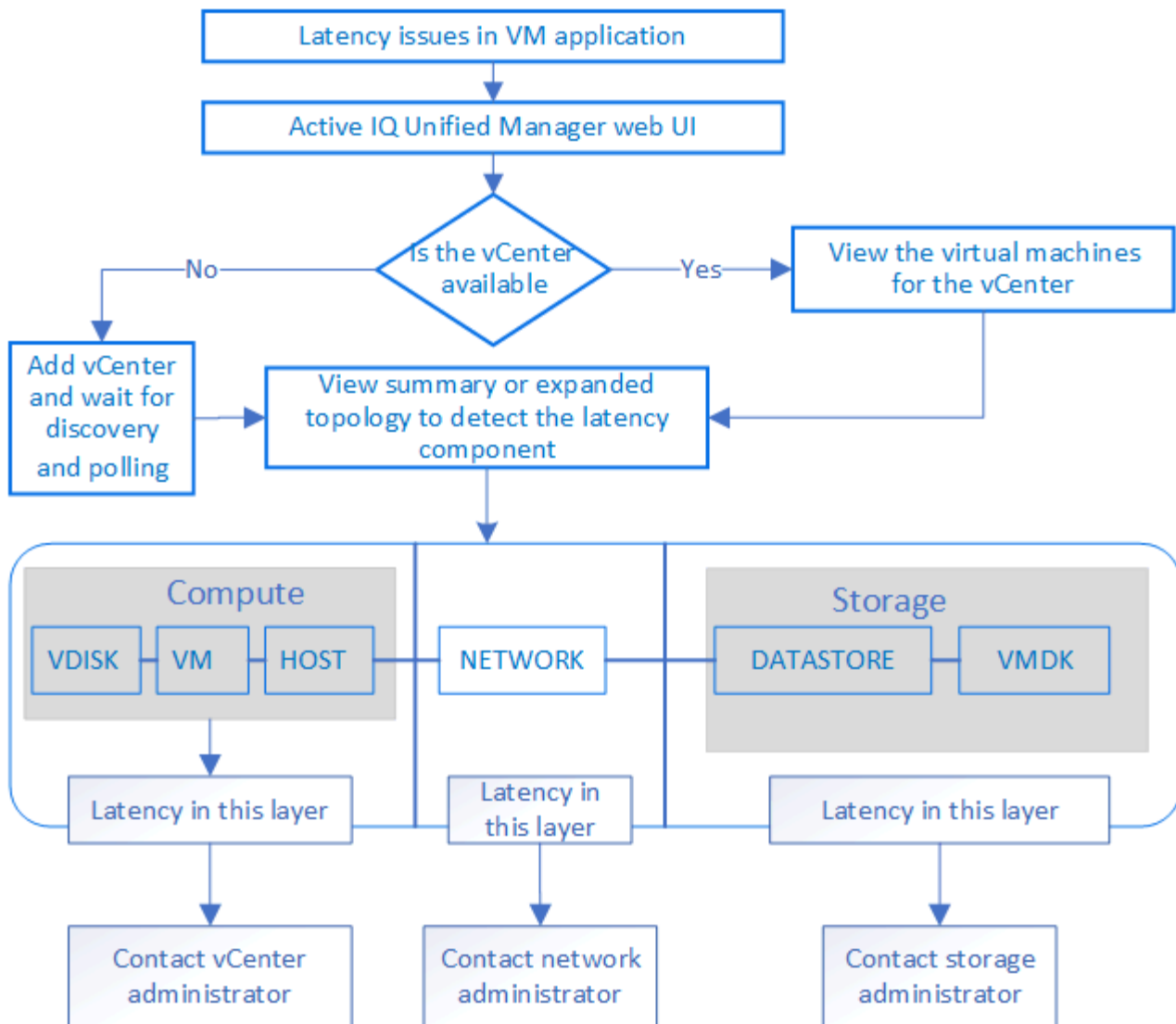
這些物件在 VM 拓撲視圖中表示。

ONTAP上的 VMware 虛擬化



使用者工作流程

下圖顯示了使用 VM 拓撲視圖的典型用例：



不支援的內容

- Unified Manager 不支援位於ONTAP之外並對應到 vCenter Server 執行個體的資料儲存庫。這些資料儲存區上具有虛擬磁碟的任何虛擬機器也不受支援。
- 不支援跨多個 LUN 的資料儲存。
- 不支援使用網路位址轉換 (NAT) 來映射資料 LIF (存取端點) 的資料儲存。
- 不支援在多 LIF 配置中將磁碟區或 LUN 匯出為具有相同 IP 位址的不同叢集上的資料存儲，因為 Unified Manager 無法識別哪個資料儲存屬於哪個叢集。

範例：假設叢集 A 具有資料儲存庫 A。資料儲存庫 A 透過具有相同 IP 位址 xxxx 的資料 LIF 匯出，且虛擬機器 A 在此資料儲存庫上建立。類似地，集群 B 具有資料儲存庫 B。資料儲存庫 B 透過相同 IP 位址 xxxx 的資料 LIF 匯出，並在資料儲存庫 B 上建立 VM B。UM 既無法將 VM A 拓樸的資料儲存庫 A 對應到對應的ONTAP磁碟區/LUN，也無法對應 VM B。

- 僅支援 NAS 和 SAN 磁碟區 (用於 VMFS 的 iSCSI 和 FCP) 作為資料存儲，不支援虛擬磁碟區 (vVols)。
- 僅支援 iSCSI 虛擬磁碟。不支援 NVMe 和 SATA 類型的虛擬磁碟。
- 這些視圖不允許您產生用於分析各個元件效能的報表。

- 對於僅支援 Unified Manager 上的虛擬基礎架構的儲存虛擬機器 (storage VM) 災難復原 (DR) 設定，必須在 vCenter Server 中手動變更配置以指向切換和切換回場景中的活動 LUN。如果沒有人工幹預，他們的資料儲存將無法存取。

檢視並新增 vCenter Server

若要檢視並排除虛擬機器 (VM) 效能故障，必須在 Active IQ Unified Manager 個體上新增關聯的 vCenter Server。

開始之前

在新增或檢視 vCenter Server 之前，請確保以下事項：

- 您知道 vCenter Server 名稱。
- 您知道 vCenter Server 的 IP 位址並擁有所需的憑證。憑證必須屬於 vCenter Server 管理員或具有 vCenter Server 唯讀存取權限的 root 使用者。
- 您要新增的 vCenter Server 執行 vSphere 6.5 或更高版本。



Unified Manager 對 VMware ESXi 和 vCenter Server 的支援提供英文和日文版本。

- vCenter Server 中的資料收集設定被設定為 *Level 3*，確保所有監控對象都達到所需的指標收集水準。間隔時間應為 *5 minutes*，保存期限應為 *1 day*。

有關詳細信息，請參閱 VMware 文件中的《vSphere 監控和效能指南》的「資料收集等級」部分。

- 為了成功計算延遲值，vCenter Server 中的延遲值以毫秒為單位進行配置，而不是以微秒為單位。
- 將資料儲存區新增至 vCenter Server 時，您可以同時使用主機的 IP 位址或完全限定網域名稱 (FQDN)。如果您要新增 FQDN，請確保 Unified Manager 伺服器可以解析該網域名稱。例如，對於 Linux 安裝，請確保在 `/etc/resolv.conf` 文件。
- vCenter Server 的目前時間與 vCenter Server 時區同步。
- vCenter Server 可成功存取並發現。
- 將 vCenter Server 新增至 Unified Manager 時，您具有對 VMware SDK 的讀取權限。這是配置輪詢所必需的。

對於新增和發現的每個 vCenter Server，Unified Manager 都會收集配置數據，例如 vCenter Server 和 ESXi 伺服器詳細資訊、ONTAP 映射、資料儲存詳細資訊以及託管的虛擬機器數量。它進一步收集組件的性能指標。

步驟

1. 前往 **VMWARE > vCenter**，並檢查您的 vCenter Server 是否在清單中。



如果您的 vCenter Server 不可用，則必須新增 vCenter Server。

- a. 按一下“新增”。
- b. 為 vCenter Server 新增正確的 IP 位址並確保該裝置可存取。
- c. 新增具有 vCenter Server 唯讀存取權限的管理員或 root 使用者的使用者名稱和密碼。
- d. 如果您使用除預設 443 之外的任何端口，請新增自訂端口號。

- e. 點選“儲存”。

成功發現後，將顯示伺服器憑證供您接受。

當您接受憑證時，vCenter Server 將會被加入到可用 vCenter Server 清單中。新增設備不會導致相關虛擬機器的資料收集，並且收集會按照計劃的時間間隔進行。

2. 如果您的 vCenter Server 在 **vCenters** 頁面上可用，請將滑鼠懸停在 **Status** 欄位上檢查其狀態，以顯示您的 vCenter Server 是否按預期運行，或者是否有警告或錯誤。



新增 vCenter Server 可讓您查看以下狀態。但是，在新增 vCenter Server 後，對應虛擬機器的效能和延遲資料可能需要長達一小時才能準確反映。

- 綠色：“正常”，表示已發現 vCenter Server，並且已成功收集效能指標
- 黃色：“警告”（例如，當 vCenter Server 的統計等級未設定為 3 或更高以取得每個物件的統計資料時）
- 橘色：“錯誤”（表示任何內部錯誤，例如異常、設定資料收集失敗或 vCenter Server 無法存取）您可以按一下下列顯示圖示（顯示/隱藏）來查看 vCenter Server 狀態的狀態訊息並解決問題。

3. 如果 vCenter Server 無法存取或憑證已更改，請選擇 **vCenter > 編輯** 來編輯 vCenter Server 詳細資訊。
4. 在*編輯 VMware vCenter Server* 頁面上進行必要的變更。
5. 點選“儲存”。

vCenter Server 資料收集開始

vCenter Server 收集即時 20 秒效能資料樣本，並將其匯總為 5 分鐘樣本。Unified Manager 效能資料收集計畫是基於 vCenter Server 的預設值。Unified Manager 處理從 vCenter Server 取得的 5 分鐘樣本，並計算虛擬磁碟、虛擬機器和主機的 IOPS 和延遲的每小時平均值。對於資料儲存庫，Unified Manager 根據從 ONTAP 取得的樣本計算每小時的 IOPS 和延遲平均值。這些值在整點時可用。新增 vCenter Server 後，效能指標不會立即可用，只有下一小時開始時才可用。效能資料輪詢在完成配置資料收集週期後開始。

對於輪詢 vCenter Server 設定數據，Unified Manager 遵循與收集叢集配置資料相同的計劃。有關 vCenter Server 配置和效能資料收集計劃的信息，請參閱「叢集配置和效能資料收集活動」。

相關資訊

["叢集配置和效能資料收集活動"](#)

移除 vCenter Server

您可以從 Active IQ Unified Manager 實例中刪除 vCenter Server。例如，如果 vCenter Server 發現失敗或不再需要該 vCenter Server，您可以將其移除。

刪除 vCenter Server 也會刪除該 vCenter 上託管的所有虛擬機器 (VM) 及其設定資料。刪除 vCenter Server 後，它將不再受到監控，同時也不會再監控其相關物件和歷史資料。這些變更將反映在 vCenter 和虛擬機器庫存頁面上。

開始之前

刪除 vCenter Server 之前，請確保以下事項：

- 您具有應用程式管理員角色或儲存管理員角色。
- 您應該了解 vCenter Server 名稱以及與其關聯的相應 IP 位址。

步驟

1. 在左側導覽窗格中，按一下 **VMWARE>vCenter**。
2. 在 vCenters 頁面上，選擇要刪除的 vCenter Server，然後按一下「刪除」。
3. 在「刪除 vCenter」訊息對話方塊中，按一下「確定」確認刪除要求。

監控虛擬機

對於虛擬機器 (VM) 應用程式上的任何延遲問題，您可能需要監控虛擬機器以分析和排除原因。當虛擬機器的 vCenter Server 和託管虛擬機器儲存的 ONTAP 叢集新增至 Unified Manager 時，虛擬機器可用。

您可以在 **VMWARE >> 虛擬機器** 頁面上看到虛擬機器的詳細資訊。顯示可用性、狀態、已使用和已分配容量、網路延遲以及虛擬機器、資料儲存區和主機의 IOPS 和延遲等資訊。對於支援多個資料儲存區的虛擬機，網格顯示延遲最嚴重的資料儲存區的指標，星號圖示 (*) 表示其他資料儲存區。如果按一下該圖標，則會顯示附加資料儲存的指標。其中一些列不可用於排序和過濾。



要查看虛擬機器及其詳細信息，必須完成 ONTAP 叢集的發現（輪詢或指標收集）。如果從 Unified Manager 中刪除集群，則在下一個發現週期之後，虛擬機器將不再可用。

從此頁面，您還可以查看虛擬機器的詳細拓撲，顯示與虛擬機器相關的元件，例如連接到它的主機、虛擬磁碟和資料儲存。拓撲視圖會依照下列順序顯示特定層中的底層元件：虛擬磁碟 > **VM** > 主機 > 網路 > 資料儲存 > **VMDK**。

您可以從拓撲角度確定 I/O 路徑和元件級延遲，並確定儲存是否是導致效能問題的原因。拓撲的摘要視圖顯示 I/O 路徑，並反白顯示具有 IOPS 和延遲問題的元件，以便您決定故障排除步驟。您還可以獲得拓撲的擴展視圖，該視圖分別描述每個組件以及該組件的延遲。您可以選擇一個元件來決定透過各層突出顯示的 I/O 路徑。

查看摘要拓撲

若要透過查看摘要拓撲中的虛擬機器來確定效能問題：

1. 前往 **VMWARE > 虛擬機器**。
2. 在搜尋框中輸入虛擬機器名稱來搜尋虛擬機器。您也可以透過點擊“過濾器”按鈕根據特定條件過濾搜尋結果。但是，如果您找不到您的虛擬機，請確保已新增並發現對應的 vCenter Server。



vCenter Server 允許在 vSphere 實體（例如 VM、群集、資料儲存區、資料夾或檔案）的名稱中使用特殊字元（例如 %, &、\、\$、#、@、!、\、/、:、\、?、"、<、>、|、;、'）。VMware vCenter Server 和 ESX/ESXi Server 不會轉義顯示名稱中使用的特殊字元。但是，在 Unified Manager 中處理該名稱時，顯示方式會有所不同。例如，名為 ``%$VC_AIQUM_clone_191124%` 在 vCenter Server 中顯示為 ``%25$VC_AIQUM_clone_191124%25`` 在統一管理器中。當您查詢名稱中包含特殊字元的虛擬機器時，必須記下此問題。

3. 檢查虛擬機器的狀態。VM 狀態從 vCenter Server 檢索。有以下狀態可用。有關這些狀態的更多信息，請參閱 VMware 文件。

- 普通的
 - 警告
 - 警報
 - 未受監控
 - 未知
4. 按一下虛擬機器旁的向下箭頭以查看運算、網路和儲存層元件的拓撲摘要檢視。存在延遲問題的節點被突出顯示。摘要視圖顯示組件的最差延遲。例如，如果虛擬機器有多個虛擬磁碟，則此視圖顯示所有虛擬磁碟中延遲最差的虛擬磁碟。
 5. 若要分析資料儲存在一段時間內的延遲和吞吐量，請按一下資料儲存物件圖示頂部的「工作負載分析器」按鈕。您轉到工作負載分析頁面，您可以在其中選擇時間範圍並查看資料儲存的效能圖表。有關工作負載分析器的更多信息，請參閱_使用工作負載分析器排除工作負載故障_。

查看擴充拓撲

您可以透過查看虛擬機器的擴展拓撲來深入了解每個組件。

步驟

1. 從摘要拓撲視圖中，按一下*展開拓撲*。您可以分別查看每個組件的詳細拓撲以及每個物件的延遲數。如果某個類別中有多個節點（例如資料儲存或 VMDK 中的多個節點），則延遲最差的節點將以紅色突出顯示。
2. 若要檢查特定物件的 IO 路徑，請按一下該物件以查看 IO 路徑和對應的對應。例如，要查看虛擬磁碟的映射，請按一下虛擬磁碟以查看其與相應 VMDK 的突出顯示的映射。如果這些組件的效能出現滯後，您可以從ONTAP收集更多資料並解決問題。



未報告 VMDK 的指標。在拓撲中，僅顯示 VMDK 名稱，而不顯示指標。

相關資訊

["使用工作負載分析器排除工作負載故障"](#)

查看災難復原設定中的虛擬基礎架構

您可以查看MetroCluster配置或儲存虛擬機器 (儲存 VM) 災難復原 (SVM DR) 設定中託管的資料儲存庫的配置和效能指標。

在 Unified Manager 上，您可以查看MetroCluster配置中作為 vCenter Server 中的資料儲存附加的 NAS 磁碟區或 LUN。MetroCluster配置中託管的資料儲存庫與標準環境中的資料儲存庫在相同的拓撲視圖中表示。

您也可以查看儲存虛擬機器災難復原配置中對應到 vCenter Server 中的資料儲存區的 NAS 磁碟區或 LUN。

查看MetroCluster配置中的資料存儲

在查看MetroCluster配置中的資料儲存之前，請注意以下先決條件：

- 在發生切換和切換回時，HA 對的主集群和輔助集群以及 vCenter Server 的發現應該是完整的。
- HA 對的主叢集和輔助叢集以及 vCenter Server 必須由 Unified Manager 管理。

- 必須在ONTAP和 vCenter Server 上完成所需的設定。有關信息，請參閱ONTAP和 vCenter 文件。

"ONTAP 9 文檔中心"

請依照以下步驟查看資料儲存：

1. 在 **VMWARE** > 虛擬機器 頁面上，按一下託管資料儲存區的 VM。按一下“工作負載分析器”或資料儲存物件連結。在標準場景中，當託管磁碟區或 LUN 的主網站按預期執行時，您可以看到主網站的 vServer 叢集詳細資訊。
2. 當災難發生並連續切換到輔助站點時，資料儲存連結指向輔助叢集中磁碟區或 LUN 的效能指標。這在下一個叢集和 vServer 發現（獲取）週期完成後反映出來。
3. 成功切換後，資料儲存連結再次反映主集群中捲或 LUN 的效能指標。這在下一個叢集和 vServer 發現週期完成後反映出來。

查看儲存虛擬機器災難復原配置中的資料存儲

在查看儲存虛擬機器災難復原配置中的資料儲存之前，請注意以下先決條件：

- 在發生切換和切換回時，HA 對的主集群和輔助集群以及 vCenter Server 的發現應該是完整的。
- 來源叢集和目標叢集以及儲存虛擬機器對等體都應由 Unified Manager 管理。
- 必須在ONTAP和 vCenter Server 上完成所需的設定。
 - 對於 NAS（NFS 和 VMFS）資料儲存區，如果發生災難，步驟包括啟動輔助儲存虛擬機器、驗證資料 LIF 和路由、在 vCenter Server 上建立遺失的連線以及啟動虛擬機器。

為了切換回主站點，應在主站點開始提供資料之前同步磁碟區之間的資料。

- 對於 SAN（iSCSI 和 VMFS 的 FC）資料存儲，vCenter Server 將掛載的 LUN 格式化為 VMFS 格式。如果發生災難，步驟包括啟動輔助儲存虛擬機器、驗證資料 LIF 和路由。如果 iSCSI 目標 IP 與主 LIF 不同，則需要手動新增。新的 LUN 應該作為主機儲存适配器的 iSCSI 适配器下的裝置可用。此後，應建立具有新 LUN 的新 VMFS 資料存儲，並使用新名稱註冊舊 VM。虛擬機器必須啟動並運作。

如果發生恢復，則磁碟區之間的資料應該同步。應使用 LUN 和以新名稱註冊的舊 VM 再次建立新的 VMFS 資料儲存。

有關設定的信息，請參閱ONTAP和 vCenter Server 文件。

"ONTAP 9 文檔中心"

請依照以下步驟查看資料儲存：

1. 在 **VMWARE** > 虛擬機器 頁面上，按一下託管資料儲存區的 VM 清單。按一下資料儲存物件連結。在標準場景中，您可以看到主儲存VM中磁碟區和LUN的效能資料。
2. 當災難發生並連續切換到輔助儲存虛擬機器時，資料儲存連結指向輔助儲存虛擬機器中的磁碟區或 LUN 的效能指標。這在下一個叢集和 vServer 發現（獲取）週期完成後反映出來。
3. 成功切換後，資料儲存連結再次反映主儲存虛擬機器中磁碟區或 LUN 的效能指標。這在下一個叢集和 vServer 發現週期完成後反映出來。

不支援的場景

- 對於MetroCluster配置，請注意以下限制：
 - 僅在 `NORMAL`` 和 ``SWITCHOVER`` 各州都已開始採取行動。其他州，例如 ``PARTIAL_SWITCHOVER,`
`PARTIAL_SWITCHBACK,` 和 ``NOT_REACHABLE`` 不受支援。
 - 除非啟用自動切換 (ASO)，否則如果主集群發生故障，則無法發現輔助集群，並且拓撲將繼續指向主集群中的磁碟區或 LUN。
- 對於儲存虛擬機器災難復原配置，請注意以下限制：
 - 不支援為 SAN 儲存環境啟用網站復原管理器 (SRM) 或儲存複製適配器 (SRA) 的配置。

預配和管理工作負載

Active IQ Unified Manager的主動管理功能提供效能服務等級、儲存效率原則和儲存提供者 API，用於設定、監控和管理資料中心中的儲存工作負載。



Unified Manager 預設提供此功能。如果您不打算使用此功能，您可以從*儲存管理*>*功能設定* 中停用它。

啟用後，您可以在由 Unified Manager 實例管理的ONTAP叢集上設定工作負載。您也可以為工作負載指派策略，例如效能服務等級和儲存效率策略，並根據這些策略管理您的儲存環境。

此功能可實現以下功能：

- 自動發現新增的叢集上的儲存工作負載，從而輕鬆評估和部署儲存工作負載
- 配置支援 NFS 和 CIFS 協定的 NAS 工作負載
- 配置支援 iSCSI 和 FCP 協定的 SAN 工作負載
- 在同一文件共享上支援 NFS 和 CIFS 協議
- 效能服務等級和儲存效率策略的管理
- 為儲存工作負載分配效能服務等級和儲存效率策略

UI 左側窗格上的 **Provisioning**、**Storage > Workloads** 和 **Policies** 選項可讓您修改各種設定。

您可以使用這些選項執行下列功能：

- 在「儲存」>「工作負載」頁面上查看儲存工作負載
- 從「配置工作負載」頁面建立儲存工作負載
- 根據策略建立和管理效能服務級別
- 從策略建立和管理儲存效率策略
- 從「工作負載」頁面向儲存工作負載指派策略

相關資訊

["基於策略的儲存管理"](#)

工作負載概述

工作負載表示儲存物件（例如磁碟區或 LUN）的輸入/輸出 (I/O) 操作。儲存的配置方式取決於預期的工作負載要求。只有當有流量往返於儲存物件後，Active IQ Unified Manager 才會追蹤工作負載統計資料。例如，使用者開始使用資料庫或電子郵件應用程式後，即可獲得工作負載 IOPS 和延遲值。

「工作負載」頁面顯示由 Unified Manager 管理的 ONTAP 叢集的儲存工作負載摘要。它提供了符合效能服務水準的儲存工作負載以及不符合效能服務水準的儲存工作負載的累積概覽資訊。它還使您能夠評估整個資料中心叢集的總容量、可用容量和已使用容量和效能 (IOPS)。



建議您評估不符合要求、不可用或不受任何效能服務等級管理的儲存工作負載的數量，並採取必要的措施來確保其一致性、容量使用率和 IOPS。

工作負載頁面包含以下兩個部分：

- 工作負載概覽：提供 Unified Manager 管理的 ONTAP 叢集上的儲存工作負載數量的概覽。
- 資料中心概覽：提供資料中心內儲存工作負載的容量和 IOPS 概覽。相關數據顯示在資料中心層級和個人層級。

工作負載概述部分

工作負載概覽部分提供了儲存工作負載的累積概覽資訊。儲存工作負載的狀態會根據已指派和未指派的效能服務等級顯示。

- 已指派：針對已指派效能服務等級的儲存工作負載報告下列狀態：
 - 符合：儲存工作負載的效能取決於指派給它們的效能服務等級。如果儲存工作負載在相關效能服務等級中定義的閾值延遲範圍內，則將其標記為「符合」。符合要求的工作負載以藍色標示。
 - 不符合：在效能監控期間，如果儲存工作負載延遲超過相關效能服務等級中定義的閾值延遲，則儲存工作負載將被標記為「不符合」。不符合要求的工作負載以橘色標示。
 - 不可用：如果儲存工作負載處於離線狀態，或者相應的叢集無法訪問，則會被標記為「不可用」。不可用的工作負載以紅色標示。
- 未分配：未分配效能服務等級的儲存工作負載被報告為「未分配」。該數字由資訊圖示傳達。

總工作負載數是已分配工作負載和未分配工作負載的總和。

您可以按一下此部分顯示的工作負載總數，然後在工作負載頁面查看它們。

依效能服務等級符合性子部分顯示可用儲存工作負載的總數：

- 符合各類績效服務水平
- 指派的效能服務等級與建議的效能服務等級不匹配

資料中心概述部分

資料中心概覽部分以圖形方式表示資料中心中所有叢集的可用和已使用容量以及 IOPS。透過使用這些數據，您應該管理儲存工作負載的容量和 IOPS。該部分還顯示所有叢集的儲存工作負載的以下資訊：

- 資料中心內所有叢集的總容量、可用容量和已使用容量
- 資料中心內所有群集的總 IOPS、可用 IOPS 和已使用 IOPS
- 基於每個效能服務等級的可用容量和已使用容量
- 基於每個效能服務等級的可用和已使用 IOPS
- 未分配效能服務等級的工作負載所使用的總空間和 IOPS

如何根據效能服務等級計算資料中心容量和效能

已使用容量和 IOPS 是根據叢集中所有儲存工作負載的總已使用容量和效能來檢索的。

可用的 IOPS 是根據節點上的預期延遲和建議的效能服務等級計算的。它包括預期延遲小於或等於其自身預期延遲的所有效能服務等級的可用 IOPS。

可用容量是根據預期延遲和聚合體的建議性能服務等級計算的。它包括所有效能服務等級的可用容量，這些等級的預期延遲小於或等於其自身的預期延遲。

查看工作負載

當您將叢集新增至 Unified Manager 時，每個叢集上的儲存工作負載都會自動被發現並顯示在「工作負載」頁面上。

只有在儲存工作負載上開始 I/O 操作後，Unified Manager 才會開始分析工作負載以供建議（建議的 PSL）。

FlexGroup 卷及其組成部分被排除在外。

工作負載概述

工作負載概覽頁面顯示資料中心內工作負載的概覽以及資料中心的空間和效能概覽。

- ***工作負載概覽*面板**：顯示工作負載總數以及分配了或未分配 PSL 的工作負載數量。也顯示了每個 PSL 的工作量計數的細分。點擊計數將帶您進入包含已過濾工作負載的「所有工作負載」視圖。您也可以查看不符合系統建議的工作負載數量，並透過點擊「指派系統建議的 PSL」按鈕為其指派系統建議的 PSL。
- ***資料中心概覽*面板**：顯示資料中心的可用和已使用空間（TiB）和效能（IOPS）。也顯示每個 PSL 下所有工作負載的可用和已使用空間（TiB）和效能（IOPS）的細分。

所有工作負載視圖

儲存 > 工作負載 > 所有工作負載 頁面列出了與 Unified Manager 管理的 ONTAP 叢集相關的儲存工作負載。

對於新發現的尚未進行 I/O 操作的儲存工作負載，狀態為「等待 I/O」。在儲存工作負載上開始 I/O 作業後，Unified Manager 開始分析，工作負載狀態變成「學習中...」。分析完成後（從 I/O 操作開始後的 24 小時內），將顯示針對儲存工作負載的建議 PSL。

此頁面還可讓您為儲存工作負載指派儲存效率策略 (SEP) 和效能服務等級 (PSL)。您可以執行多項任務：

- 新增或配置儲存工作負載
- 查看和過濾工作負載列表
- 將 PSL 分配給儲存工作負載

- 評估系統建議的 PSL 並將其分配給工作負載
- 將 SEP 分配給儲存工作負載

新增或配置儲存工作負載

您可以將儲存工作負載新增或設定到支援的 LUN（支援 iSCSI 和 FCP 協定）、NFS 檔案共用和 SMB 共用。

步驟

1. 按一下「儲存」>「工作負載」>「所有工作負載」>「建立」。
2. 建立工作負載。有關信息，請參閱["預配和管理工作負載"](#)。

查看和過濾工作負載

在「所有工作負載」畫面上，您可以查看資料中心中的所有工作負載，或根據 PSL 或名稱搜尋特定的儲存工作負載。您可以使用篩選器圖示輸入特定的搜尋條件。您可以根據不同的篩選條件進行搜索，例如按主機叢集或儲存虛擬機器。**Capacity Total** 選項允許按工作負載的總容量（以 MB 為單位）進行過濾。但是，在這種情況下，傳回的工作負載數量可能會有所不同，因為總容量是在位元組層級進行比較的。

對於每個工作負載，都會顯示主機叢集和儲存虛擬機器等信息，以及分配的 PSL 和 SEP。

該頁面還允許您查看工作負載的效能詳細資訊。您可以透過點擊「選擇/排序列」按鈕並選擇要查看的特定欄位來查看有關工作負載的 IOPS、容量和延遲的詳細資訊。效能視圖列顯示工作負載的平均 IOPS 和峰值 IOPS，您可以按一下工作負載分析器圖示以查看詳細的 IOPS 分析。

分析工作負載的效能和容量標準

*IOPS 分析*彈出視窗中的*分析工作負載*按鈕將帶您進入工作負載分析頁面，您可以在其中選擇時間範圍並查看所選工作負載的延遲、吞吐量和容量趨勢。有關工作負載分析器的更多信息，請參閱["使用工作負載分析器排除工作負載故障"](#)。

您可以透過點擊「效能視圖」列中的長條圖圖示來查看有關工作負載的效能信息，以協助進行故障排除。若要查看「工作負載分析」頁面上的效能和容量圖表來分析對象，請按一下「分析工作負載」按鈕。

有關詳細信息，請參閱 ["工作負載分析器顯示哪些數據"](#)。

為工作負載分配策略

您可以使用不同的導覽選項從「所有工作負載」頁面將儲存效率策略 (SEP) 和效能服務等級 (PSL) 指派給儲存工作負載。

將策略指派給單一工作負載

您可以為單一工作負載指派 PSL 或 SEP，或者兩者兼而有之。請依照以下步驟操作：

1. 選擇工作負載。
2. 點擊行旁邊的編輯圖標，然後點擊“編輯”。
- *指派的效能服務等級*和*儲存效率策略*欄位已啟用。
3. 選擇所需的 PSL 或 SEP，或兩者。

4. 按一下複選圖示以套用變更。



您也可以選擇一個工作負載並點擊“更多操作”來指派策略。

將策略指派給多個儲存工作負載

您可以將 PSL 或 SEP 一起指派給多個儲存工作負載。請依照以下步驟操作：

1. 選取要指派策略的工作負載的複選框，或選擇資料中心內的所有工作負載。
2. 按一下“更多操作”。
3. 若要指派 PSL，請選擇*指派效能服務等級*。若要指派 SEP，請選擇*指派儲存效率策略*。將顯示一個彈出視窗供您選擇策略。
4. 選擇適當的策略並點擊*應用*。顯示分配了策略的工作負載的數量。也列出了未分配策略的工作負載及其原因。



根據所選工作負載的數量，批量應用策略可能需要一些時間。您可以按一下「在背景執行」按鈕，並在操作在背景執行時繼續執行其他任務。當批次分配完成後，您可以查看完成狀態。如果您在多個工作負載上套用 PSL，則在批次分配的前一個作業執行時，您無法觸發另一個要求。

將系統建議的 PSL 分配給工作負載

您可以將系統建議的 PSL 指派給資料中心中尚未指派 PSL 或指派的 PSL 與系統建議不符的儲存工作負載。若要使用此功能，請按一下「指派系統建議的 PSL」按鈕。您不必選擇特定的工作負載。

該建議由系統分析內部確定，並且對於那些 IOPS 和其他參數與任何可用 PSL 的定義不一致的工作負載將被跳過。儲存工作負載 `Waiting for I/O` 學習狀態也被排除在外。



Unified Manager 會在工作負載名稱中尋找特殊關鍵字來覆寫系統分析並為工作負載建議不同的 PSL。當工作負載名稱中包含字母「ora」時，建議使用極限效能 PSL。當工作負載名稱中包含字母「vm」時，建議使用 **Performance** PSL。

另請參閱知識庫 (KB) 文章 ["ActiveIQ Unified Manager「分配系統建議的效能服務等級」不適應高度變化的工作負載"](#)

設定檔共享卷

您可以從「設定工作負載」頁面在現有叢集和儲存虛擬機器（儲存 VM）上建立支援 CIFS/SMB 和 NFS 協定的檔案共用磁碟區。

開始之前

- 儲存虛擬機器必須具有用於設定檔共用磁碟區的空間。
- 您的儲存虛擬機器上應啟用 SMB 和/或 NFS 服務。
- 為了在工作負載上選擇和分配效能服務等級 (PSL) 和儲存效率策略 (SEP)，必須在開始建立工作負載之前建立這些策略。

步驟

1. 在「Provision Workload」頁面上，新增要建立的工作負載的名稱，然後從可用清單中選擇叢集。
2. 根據您選擇的集群，**STORAGE VM** 欄位會過濾該集群可用的儲存 VM。從清單中選擇所需的儲存虛擬機器。

根據儲存虛擬機器上支援的 SMB 和 NFS 服務，在主機資訊部分啟用 NAS 選項。

3. 在儲存和最佳化部分，分配儲存容量和 PSL，也可以選擇為工作負載分配 SEP。

在建立工作負載時，SEP 的規格會指派給 LUN，而 PSL 的定義則會套用於工作負載。

4. 如果您想要強制執行已指派給工作負載的 PSL，請勾選「強制執行效能限制」複選框。

將 PSL 指派給工作負載可確保建立工作負載的聚合體能夠支援對應策略中定義的效能和容量目標。例如，如果為工作負載分配了「極限效能」PSL，則要配置工作負載的聚合體應該具有支援「極限效能」策略的效能和容量目標的能力，例如 SSD 儲存。



除非您選取此複選框，否則 PSL 不會套用於工作負載，且儀表板上的工作負載狀態將顯示為未指派。

5. 選擇 **NAS** 選項。

如果您看不到啟用的 **NAS** 選項，請驗證您選擇的儲存虛擬機器是否支援 SMB 或 NFS，或兩者。



如果您的儲存虛擬機器同時啟用了 SMB 和 NFS 服務，您可以選取 **透過 NFS 共用** 和 **透過 SMB 共用** 複選框，並建立同時支援 NFS 和 SMB 協定的檔案共用。如果要建立 SMB 或 CIFS 共享，請僅選取相應的核取方塊。

6. 對於 NFS 檔案共用卷，指定用於存取檔案共用磁碟區的主機或網路的 IP 位址。您可以為多個主機輸入逗號分隔的值。

新增主機 IP 位址時，將執行內部檢查以將主機詳細資訊與儲存 VM 匹配，並建立該主機的匯出策略，或者如果存在現有策略，則重新使用該策略。如果為相同主機建立了多個 NFS 共用，則具有符合規則的相同主機的可用匯出策略將對所有檔案共用重複使用。當您使用 API 設定 NFS 共用時，可以使用指定單一原則的規則或透過提供特定的策略金鑰來重複使用策略的功能。

7. 對於 SMB 共享，指定哪些使用者或使用者群組可以存取 SMB 共享並分配所需的權限。對於每個使用者群組，在檔案共用建立期間都會產生新的存取控制清單 (ACL)。

8. 點選“儲存”。

此工作負載已新增至儲存工作負載清單中。

配置 LUN

您可以從「設定工作負載」頁面在現有叢集和儲存虛擬機器（儲存 VM）上建立支援 CIFS/SMB 和 NFS 協定的 LUN。

開始之前

- 儲存虛擬機器必須具有用於設定 LUN 的空間。
- 在建立 LUN 的儲存 VM 上必須同時啟用 iSCSI 和 FCP。

- 為了在工作負載上選擇和分配效能服務等級 (PSL) 和儲存效率策略 (SEP)，必須在開始建立工作負載之前建立這些策略。

步驟

1. 在「Provision Workload」頁面上，新增要建立的工作負載的名稱，然後從可用清單中選擇叢集。

根據您選擇的集群，**STORAGE VM** 欄位會過濾該集群可用的儲存 VM。

2. 從清單中選擇支援 iSCSI 和 FCP 服務的儲存虛擬機器。

根據您的選擇，SAN 選項在主機資訊部分中啟用。

3. 在「儲存和最佳化」部分中，分配儲存容量和 PSL，以及可選的工作負載的 SEP。

在建立工作負載時，SEP 的規格會指派給 LUN，而 PSL 的定義則會套用於工作負載。

4. 如果您想要在工作負載上強制執行指派的 PSL，請勾選「強制執行效能限制」複選框。

將 PSL 指派給工作負載可確保建立工作負載的聚合體能夠支援對應策略中定義的效能和容量目標。例如，如果為工作負載分配了「極限效能」PSL，則要配置工作負載的聚合體應該具有支援「極限效能」策略的效能和容量目標的能力，例如 SSD 儲存。



除非您選取此複選框，否則 PSL 不會套用於工作負載，且工作負載的狀態在儀表板上顯示為 unassigned。

5. 選擇 **SAN** 選項。如果您看不到啟用的 **SAN** 選項，請驗證您選擇的儲存虛擬機器是否支援 iSCSI 和 FCP。
6. 選擇主機作業系統。
7. 指定主機對映以控制啟動器對 LUN 的存取。您可以指派現有的啟動器群組 (igroup)，或定義和對應新的 igroup。



如果在設定 LUN 時建立新的 igroup，則需要等到下一個發現週期（最多 15 分鐘）才能使用它。因此，建議您使用可用 igroup 清單中的現有 igroup。

如果要建立新的 igroup，請選擇「建立新的啟動器群組」按鈕，然後輸入該 igroup 的資訊。

8. 點選“儲存”。

LUN 已新增至儲存工作負載清單中。

性能服務水平

效能服務等級 (PSL) 可讓您定義工作負載的效能和儲存目標。您可以在最初建立工作負載時將 PSL 指派給工作負載，也可以在之後透過編輯工作負載來指派 PSL。

儲存資源的管理和監控基於服務等級目標 (SLO)。SLO 由基於所需效能和容量的服務等級協定定義。在 Unified Manager 中，SLO 是指在 NetApp 儲存體上執行的應用程式的 PSL 定義。儲存服務根據底層資源的效能和利用率進行區分。PSL 是對儲存服務目標的描述。PSL 使儲存提供者能夠指定工作負載的效能和容量目標。當您在工作負載上指派 PSL 時，ONTAP 上的對應工作負載將由其效能和容量目標進行管理。每個 PSL 都受峰值、預期和絕對最小 IOP 以及預期延遲的控制。

Unified Manager 具有以下類型的 PSL：

- 系統定義：Unified Manager 提供了一些無法變更的固定策略。這些預定義的 PSL 是：
 - 極致性能
 - 表現
 - 價值

極限效能、效能和價值 PSL 適用於資料中心中的大多數常見儲存工作負載。

Unified Manager 也為資料庫應用程式提供三種效能服務等級。這些是支援突發 IOPS 的極高效能 PSL，適用於具有最高吞吐量需求的資料庫應用程式。

- 資料庫日誌的極致
- 資料庫共享資料的極致
- 資料庫資料的極致
- 使用者定義：如果預先定義的效能服務等級無法滿足您的要求，那麼您可以建立新的 PSL 來滿足您的需求。有關信息，請參閱["建立和編輯效能服務級別"](#)。
- 超越極限：超越極限 PSL 是系統建議的 PSL，建議用於需要高於極限的 IOP 的工作負載。根據工作負載的 IOPS、容量和延遲進行內部分析，並在「儲存」>「工作負載」>「所有工作負載」畫面上為每個工作負載推薦一個 Beyond Extreme PSL。您可以將 PSL 應用於工作負載以確保最佳效能。

工作負載的 IOP 參數是根據工作負載行為動態產生的，並以以下格式附加到 Beyond Extreme PSL 的名稱中 `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`。例如，如果系統確定工作負載的峰值和預期 IOP 為 106345 和 37929 分別為工作負載產生的 Beyond Extreme PSL 命名為 `\Beyond Extreme 106345 37929`。雖然這些 PSL 是系統建議的，但當您將它們指派給工作負載時，這些 PSL 會被標記為 `\User-defined` 在類型中。

透過分配 PSL 來管理工作負載

您可以從「策略」>「效能服務等級」頁面存取 PSL，也可以使用儲存提供者 API 存取。透過為儲存工作負載指派 PSL 來管理儲存工作負載非常方便，因為您不必單獨管理儲存工作負載。任何修改也可以透過重新分配另一個 PSL 來管理，而不是單獨管理它們。Unified Manager 可協助您根據內部評估和建議為工作負載指派 PSL。

有關將系統建議的 PSL 指派給工作負載的信息，請參閱["將系統建議的 PSL 分配給工作負載"](#)

效能服務等級頁面列出了可用的 PSL 策略，並允許您新增、編輯和刪除它們。



您不能修改系統定義或目前指派給工作負載的 PSL。您無法刪除已指派給工作負載的 PSL，或它是唯一可用的 PSL。

此頁面顯示以下資訊：

場地	描述
Name	PSL 的名稱。

場地	描述
類型	該策略是系統定義的還是使用者定義的。
預期 IOPS/TB	應用程式預計在 LUN 或檔案共用上執行的最小 IOPS 數。預期 IOPS 根據分配的儲存物件大小指定分配的最小預期 IOPS。
峰值 IOPS/TB	<p>應用程式在 LUN 或檔案共用上可以執行的最大 IOPS 數。峰值 IOPS 根據分配的儲存物件大小或使用的儲存物件大小指定可能分配的最大 IOPS。</p> <p>峰值 IOPS 基於分配策略。分配策略是已分配空間或已使用空間。當分配策略設定為allocated-space時，峰值IOPS是根據儲存物件的大小來計算的。當分配策略設定為已使用空間時，峰值 IOPS 是根據儲存物件中儲存的資料量計算的，同時考慮儲存效率。預設情況下，分配策略設定為已使用空間。</p>
絕對最小 IOPS	<p>當預期 IOPS 小於此值時，絕對最小 IOPS 將用作覆蓋。系統定義的PSL的預設值如下：</p> <ul style="list-style-type: none"> • 極限表現：如果預期 IOPS \geq 6144/TB，則絕對最小 IOPS = 1000 • 效能：如果預期 IOPS \geq 2048/TB 且 $<$ 6144/TB，則絕對最小 IOPS = 500 • 值：如果預期 IOPS \geq 128/TB 且 $<$ 2048/TB，則絕對最小 IOPS = 75 <p>系統定義的資料庫 PSL 的預設值如下：</p> <ul style="list-style-type: none"> • 資料庫日誌的極限：如果預期 IOPS \geq 22528，則絕對最小 IOPS = 4000 • 資料庫共享資料的極限：如果預期 IOPS \geq 16384，則絕對最小 IOPS = 2000 • 資料庫資料的極端情況：如果預期 IOPS \geq 12288，則絕對最小 IOPS = 2000 <p>自訂 PSL 的絕對最小 IOPS 的較高值最大可以為 75000。較低值的計算方法如下：</p> <p>1000/預期延遲</p>
預期延遲	儲存 IOPS 的預期延遲（以每次操作的毫秒數 (ms/op) 為單位）。
容量	叢集中可用和已使用的總容量。

場地	描述
工作負載	已分配 PSL 的儲存工作負載的數量。

有關峰值 IOPS 和預期 IOPS 如何幫助在 ONTAP 叢集上實現一致的差異化效能的信息，請參閱以下知識庫文章：https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["什麼是績效預算?"]

因工作負載超出 **PSL** 定義的閾值而產生的事件

請注意，如果工作負載在前一小時內有 30% 的時間超過預期延遲值，Unified Manager 將產生以下事件之一來通知您潛在的效能問題：

- 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
- 工作負載 LUN 延遲閾值已超出效能服務等級策略所定義的範圍。

您可能需要分析工作負載以查看導致較高延遲值的原因。

有關詳細信息，請參閱以下連結：

- ["成交量事件"](#)
- ["當違反績效閾值策略時會發生什麼"](#)
- ["Unified Manager 如何使用工作負載延遲來識別效能問題"](#)
- ["什麼是表演活動"](#)

系統定義的 **PSL**

下表提供了有關係統定義的 PSL 的資訊：

性能服務水平	描述和用例	預期延遲 (毫秒/操作)	峰值 IOPS	預期 IOPS	絕對最小 IOPS
極致性能	以極低的延遲提供極高的吞吐量 非常適合延遲敏感的應用程式	1	12288	6144	1000
表現	以低延遲提供高吞吐量 非常適合資料庫和虛擬化應用程式	2	4096	2048	500

性能服務水平	描述和用例	預期延遲 (毫秒/操作)	峰值 IOPS	預期 IOPS	絕對最小 IOPS
價值	<p>提供高儲存容量和適度延遲</p> <p>非常適合電子郵件、Web 內容、文件共享和備份目標等大容量應用程式</p>	17	512	128	75
資料庫日誌的極致	<p>以最低的延遲提供最大的吞吐量。</p> <p>非常適合支援資料庫日誌的資料庫應用程式。由於資料庫日誌極為突發且對日誌記錄的需求不斷增加，因此此 PSL 可提供最高的吞吐量。</p>	1	45056	22528	4000
資料庫共享資料的極致	<p>以最低的延遲提供非常高的吞吐量。</p> <p>非常適合儲存在公共資料儲存中但跨資料庫共享的資料庫應用程式資料。</p>	1	32768	16384	2000
資料庫資料的極致	<p>以最低的延遲提供高吞吐量。</p> <p>非常適合資料庫應用程式數據，例如資料庫表格資訊和元數據。</p>	1	24576	12288	2000

建立和編輯效能服務級別

當系統定義的效能服務等級與您的工作負載要求不符時，您可以建立針對您的工作負載進行最佳化的效能服務等級。

開始之前

- 您必須具有應用程式管理員角色。

- 效能服務等級名稱必須是唯一的，且不能使用以下保留關鍵字：

Prime , Extreme , Performance , Value , Unassigned , Learning , Idle , Default , 和 None 。

您可以從「效能服務等級」頁面建立和編輯自訂效能服務級別，方法是定義存取儲存空間的應用程式所需的服務等級目標。



如果效能服務等級目前已指派給工作負載，則您無法修改它。

步驟

1. 在左側導覽窗格的「設定」下，選擇「策略」>「效能服務等級」。
2. 在「效能服務級別」頁面中，根據您是要建立新的效能服務級別還是要編輯現有的效能服務級別，按一下對應的按鈕。

到...	請依照以下步驟操作...
建立新的效能服務級別	按一下“新增”。
編輯現有的效能服務級別	選擇現有的效能服務級別，然後按一下「編輯」。

顯示新增或編輯效能服務等級的頁面。

3. 透過指定效能目標來自訂效能服務級別，然後按一下*提交*以儲存效能服務等級。

您可以從「工作負載」頁面或在配置新的工作負載時將新的或變更的效能服務等級套用至工作負載（LUN、NFS 檔案共用、CIFS 共用）。

管理儲存效率策略

儲存效率策略 (SEP) 可讓您定義工作負載的儲存效率特性。您可以在最初建立工作負載時將 SEP 指派給工作負載，也可以在之後透過編輯工作負載來指派 SEP。

儲存效率包括使用精簡配置、重複資料刪除和資料壓縮等技術來提高儲存利用率並降低儲存成本。在創建 SEP 時，您可以單獨或一起使用這些節省空間的技術來實現最大的儲存效率。當您將策略與儲存工作負載關聯時，指定的策略設定就會指派給它們。Unified Manager 讓您能夠指派系統定義和使用者定義的 SEP，以最佳化資料中心的儲存資源。

Unified Manager 提供兩個系統定義的 SEP：高和低。這些 SEP 適用於資料中心中的大多數儲存工作負載，但是，如果系統定義的 SEP 無法滿足您的要求，您可以建立自己的策略。

您無法修改系統定義或目前指派給工作負載的 SEP。您無法刪除已指派給工作負載的 SEP，或它是唯一可用的 SEP。

儲存效率策略頁面列出了可用的 SEP，並允許您新增、編輯和刪除自訂 SEP。此頁面顯示以下資訊：

場地	描述
Name	SEP 的名稱。
類型	該策略是系統定義的還是使用者定義的。
太空儲備	該卷是精簡配置的還是厚配置的。
重複資料刪除	工作負載上是否啟用了重複資料刪除： <ul style="list-style-type: none"> • 內嵌：重複資料刪除在工作負載寫入時發生 • 背景：重複資料刪除發生在工作負載中 • 停用：工作負載上停用重複資料刪除
壓縮	工作負載是否啟用資料壓縮： <ul style="list-style-type: none"> • 內嵌：資料壓縮在工作負載寫入時進行 • 背景：資料壓縮發生在工作負載中 • 停用：工作負載上停用資料壓縮
工作負載	已分配 SEP 的儲存工作負載數量

建立自訂儲存效率策略的指南

如果現有的 SEP 不符合您的儲存工作負載的策略要求，您可以建立自訂 SEP。但是，建議您嘗試將系統定義的 SEP 用於儲存工作負載，並且僅在必要時建立自訂 SEP。

您可以在「所有工作負載」頁面和「磁碟區/運行狀況詳細資料」頁面中查看指派給工作負載的 SEP。您可以在儀表板上的容量面板和容量：所有叢集視圖中查看基於這些儲存效率的叢集級資料縮減率（不含 Snapshot 副本）。

建立和編輯儲存效率策略

當系統定義的儲存效率策略不符合您的工作負載要求時，您可以建立針對您的工作負載最佳化的儲存效率策略。

開始之前

- 您必須具有應用程式管理員角色。
- 儲存效率策略名稱必須是唯一的，且不能使用以下保留關鍵字：

High , Low , Unassigned , Learning , Idle , Default , 和 None 。

您可以從「儲存效率策略」頁面建立和編輯自訂儲存效率策略，方法是定義存取儲存空間的應用程式所需的儲存效率特性。



如果儲存效率策略目前已指派給工作負載，則您無法修改該策略。

步驟

1. 在左側導覽窗格的「設定」下，選擇「策略」>「儲存效率」。
2. 在「儲存效率策略」頁面中，根據您是要建立新的儲存效率策略還是要編輯現有的儲存效率策略，按一下對應的按鈕。

到...	請依照以下步驟操作...
建立新的儲存效率策略	點擊“新增”
編輯現有的儲存效率策略	選擇現有的儲存效率策略並點擊“編輯”

將顯示新增或編輯儲存效率策略的頁面。

3. 透過指定儲存效率特性來自訂儲存效率策略，然後按一下*提交*以儲存儲存效率策略。

您可以從「工作負載」頁面或在配置新的工作負載時將新的或變更的儲存效率策略套用至工作負載（LUN、NFS 檔案共用、CIFS 共用）。

管理和監控MetroCluster配置

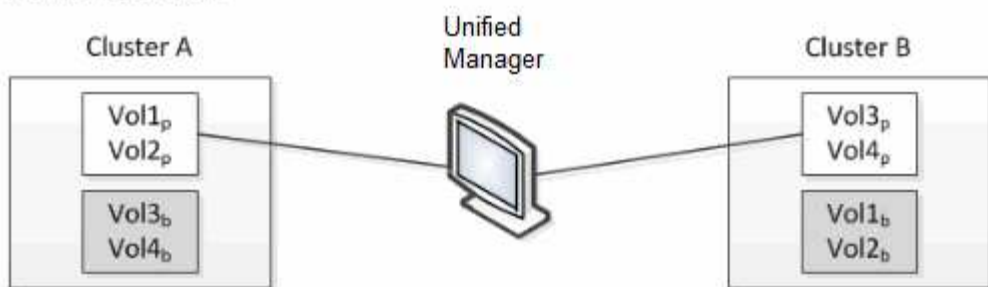
Unified Manager Web UI 中對MetroCluster配置的監控支援可讓您檢查MetroCluster透過FC和IP設定中的任何連線問題。儘早發現連線問題使您能夠有效地管理MetroCluster配置。

切換和切回期間的捲行為

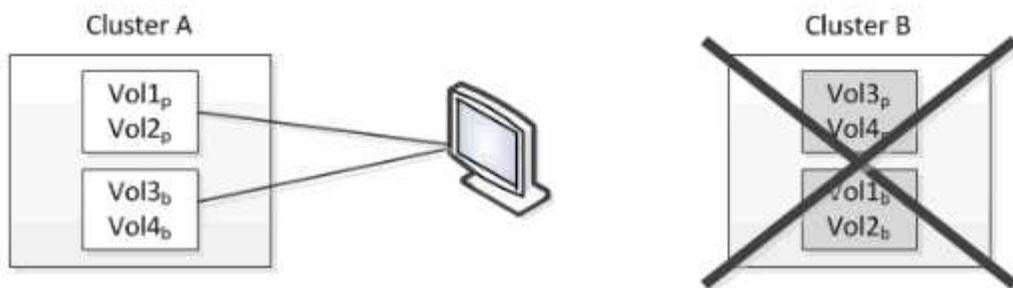
觸發切換或切回的事件會導致活動磁碟區從災難復原群組中的一個叢集移動到另一個叢集。叢集上處於活動狀態並向客戶端提供資料的磁碟區將停止，而另一個叢集上的磁碟區將啟動並開始提供資料。Unified Manager 僅監控處於活動狀態且正在執行的磁碟區。

由於磁碟區從一個集群移動到另一個集群，因此建議您監視兩個集群。Unified Manager 的單一實例可以監控MetroCluster配置中的兩個集群，但有時兩個位置之間的距離需要使用兩個 Unified Manager 實例來監控兩個集群。下圖顯示了 Unified Manager 的單一實例：

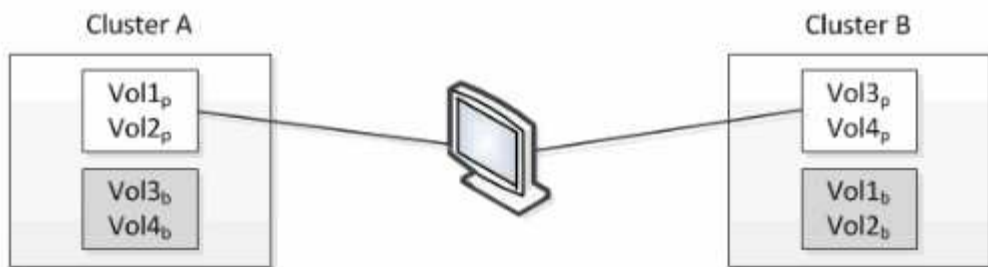
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



□ = active and monitored

■ = inactive and not monitored

名稱中帶有 p 的卷表示主磁碟區，名稱中帶有 b 的磁碟區表示由 SnapMirror 建立的鏡像備份磁碟區。

正常運作期間：

- 集群 A 有兩個活動卷：Vol1_p 和 Vol2_p。
- 集群 B 有兩個活動卷：Vol3_p 和 Vol4_p。
- 集群 A 有兩個非活動磁碟區：Vol3_b 和 Vol4_b。
- 集群 B 有兩個非活動磁碟區：Vol1_b 和 Vol2_b。

Unified Manager 收集與每個活動卷相關的資訊（統計資料、事件等）。Vol1_p 和 Vol2_p 統計資料由 Cluster A 收集，Vol3_p 和 Vol4_p 統計資料由 Cluster B 收集。

災難性故障導致活動卷從集群 B 切換到集群 A 後：

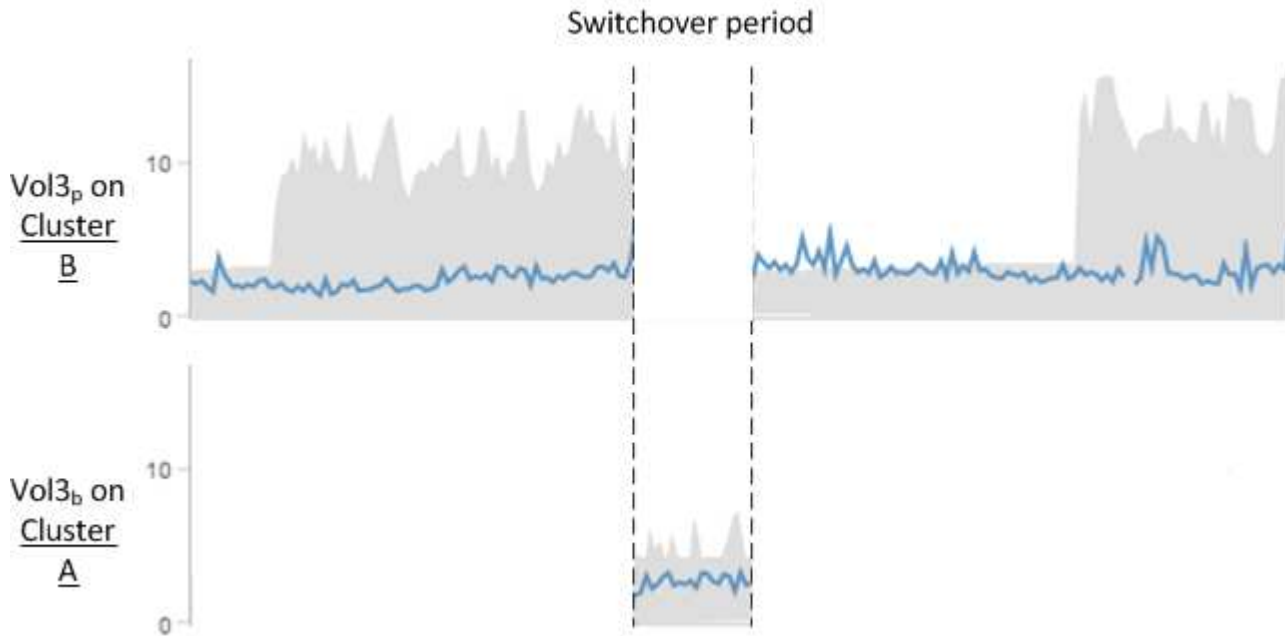
- 集群 A 有四個活動卷：Vol1_p、Vol2_p、Vol3_b 和 Vol4_b。
- 集群 B 有四個非活動卷：Vol3_p、Vol4_p、Vol1_b 和 Vol2_b。

與正常運作期間一樣，Unified Manager 會收集與每個活動磁碟區相關的資訊。但在這種情況下，Vol1p 和 Vol2p 統計資料由 Cluster A 收集，Vol3b 和 Vol4b 統計資料也由 Cluster A 收集。

請注意，Vol3p 和 Vol3b 不是相同的捲，因為它們位於不同的叢集上。Unified Manager 中有關 Vol3p 的資訊與 Vol3b 的資訊不同：

- 在切換到叢集 A 期間，Vol3p 統計資料和事件不可見。
- 在第一次切換時，Vol3b 看起來像一個沒有歷史資訊的新卷。

當叢集 B 修復並執行切換時，Vol3p 在叢集 B 上再次處於活動狀態，並具有歷史統計資料和切換期間的統計資料間隙。在發生另一次切換之前，無法從叢集 A 查看 Vol3b：



- 處於非活動狀態的MetroCluster磁碟區（例如，切換回叢集 A 上的 Vol3b）將顯示訊息「此磁碟區已被刪除」。該卷實際上並未被刪除，但由於它不是活動卷，因此目前未被 Unified Manager 監控。
- 如果單一 Unified Manager 正在監控MetroCluster配置中的兩個集群，則磁碟區搜尋將傳回當時處於活動狀態的磁碟區的資訊。例如，如果發生了切換並且 Vol3 在群集 A 上變為活動狀態，則搜尋「Vol3」將傳回群集 A 上 Vol3b 的統計資料和事件。

透過 FC 配置的MetroCluster的叢集連線狀態定義

透過 FC 配置的MetroCluster中的叢集之間的連接可以是以下狀態之一：最佳、受影響或關閉。了解連線狀態使您能夠有效地管理MetroCluster配置。

連線狀態	描述	顯示的圖示
最佳的	MetroCluster配置中的叢集之間的連線正常。	● ● ● ●

連線狀態	描述	顯示的圖示
受影響	一個或多個錯誤損害了故障轉移可用性的狀態；但是，MetroCluster配置中的兩個叢集仍然處於啟動狀態。例如，當 ISL 連結斷開時、當叢集間 IP 連結斷開時或當夥伴叢集無法存取時。	
向下	MetroCluster配置中的叢集之間的連線已斷開，因為其中一個或兩個叢集已關閉，或叢集處於故障轉移模式。例如，當合作夥伴叢集因災難而關閉或為了測試目的而計劃切換時。	<p>切換時出現錯誤：</p> <p>切換成功：</p>

MetroCluster over FC 的資料鏡像狀態定義

FC 配置上的MetroCluster提供資料鏡像以及在整個站點不可用時啟動故障轉移的附加功能。透過 FC 配置的MetroCluster中叢集之間的資料鏡像狀態可以是「正常」或「鏡像不可用」。了解狀態使您能夠有效地管理MetroCluster配置。

資料鏡像狀態	描述	顯示的圖示
普通的	MetroCluster配置中的叢集之間的資料鏡像正常。	
鏡像不可用	由於切換，MetroCluster配置中的叢集之間的資料鏡像不可用。例如，當合作夥伴叢集因災難而關閉或為了測試目的而計劃切換時。	<p>切換時出現錯誤：</p> <p>切換成功：</p>

監控MetroCluster配置

您可以監控MetroCluster配置中的連線問題。詳細資訊包括叢集內的組件和連接狀態以及MetroCluster配置中叢集之間的連接狀態。在這裡，您將了解如何監控由MetroCluster over FC 和MetroCluster over IP 配置保護的叢集中的連線問題。

您可以從Active IQ Unified Manager左側導覽窗格中的下列視圖監控MetroCluster配置：

- 儲存 > 叢集 > 保護： **MetroCluster** 視圖
- 保護 > 關係 > *關係： MetroCluster*視圖

Unified Manager 使用系統運作狀況警報來指示MetroCluster配置中的元件和連線的狀態。

開始之前

- MetroCluster配置中的本機叢集和遠端叢集都必須新增至Active IQ Unified Manager。
- 在MetroCluster over IP 配置中，如果要支援調解器，則應透過對應的 API 配置調解器並將其新增至叢集。
- 您必須具有操作員、應用程式管理員或儲存管理員角色。

透過 **FC** 設定監控**MetroCluster**中的連線問題

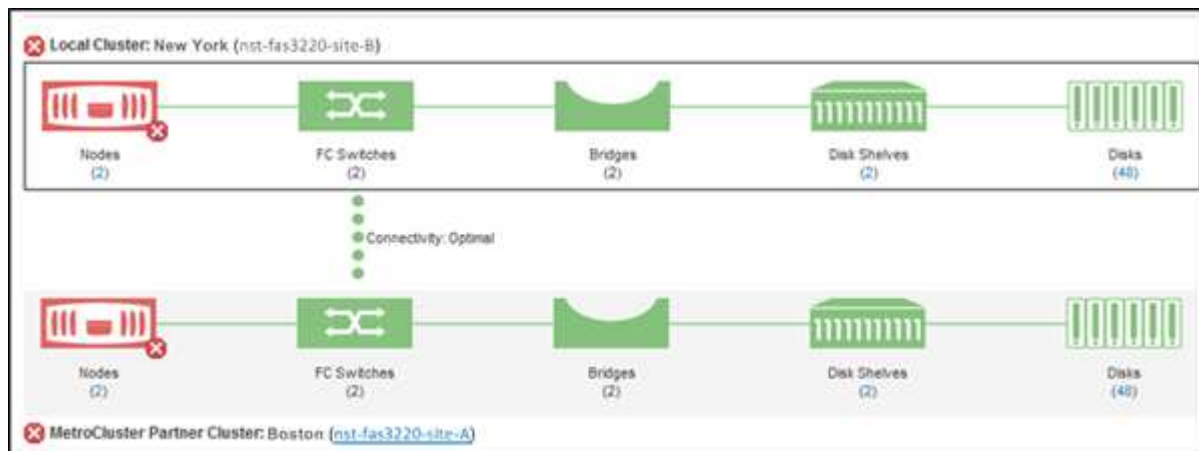
對於MetroCluster over FC 配置中的集群，連接圖表顯示在 集群/運行狀況 詳細資訊頁面上。請依照以下步驟操作。

步驟

1. 在左側導覽窗格中，按一下「儲存」 > 「叢集」。

顯示所有受監控集群的清單。

2. 從 **Protection: MetroCluster** 視圖中，按一下要查看MetroCluster over FC 配置詳細資訊的叢集的名稱。或者，您可以按MetroCluster配置中的叢集進行過濾。
3. 在「叢集/運作狀況」詳細資料頁面中，按一下「MetroCluster連線」標籤。「MetroCluster Connectivity」標籤僅適用於 FC 設定上的MetroCluster。



MetroCluster配置的拓樸顯示在對應的叢集物件區域中。您可以使用集群/健康詳情頁面中顯示的資訊來修正任何連線問題。例如，如果叢集中的節點和交換器之間的連線中斷，則會顯示下列圖示：



如果將指標移到圖示上，您可以查看有關產生的事件詳細資訊。

如果您發現MetroCluster配置中存在連線問題，則必須登入系統管理員或存取ONTAP CLI 來解決這些問題。

有關確定群集健康狀況的更多信息，請參閱["確定MetroCluster透過 FC 配置中的叢集運作狀況"](#)。

監控MetroCluster透過 IP 設定中的連線問題

對於MetroCluster over IP 配置中的叢集，連接圖表顯示在 叢集 頁面上。請依照以下步驟操作。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。

顯示所有受監控叢集的清單。

2. 從 **Protection: MetroClusters** 視圖中，按一下要查看MetroCluster over IP 設定詳細資訊的叢集的名稱。或者，您可以按MetroCluster配置中的叢集進行過濾。
3. 按一下插入符號展開行 `v` 圖示。只有當叢集受到MetroCluster over IP 配置保護時，才會顯示插入符號圖示。

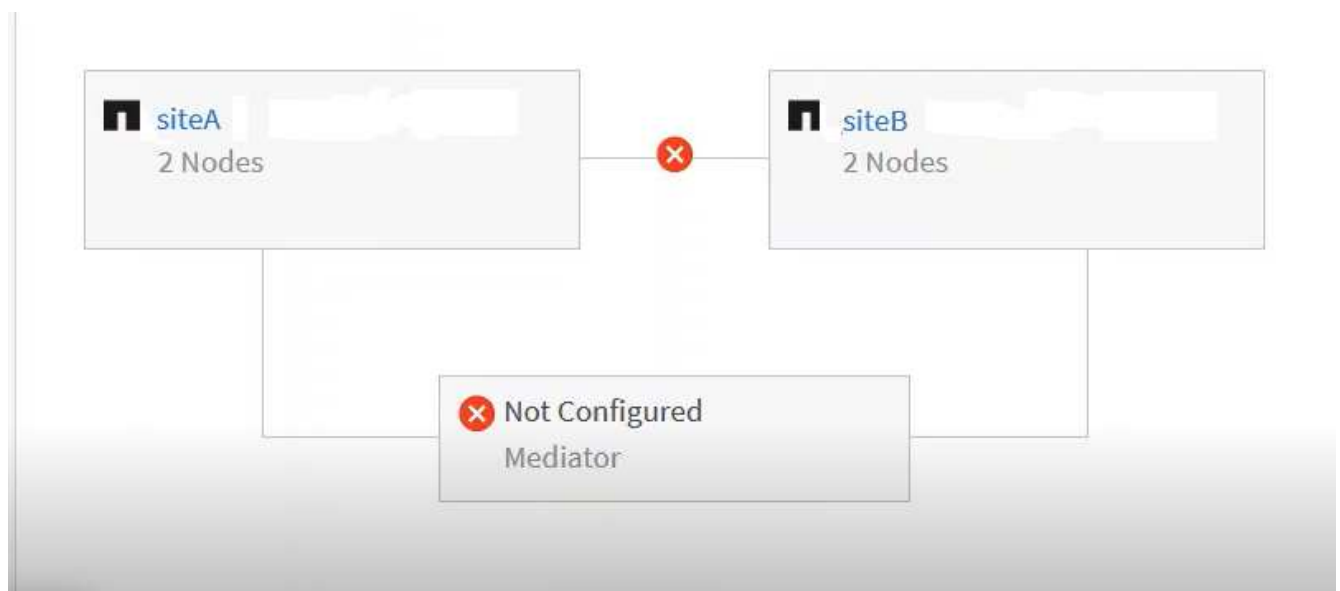
您可以查看來源網站和鏡像網站的拓撲結構，以及用於連接的中介器（如果有）。您可以查看以下資訊：

- 跨站點連接
- 兩個站點的健康和可用性問題（如果有）
- 調解員相關問題
- 複製相關問題。



報告以下狀態：嚴重 (❌)，錯誤 (⚠️) 或正常 (✅)。您也可以查看相同拓撲中主資料和鏡像資料的聚合資料複製狀態。

在下圖中，您可以看到來源叢集和目標叢集之間的站點間連線不可用，且它們之間的中介器未配置。



4. 單擊狀態圖示。顯示帶有錯誤定義的訊息。如果您的MetroCluster over IP 設定中出現了與該問題相關的事件，您可以點擊訊息上的「檢視事件」按鈕並查看事件詳細資料。解決問題和事件後，此拓撲中的狀態圖示將變為正常 (✔)。
5. 您可以在「叢集/運行狀況」詳細資料頁面的「配置」標籤上的「MetroCluster概覽」和「保護」部分中查看更多配置詳細資訊。



僅對於MetroCluster over IP 配置，您才可以在 **Clusters** 頁面上查看叢集拓撲。對於MetroCluster over FC 配置中的集群，拓撲顯示在「集群/運行狀況」詳細資訊頁面上的「MetroCluster連接」標籤上。

相關資訊

- ["集群/健康詳情頁面"](#)
- 有關關係：**MetroCluster** 視圖的信息，請參閱["監控MetroCluster配置"](#)。
- 有關*關係：過去 1 個月轉移狀態*視圖的信息，請參閱["關係：最近 1 個月的轉移狀態視圖"](#)。
- 有關*關係：過去 1 個月轉移率*視圖的信息，請參閱["關係：過去 1 個月的轉移率視圖"](#)。
- 有關"關係：所有關係"視圖的信息，請參閱["關係：所有關係視圖"](#)。

監控MetroCluster複製

您可以在鏡像資料的同時監控和診斷邏輯連接的整體健康狀況。您可以識別中斷叢集元件（例如聚合、節點和儲存虛擬機器）鏡像的問題或任何風險。

Unified Manager 使用系統運作狀況警報來監控MetroCluster配置中的元件和連線的狀態。

開始之前

MetroCluster配置中的本機和遠端叢集都必須新增至 Unified Manager

查看MetroCluster over IP 配置的複製

對於MetroCluster over IP 配置，資料複製狀態顯示在受MetroCluster over IP 保護的叢集的拓撲預覽視圖中，該視圖來自 Unified Manager 左側導覽窗格中的下列視圖：

- 儲存 > 叢集 > 保護：**MetroCluster** 視圖
- 保護 > 關係 > *關係：MetroCluster*視圖

有關信息，請參閱["監控MetroCluster over IP 中的連線問題"](#)。

查看MetroCluster透過 FC 配置的複製

請依照下列步驟確定MetroCluster透過 FC 配置的資料複製中的任何問題。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。

顯示受監控集群的清單。

2. 從「**Health: All Clusters**」檢視中，按一下要查看MetroCluster複製詳細資料的叢集的名稱。在「叢集/運作狀況詳細資料」頁面上，按一下「MetroCluster複製」標籤。

要複製的MetroCluster配置的拓撲顯示在本地站點的相應叢集物件區域中，以及有關正在鏡像資料的遠端站點的資訊。如果將指標移到圖示上，您可以查看有關所產生事件的詳細資訊。

您可以使用集群/健康詳情頁面中顯示的資訊來修正任何複製問題。如果您發現MetroCluster配置中存在鏡像問題，則必須登入系統管理員或存取ONTAP CLI 來解決這些問題。

相關資訊

["集群/健康詳情頁面"](#)

管理配額

您可以使用使用者和群組配額來限制使用者或使用者群組可以使用的磁碟空間量或檔案數量。您可以查看使用者和使用者群組配額信息，例如磁碟和檔案使用情況以及對磁碟設定的各種限制。

什麼是配額限制

使用者配額限制是 Unified Manager 伺服器用來評估使用者的空間消耗是否接近限制或已達到使用者配額設定的限制的值。如果超過軟體限制或達到硬限制，Unified Manager 伺服器將產生使用者配額事件。

預設情況下，Unified Manager 伺服器會向超過配額軟體限制或達到配額硬限制且配置了使用者配額事件的使用者發送通知電子郵件。具有應用程式管理員角色的使用者可以設定警報，以通知指定的接收者有關使用者或使用者群組配額事件的資訊。

您可以使用ONTAP系統管理員或ONTAP CLI 指定配額限制。

查看使用者和使用者群組配額

儲存虛擬機器/運作狀況詳細資訊頁面顯示有關在 SVM 上配置的使用者和使用者群組配額的資訊。您可以查看使用者或使用者群組的名稱、磁碟和檔案的限制設定、已使用的磁碟和檔案空間以及用於通知的電子郵件地址。

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「儲存」>「儲存虛擬機器」。
2. 在*Health: All Storage VMs*視圖中，選擇儲存虛擬機，然後按一下*User and Group Quotas*選項卡。

相關資訊

["新增用戶"](#)

建立規則以產生電子郵件地址

您可以建立規則，根據與叢集、儲存虛擬機器 (SVM)、磁碟區、qtree、使用者或使用者群組關聯的使用者配額來指定電子郵件地址。當配額超出時，會向指定的電子郵件地址發送通知。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已查看「產生使用者和群組配額電子郵件地址的規則」頁面上的指南。

您必須定義配額電子郵件地址的規則，並按照您想要執行的順序輸入它們。例如，如果您要使用電子郵件地址 abc@xyz.com 接收有關 abc 的配額違規通知，並使用電子郵件地址 `dl-$GROUP@$DOMAIN` 接收所有其他群組的配額違規通知，則必須按以下順序列出規則：

- 如果 (`$USER == 'abc'`) 則 abc@xyz.com
- 如果 (`$GROUP == *`) 則 `dl-$GROUP@$DOMAIN`

如果您指定的規則均不符合任何條件，則使用預設規則：

如果 (`$USER_OR_GROUP == *`) 則 `$USER_OR_GROUP@$DOMAIN`

步驟

1. 在左側導覽窗格中，按一下「常規」>「配額電子郵件規則」。
2. 根據您的標準輸入規則。
3. 按一下“驗證”以驗證規則的語法。

如果規則的語法不正確，則會顯示錯誤訊息。您必須更正語法並再次點擊“驗證”。

4. 點選“儲存”。
5. 驗證您建立的電子郵件地址是否顯示在儲存*VM/健康*詳細資料頁面的*使用者和群組配額*標籤中。

為使用者和使用者群組配額建立電子郵件通知格式

您可以建立通知格式，當出現與配額相關的問題（超出軟限制或達到硬限制）時，向使用者或使用者群組發送電子郵件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「配額電子郵件格式」。
2. 輸入或修改「寄件者」、「主題」和「電子郵件詳細資料」欄位中的詳細資料。
3. 按一下「預覽」即可預覽電子郵件通知。
4. 按一下「關閉」關閉預覽視窗。
5. 如有需要，修改電子郵件通知的內容。

6. 點選“儲存”。

編輯使用者和群組配額電子郵件地址

您可以根據與叢集、儲存虛擬機器 (SVM)、磁碟區、qtree、使用者或使用者群組關聯的使用者配額修改電子郵件地址。當您想要覆寫「產生使用者和群組配額電子郵件地址的規則」對話方塊中指定的規則所產生的電子郵件地址時，您可以修改電子郵件地址。

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。
- 您必須已經查看過“[建立規則的指南](#)”。

如果您編輯電子郵件地址，則產生使用者和群組配額電子郵件地址的規則將不再適用於該配額。若要將通知傳送至指定規則產生的電子郵件地址，您必須刪除該電子郵件地址並儲存變更。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「SVM」。
2. 在 **Health: All Storage VMs** 視圖中，選擇一個 SVM，然後按一下 **User and Group Quotas** 選項卡。
3. 點擊選項卡行下方的“編輯電子郵件地址”。
4. 在「編輯電子郵件地址」對話方塊中，執行對應的操作：

如果...	然後...
您希望將通知傳送到指定規則產生的電子郵件地址	<ol style="list-style-type: none"> a. 刪除「電子郵件地址」欄位中的電子郵件地址。 b. 點選“儲存”。 c. 按 F5 重新整理瀏覽器以重新載入「編輯電子郵件地址」對話方塊。指定規則產生的電子郵件地址顯示在「電子郵件地址」欄位中。
您希望將通知傳送到指定的電子郵件地址	<ol style="list-style-type: none"> a. 在*電子郵件地址*欄位中修改電子郵件地址。 b. 點選“儲存”。產生使用者和群組配額電子郵件地址的規則不再適用於配額。

詳細了解配額

了解有關配額的概念有助於您有效地管理使用者配額和使用者群組配額。

配額流程概述

配額可以是軟的，也可以是硬的。當超出指定限制時，軟配額會導致ONTAP發送通知，而當超出指定限制時，硬配額會阻止寫入作業成功。

當ONTAP收到使用者或使用者群組向FlexVol volume寫入的請求時，它會檢查該磁碟區上是否為該使用者或使用者群組啟動了配額，並確定以下內容：

- 是否會達到硬限制

如果是，則達到硬限制時寫入操作失敗，並發送硬配額通知。

- 軟限制是否會被突破

如果是，則當超出軟限制時寫入操作成功，並發送軟配額通知。

- 寫入操作是否不會超出軟限制

如果是，則寫入操作成功，不發送通知。

關於配額

配額提供了一種限制或追蹤使用者、群組或 qtree 使用的磁碟空間和檔案數量的方法。您可以使用 `/etc/quotas` 文件。配額適用於特定卷或 qtree。

為什麼要使用配額

您可以使用配額來限制 FlexVol 磁碟區中的資源使用情況，在資源使用達到特定水準時提供通知，或追蹤資源使用情況。

您指定配額的原因如下：

- 限制使用者或群組可以使用的磁碟空間量或檔案數量，或限制 qtree 可以包含的磁碟空間量或檔案數量
- 追蹤使用者、群組或 qtree 使用的磁碟空間量或檔案數量，而不施加限制
- 當使用者的磁碟使用率或檔案使用率過高時發出警告

配額對話框的說明

您可以使用「健康狀況：所有儲存虛擬機器」檢視中「使用者和群組配額」標籤中的對應選項來配置發生配額相關問題時發送的電子郵件通知的格式，並配置規則以根據使用者配額指定電子郵件地址。

電子郵件通知格式頁面

電子郵件通知格式頁面顯示當出現與配額相關的問題（超出軟限制或達到硬限制）時發送給使用者或使用者群組的電子郵件的規則。

只有在產生以下使用者或使用者群組配額事件時才會發送電子郵件通知：超出使用者或群組配額磁碟空間軟限制、超出使用者或群組配額檔案計數軟限制、達到使用者或群組配額磁碟空間硬限制或達到使用者或群組配額檔案計數硬限制。

- 從

顯示發送電子郵件的電子郵件地址，您可以修改該地址。預設情況下，這是通知頁面指定的電子郵件地址。

- 主題

顯示通知電子郵件的主題。

- 電子郵件詳細資訊

顯示通知電子郵件的文字。您可以根據您的要求修改文字。例如，您可以提供與配額屬性相關的資訊並減少關鍵字數量。但是，您不應該修改關鍵字。

有效關鍵字如下：

- \$事件名稱

指定導致電子郵件通知的事件名稱。

- \$QUOTA_TARGET

指定配額適用的 qtree 或卷。

- \$QUOTA_USED_PERCENT

指定使用者或使用者群組使用的磁碟硬限制、磁碟軟限制、檔案硬限制或檔案軟限制的百分比。

- \$QUOTA_LIMIT

指定使用者或使用者群組達到的磁碟硬限制或檔案硬限制，並產生以下事件之一：

- 已達到使用者或群組配額磁碟空間硬限制
- 已達到使用者或群組配額磁碟空間軟限制
- 已達到使用者或群組配額檔案數硬限制
- 已達到使用者或群組配額檔案計數軟限制

- \$QUOTA_USED

指定使用者或使用者群組使用的磁碟空間或建立的檔案數。

- \$QUOTA_USER

指定使用者或使用者群組的名稱。

命令按鈕

命令按鈕可讓您預覽、儲存或取消電子郵件通知格式所做的變更：

- 預覽

顯示通知電子郵件的預覽。

- 恢復出廠預設值

使您能夠將通知格式恢復為原廠預設值。

- 節省

儲存通知格式所做的變更。

產生使用者和群組配額電子郵件地址的規則頁面

透過「產生使用者和群組配額電子郵件地址的規則」頁面，您可以建立規則，以根據與叢集、SVM、磁碟區、qtree、使用者或使用者群組關聯的使用者配額指定電子郵件地址。當超出配額時，會向指定的電子郵件地址發送通知。

規則區域

您必須定義配額電子郵件地址的規則。您也可以新增評論來解釋規則。

如何定義規則

您必須按照要執行的順序輸入規則。如果符合第一條規則的標準，則根據該規則產生電子郵件地址。如果不符合該標準，則考慮下一個規則的標準，依此類推。每行列出一條單獨的規則。預設規則是清單中的最後一條規則。您可以更改規則的優先順序。但是，您不能更改預設規則的順序。

例如，如果您要使用電子郵件地址 `qtree1@xyz.com` 接收有關 `qtree1` 配額違規的通知，並使用電子郵件地址 `admin@xyz.com` 接收所有其他 `qtree` 的配額違規通知，則必須按以下順序列出規則：

- 如果 (`$QTREE == 'qtree1'`) 則 `qtree1@xyz.com`
- 如果 (`$QTREE == *`) 則 `admin@xyz.com`

如果您指定的規則均不符合任何條件，則使用預設規則：

如果 (`$USER_OR_GROUP == *`) 則 `$USER_OR_GROUP@$DOMAIN`

如果多個使用者俱有相同的配額，則使用者的名稱將顯示為逗號分隔的值，且規則不適用於該配額。

如何添加評論

您可以新增評論來解釋規則。您應該在每個註解的開頭使用`#`，並且每行列出一個單獨的註解。

規則語法

規則的語法必須是下列之一：

- 如果 (`valid variableoperator *`) 然後 `email ID@domain name`

`if` 是關鍵字且是小寫的。運算符是 `==`。電子郵件 ID 可以包含任意字元、有效變數 `$USER_OR_GROUP`、`$USER` 或 `$GROUP`，或任意字元和有效變數 `$USER_OR_GROUP`、`$USER` 或 `$GROUP` 的組合。網域可以包含任意字元、有效變數 `$DOMAIN` 或任意字元和有效變數 `$DOMAIN` 的組合。有效變數可以是大寫或小寫，但不能是兩者的組合。例如，`$domain` 和 `$DOMAIN` 是有效的，但 `$Domain` 不是有效變數。

- 如果 (`valid variableoperator `string``) 然後 `email ID@domain name`

`if` 是關鍵字且是小寫的。運算符可以是 `contains` 或 `==`。電子郵件 ID 可以包含任意字元、有效變數 `$USER_OR_GROUP`、`$USER` 或 `$GROUP`，或任意字元和有效變數 `$USER_OR_GROUP`、`$USER` 或 `$GROUP` 的組合。網域可以包含任意字元、有效變數 `$DOMAIN` 或任意字元和有效變數 `$DOMAIN` 的組合。有效變數可以是大寫或小寫，但不能是兩者的組合。例如，`$domain` 和 `$DOMAIN` 是有效的，但

\$Domain 不是有效變數。

命令按鈕

命令按鈕可讓您儲存、驗證或取消已建立的規則：

- 證實

驗證所建立規則的語法。如果驗證期間出現錯誤，則會顯示產生錯誤的規則以及錯誤訊息。

- 恢復出廠預設值

使您能夠將位址規則恢復為出廠預設值。

- 節省

驗證規則的語法，如果沒有錯誤則儲存規則。如果驗證期間出現錯誤，則會顯示產生錯誤的規則以及錯誤訊息。

故障排除

故障排除資訊可協助您識別和解決使用 Unified Manager 時遇到的問題。

向 Unified Manager 資料庫目錄新增磁碟空間

Unified Manager 資料庫目錄包含從ONTAP系統收集的所有健康和效能資料。某些情況下可能需要您增加資料庫目錄的大小。

例如，如果 Unified Manager 從大量叢集（每個叢集都有許多節點）收集數據，則資料庫目錄可能會已滿。當資料庫目錄已滿 90% 時，您將收到警告事件；當資料庫目錄已滿 95% 時，您將收到嚴重事件。



當目錄達到 95% 滿度後，將不再從群集收集其他資料。

根據 Unified Manager 是在 VMware ESXi 伺服器、Red Hat Linux 伺服器或 Microsoft Windows 伺服器上執行，為資料目錄新增容量所需的步驟會有所不同。

為VMware虛擬機器資料盤新增空間

如果需要增加 Unified Manager 資料庫的資料磁碟空間量，則可以在安裝後使用 Unified Manager 維護控制台增加磁碟空間來增加容量。

開始之前

- 您必須具有 vSphere Client 的存取權限。
- 虛擬機器一定不能本地儲存的快照。
- 您必須擁有維護使用者憑證。

我們建議您在增加虛擬磁碟的大小之前備份虛擬機器。

步驟

1. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後在資料中新增更多磁碟容量 disk 3。有關詳細信息，請參閱 VMware 文件。

在極少數情況下，Unified Manager 部署使用「硬碟 2」而不是「硬碟 3」作為資料磁碟。如果您的部署中出現這種情況，請增加較大磁碟的空間。資料磁碟的空間總是比其他磁碟大。

2. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後選擇「控制台」標籤。
3. 按一下控制台窗口，然後使用您的使用者名稱和密碼登入維護控制台。
4. 在*主選單*中，輸入*系統配置*選項的編號。
5. 在*系統設定選單*中，輸入*增加資料磁碟大小*選項的數字。

為Linux主機的資料目錄新增空間

如果您分配的磁碟空間不足 `/opt/netapp/data` 目錄以支援 Unified Manager，當您最初設定 Linux 主機然後安裝 Unified Manager 時，您可以在安裝後透過增加 `/opt/netapp/data` 目錄。

開始之前

您必須具有安裝了 Unified Manager 的 Red Hat Enterprise Linux 機器的 root 使用者存取權。

我們建議您在增加資料目錄的大小之前備份 Unified Manager 資料庫。

步驟

1. 以 root 使用者身分登入要新增磁碟空間的 Linux 機器。
2. 以所示順序停止 Unified Manager 服務和相關的 MySQL 軟體：`systemctl stop ocieau ocie mysqld`
3. 建立臨時備份資料夾（例如，`/backup-data`）具有足夠的磁碟空間來包含當前 `/opt/netapp/data` 目錄。
4. 複製現有 `/opt/netapp/data` 目錄到備份資料目錄：

```
cp -arp /opt/netapp/data/* /backup-data
```

5. 如果啟用了 SE Linux：
 - a. 取得現有資料夾的 SE Linux 類型 `/opt/netapp/data` 資料夾：

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

系統傳回類似如下的確認訊息：

```
echo $se_type
mysqld_db_t
```

- a. 運行 `chcon` 指令設定備份目錄的 SE Linux 類型：


```
chcon -R --type=mysqlld_db_t /backup-data
```

6. 刪除 `/opt/netapp/data` 目錄：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. 擴大規模 `/opt/netapp/data` 透過 LVM 指令或新增額外的磁碟將目錄大小增加到至少 150 GB。



如果您已經創建 `/opt/netapp/data` 從磁碟，那麼您不應該嘗試安裝 `/opt/netapp/data` 作為 NFS 或 CIFS 共享。因為在這種情況下，如果您嘗試擴展磁碟空間，則一些 LVM 命令，例如 `resize` 和 `extend` 可能無法如預期工作。

8. 確認 `/opt/netapp/data` 目錄擁有者 (mysql) 和群組 (root) 保持不變：

```
ls -ltr /opt/netapp/ | grep data
```

系統傳回類似如下的確認訊息：

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. 如果啟用了 SE Linux，請確認 `/opt/netapp/data` 目錄仍然設定為 `mysqlld_db_t`：

- a. `touch /opt/netapp/data/abc`
- b. `ls -Z /opt/netapp/data/abc`

系統傳回類似如下的確認訊息：

```
-rw-r--r--. root root unconfined_u:object_r:mysqlld_db_t:s0  
/opt/netapp/data/abc
```

10. 刪除文件 `abc` 這樣這個多餘的檔案就不會在將來導致資料庫錯誤。

11. 複製內容 `backup-data` 回到擴展 `/opt/netapp/data` 目錄：

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. 如果啟用了 SE Linux，請執行以下命令：

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. 啟動 MySQL 服務：

```
systemctl start mysqld
```

14. MySQL 服務啟動後，依照所示順序啟動 `ocie` 和 `ocieau` 服務：

```
systemctl start ocie ocieau
```

15. 所有服務啟動後，刪除備份資料夾 /backup-data：

```
rm -rf /backup-data
```

為 Microsoft Windows 伺服器的邏輯磁碟機新增空間

如果需要增加 Unified Manager 資料庫的磁碟空間量，您可以為安裝 Unified Manager 的邏輯磁碟機新增容量。

開始之前

您必須具有 Windows 管理員權限。

我們建議您在新增磁碟空間之前備份 Unified Manager 資料庫。

步驟

1. 以管理員身分登入要新增磁碟空間的 Windows 伺服器。
2. 按照與您想要使用的方法相對應的步驟來增加更多空間：

選項	描述
在實體伺服器上，為安裝 Unified Manager 伺服器的邏輯磁碟機新增容量。	請依照 Microsoft 主題中的步驟操作： "擴充基本捲"
在實體伺服器上，新增硬碟。	請依照 Microsoft 主題中的步驟操作： "新增硬碟驅動器"
在虛擬機器上，增加磁碟分割的大小。	請按照 VMware 主題中的步驟操作： "增加磁碟分割區的大小"

修改效能統計收集間隔

效能統計資訊的預設收集間隔為5分鐘。如果您發現大型叢集的收集未在預設時間內完成，則可以將此間隔變更為 10 或 15 分鐘。此設定會影響此 Unified Manager 實例所監控的所有叢集的統計資訊收集。

開始之前

您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。

橫幅訊息指出了效能統計資料收集未按時完成的問題 `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>`.

僅當因統計資訊收集問題而需要時才應變更收集間隔。請勿因任何其他原因更改此設定。



將此值從預設設定 5 分鐘變更為其他值可能會影響 Unified Manager 報告的效能事件的數量和頻率。例如，當超過策略 30 分鐘時，系統定義的效能閾值會觸發事件。當使用 5 分鐘收集時，必須超過該政策連續六次收集。對於 15 分鐘的收集，政策必須僅超出兩個收集期。

叢集設定頁面底部的訊息指示目前統計資料收集間隔。

步驟

1. 使用 SSH 以維護使用者身分登入 Unified Manager 主機。

將顯示 Unified Manager 維護控制台提示。

2. 鍵入標示為「效能輪詢間隔配置」的選單選項的編號，然後按 Enter。
3. 如果出現提示，請再次輸入維護使用者密碼。
4. 鍵入要設定的新輪詢間隔的數字，然後按 Enter。

如果您將 Unified Manager 收集間隔變更為 10 或 15 分鐘，且您目前已連線至外部資料提供者（例如 Graphite），則必須變更資料提供者傳輸間隔，使其等於或大於 Unified Manager 收集間隔。

更改 Unified Manager 保留事件和效能資料的時間長度

預設情況下，Unified Manager 會為所有受監控的叢集儲存 6 個月的事件資料和效能資料。此後，舊資料將自動刪除，為新資料騰出空間。此預設時間範圍適用於大多數配置，但具有許多叢集和節點的超大型配置可能需要減少保留期，以便 Unified Manager 以最佳方式運作。

開始之前

您必須具有應用程式管理員角色。

您可以在資料保留頁面中變更這兩類資料的保留期限。這些設定會影響此 Unified Manager 實例所監控的所有叢集的資料保留。



Unified Manager 每 5 分鐘收集一次效能統計資料。每天將 5 分鐘的統計資料匯總為每小時的效能統計資料。它保留 30 天的 5 分鐘歷史性能數據和 6 個月的每小時匯總性能數據（預設）。

只有當空間不足或備份和其他作業需要很長時間才能完成時，才應減少保留期。縮短保留期有以下影響：

- 午夜後，舊的效能資料將從 Unified Manager 資料庫中刪除。
- 舊事件資料將立即從 Unified Manager 資料庫中刪除。
- 保留期之前的事件將無法再在使用者介面中查看。
- 在保留期之前，UI 中顯示每小時效能統計資料的位置將為空白。
- 如果事件保留期超過效能資料保留期，效能滑桿下方將顯示一則訊息，警告較舊的效能事件可能在其關聯圖表中沒有支援資料。

步驟

1. 在左側導覽窗格中，按一下「策略」>「資料保留」。
2. 在*資料保留*頁面中，選擇事件保留或效能資料保留區域中的滑桿工具並將其移至應保留資料的月份數，然

後按一下*儲存*。

未知的身份驗證錯誤

當您執行與驗證相關的操作（例如新增、編輯、刪除或測試遠端使用者或群組）時，可能會顯示下列錯誤訊息：Unknown authentication error.

原因

如果您為以下選項設定了不正確的值，則可能會出現此問題：

- Active Directory 驗證服務的管理員名稱
- 綁定 OpenLDAP 驗證服務的可分辨名稱

糾正措施

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 根據您選擇的身份驗證服務，輸入管理員名稱或綁定可分辨名稱的相應資訊。
3. 按一下「測試身份驗證」以使用您指定的詳細資料測試身份驗證。
4. 點選“儲存”。

未找到用戶

當您執行與驗證相關的操作（例如新增、編輯、刪除或測試遠端使用者或群組）時，會顯示下列錯誤訊息：User not found.

原因

如果使用者存在於 AD 伺服器或 LDAP 伺服器中，並且您將基本可分辨名稱設為不正確的值，則可能會發生此問題。

糾正措施

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 輸入基本可分辨名稱的適當資訊。
3. 點選“儲存”。

使用其他驗證服務新增 LDAP 的問題

當您選擇其他作為驗證服務時，使用者和群組物件類別將保留先前選取的範本中的值。如果 LDAP 伺服器不使用相同的值，操作可能會失敗。

原因

OpenLDAP 中的使用者設定不正確。

糾正措施

您可以使用以下解決方法之一手動修復此問題。

如果您的 LDAP 使用者物件類別和群組物件類別分別是使用者和群組，請執行下列步驟：

1. 在左側導覽窗格中，按一下常規 > 遠端驗證。
2. 在*驗證服務*下拉選單中，選擇*Active Directory*，然後選擇*其他*。
3. 完成文字欄位。

如果您的 LDAP 使用者物件類別和群組物件類別分別是 posixAccount 和 posixGroup，請執行下列步驟：

1. 在左側導覽窗格中，按一下常規 > 遠端驗證。
2. 在*身份驗證服務*下拉式選單中，選擇*OpenLDAP*，然後選擇*其他*。
3. 完成文字欄位。

如果前兩種解決方法不適用，請致電 `option-set` API，並設定 `auth.ldap.userObjectClass` 和 `auth.ldap.groupObjectClass` 選項為正確的值。

Windows 系統上的 NetApp 可管理性 SDK 日誌輪替問題

在 Windows 作業系統上將基於 ONTAPI API 的叢集新增至 Unified Manager 後，`nmsdk.log` 檔案大小增加並超出 10 MB 的大小限制。

原因

如果沒有發生日誌輪換，則可能會發生此問題。

糾正措施

1. 停止 Unified Manager。
2. 在 Windows 上安裝 Unified Manager 時，請安裝 Logrotate 版本 0.0.0.18。欲了解更多信息，請參閱["NetApp 可管理性 SDK 技術報告的安全強化指南"](#)。
3. 啟動 Unified Manager。

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	waf1.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.cifsMaxSessPerUserConn	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.vscanBadUserPriv Access	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	wافل.vol.自動調整大小失敗	體積	錯誤
WAFL卷自動調整大小完成	wافل.vol.自動大小.完成	體積	資訊
WAFL READDIR 檔案操作逾時	wافل.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「適用於叢集」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。

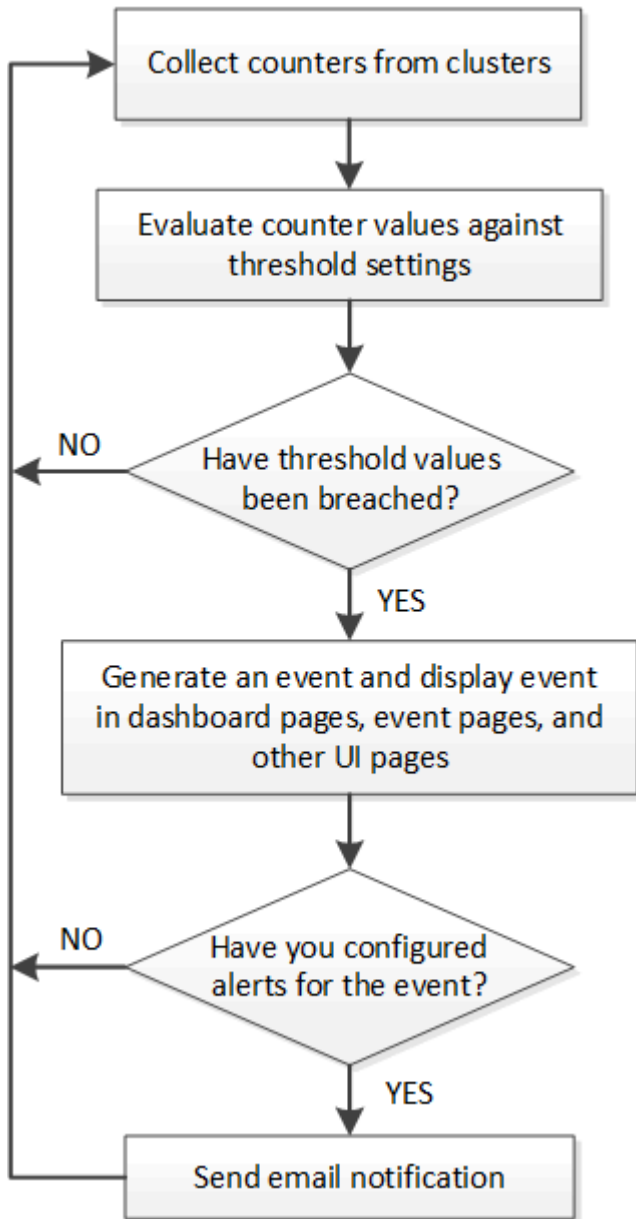
當 Unified Manager 偵測到相同叢集元件連續多次出現相同事件條件時，它會將所有出現的事件視為單一事件，而不是單獨的事件。事件的持續時間會增加，以表明事件仍然有效。

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none"> 從相應的事件詳細資訊頁面確定事件的原因。 選擇事件。 點選*確認*。 採取適當的糾正措施。 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	<ol style="list-style-type: none"> 點選*指派給*>*其他使用者*。 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。 點選*分配*。 <p>電子郵件通知已發送給使用者。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  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。 </div>

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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">a. 選取要啟用的一個或多個事件的複選框。b. 按一下“啟用”。

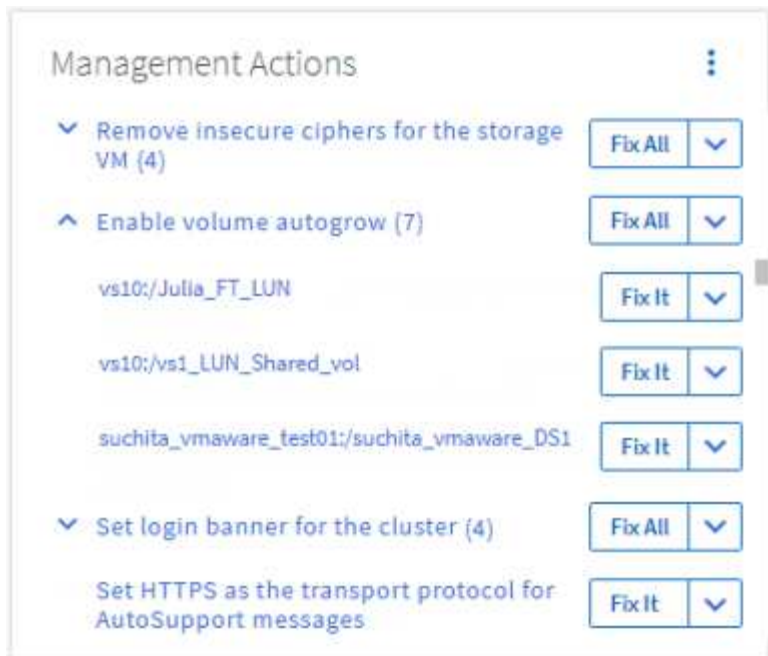
使用 Unified Manager 自動修復功能解決問題

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*。



- 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

- 在左側導覽窗格中，按一下「常規」>「功能設定」。
- 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*。

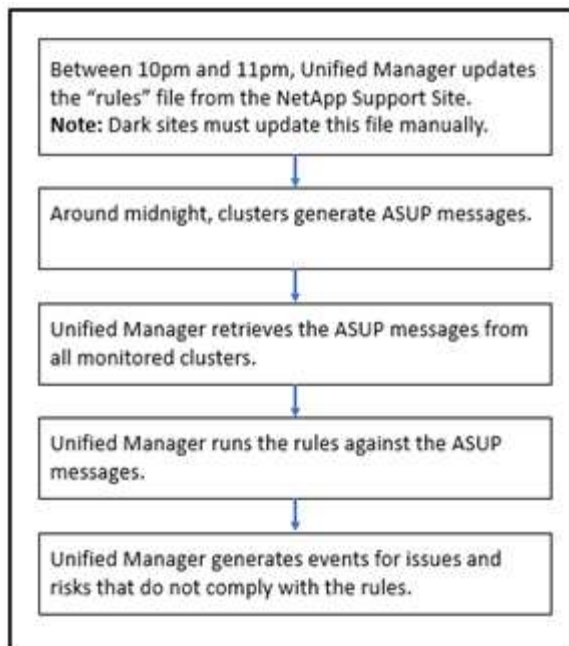
此過程可能需要幾分鐘。

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 AIQCA Secure 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。

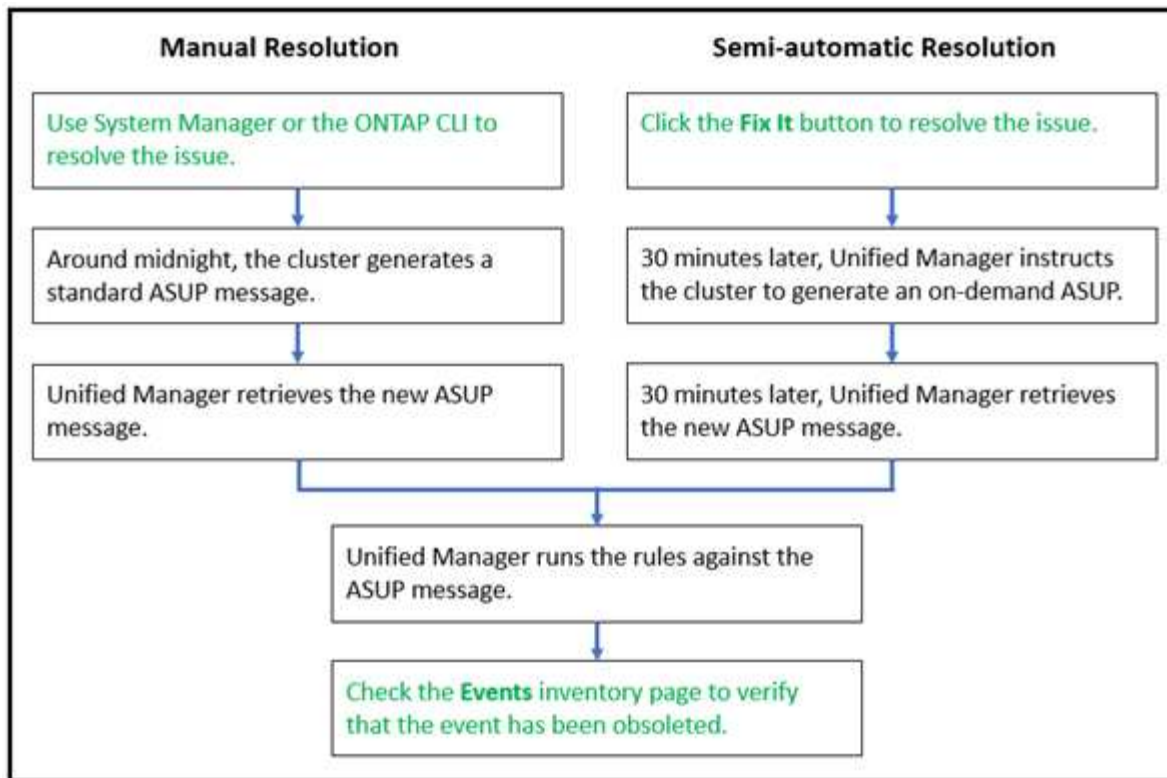


如您所見，在Active IQ平台上編譯的規則檔案保持最新，叢集AutoSupport訊息每天生成，並且 Unified Manager 每天更新事件清單。

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」。

動態效能事件圖表詳情

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。

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
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 *(arINetraCaCheckFailed)	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新定位 *(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* (wafCaResyncComplete)	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： <ul style="list-style-type: none"> • 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 (ocumLunLatencyIopsInci dent)	事件	邏輯單元號	批判的
LUN 延遲和 IOPS 警告閾 值超出 (ocumLunLatencyIopsWar ning)	風險	邏輯單元號	警告
LUN 延遲和 MB/s 臨界閾 值被突破 (ocumLunLatencyMbpsI ncident)	事件	邏輯單元號	批判的
超出 LUN 延遲和 MB/s 警 告閾值 (ocumLunLatencyMbpsW arning)	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 (ocumLunLatencyAggreg atePerfCapacityUsedIncid ent)	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 (ocumEvtMysqlLogFileSi zeWarning)	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 (ocumEvtMccNodeSwitchFcvlLinksDown)	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)	事件	MetroCluster交換機	批判的
 此事件僅適用於Cisco交換器。			

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 *(nvmeNamespaceSpace OutOfSpace)	風險	命名空間	警告
NVMeNS 銷毀 *(nvmeNamespaceDestro y)	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 (ocumNvmeNamespacel opsIncident)	事件	命名空間	批判的
NVMe 命名空間 IOPS 警 告閾值已超出 (ocumNvmeNamespacelo psWarning)	風險	命名空間	警告
NVMe 命名空間 MB/s 臨 界閾值被突破 (ocumNvmeNamespace MbpsIncident)	事件	命名空間	批判的
超出 NVMe 命名空間 MB/s 警告閾值 (ocumNvmeNamespaceM bpsWarning)	風險	命名空間	警告
NVMe 命名空間延遲 ms/op 臨界閾值突破 (ocumNvmeNamespace LatencyIncident)	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 (ocumNvmeNamespaceL atencyWarning)	風險	命名空間	警告
NVMe 命名空間延遲和 IOPS 臨界閾值被突破 (ocumNvmeNamespace LatencyIopsIncident)	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- <i><advisory ID></i> (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(ocumEvtQtreeSpaceNearFull)	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 *(wafIVolAutoSizeFail)	風險	體積	錯誤
WAFL磁碟區自動調整大小完成 *(wafIVolAutoSizeDone)	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 (ocumVolumeLatencyAggregatePerfCapacityUsed Incident)	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 (ocumVolumeLatencyAggregatePerfCapacityUsed Warning)	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 (ocumVolumeLatencyNodePerfCapacityUsed Incident)	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 (ocumVolumeLatencyNodePerfCapacityUsed Warning)	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 (i)。

- 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

導致事件過時的動作，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 (ℹ️)。

- 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 and 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 and 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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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
<code>um cli login -u <username> [-p <password>]</code>	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。
<code>um cli logout</code>	退出 CLI。	顯示相應的訊息。
<code>um help</code>	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
<code>um run cmd [-t <timeout>] <cluster> <command></code>	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。
<code>um run query <sql command></code>	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。
<code>um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip></code>	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。
<code>um datasource list [<datasource-id>]</code>	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。
<code>um datasource modify [-h <hostname-or-ip>] [-u <username>] [-P <password>] [-t <protocol>] [-p <port>] <datasource-id></code>	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。
<code>um datasource remove <datasource-id></code>	從 Unified Manager 中刪除資料來源（叢集）。	顯示相應的訊息。
<code>um option list [<option> ..]</code>	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>]	<p>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。</p> <p>例如：</p> <p>um lun list -cluster 1</p> <p>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。</p>	以表格形式顯示以下值：ID and LUN path.
um svm list [-q] [-ObjectType <object-id>]	<p>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。</p> <p>例如：</p> <p>um svm list -cluster 1</p> <p>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。</p>	以表格形式顯示以下值：Name and Cluster ID.

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

CLI 命令	描述	輸出
<pre>um cluster node list [-q] [-ObjectType <object-id>]</pre>	<p>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。</p> <p>例如：</p> <pre>um cluster node list -cluster 1</pre> <p>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。</p>	<p>以表格形式顯示以下值 Name and Cluster ID。</p>
<pre>um volume list [-q] [-ObjectType <object-id>]</pre>	<p>列出按指定物件篩選後的磁碟區。ObjectType 可以是 lun、mtree、cluster、volume、quota、svm 或 aggregate。</p> <p>例如：</p> <pre>um volume list -cluster 1</pre> <p>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。</p>	<p>以表格形式顯示以下值 Volume ID and Volume Name。</p>
<pre>um quota user list [-q] [-ObjectType <object-id>]</pre>	<p>列出按指定物件篩選後的配額使用者。ObjectType 可以是 mtree、cluster、volume、quota 或 svm。</p> <p>例如：</p> <pre>um quota user list -cluster 1</pre> <p>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。</p>	<p>以表格形式顯示以下值 ID, Name, SID and Email。</p>

CLI 命令	描述	輸出
<code>um aggr list [-q] [-ObjectType <object-id>]</code>	<p>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。</p> <p>例如：</p> <p>um aggr list -cluster 1</p> <p>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。</p>	以表格形式顯示以下值 Aggr ID, and Aggr Name。
<code>um event ack <event-ids></code>	確認一個或多個事件。	顯示相應的訊息。
<code>um event resolve <event-ids></code>	解決一個或多個事件。	顯示相應的訊息。
<code>um event assign -u <username> <event-id></code>	將事件分配給使用者。	顯示相應的訊息。
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	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。
<code>um backup restore -f <backup_file_path_and_name></code>	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。

監控和管理叢集效能

Active IQ Unified Manager效能監控簡介

Active IQ Unified Manager（以前稱為OnCommand Unified Manager）為執行NetApp ONTAP軟體的系統提供效能監控功能和事件根本原因分析。

Unified Manager 可協助您辨識過度使用叢集元件並降低叢集上其他工作負載效能的工作負載。透過定義效能閾值策略，您還可以指定某些效能計數器的最大值，以便在超過閾值時產生事件。Unified Manager 會向您發出有關這些效能事件的警報，以便您採取糾正措施，並使效能恢復到正常運作水準。您可以在 Unified Manager UI 中檢視和分析事件。

Unified Manager 監控兩種類型工作負載的效能：

- 使用者定義的工作負載

這些工作負載包括您在叢集中建立的FlexVol磁碟區和FlexGroup磁碟區。

- 系統定義的工作負載

這些工作負載由內部系統活動組成。

Unified Manager 效能監控功能

Unified Manager 收集並分析執行ONTAP軟體的系統的效能統計資料。它使用動態效能閾值和使用使用者定義的效能閾值來監控許多叢集組件的各種效能計數器。

反應時間（延遲）較長表示儲存物件（例如磁碟區）的執行速度比正常情況慢。此問題還表明使用該磁碟區的客戶端應用程式的效能有所下降。Unified Manager 可識別有效能問題的儲存元件，並提供可採取的解決效能問題的建議操作清單。

Unified Manager 包含以下功能：

- 監控並分析運行ONTAP軟體的系統的工作負載效能統計資料。
- 追蹤叢集、節點、聚合、連接埠、SVM、磁碟區、LUN、NVMe 命名空間和網路介面 (LIF) 的效能計數器。
- 顯示繪製工作負載活動隨時間變化的詳細圖表；包括 IOPS（操作）、MB/s（吞吐量）、延遲（回應時間）、利用率、效能容量和快取比率。
- 使您能夠建立使用者定義的效能閾值策略，當閾值被突破時觸發事件並發送電子郵件警報。
- 使用系統定義的閾值和動態效能閾值來了解您的工作負載活動，以識別效能問題並向您發出警報。
- 識別套用於您的磁碟區和 LUN 的服務品質 (QoS) 策略和效能服務等級原則 (PSL)。
- 清楚地辨識存在爭用的群集組件。
- 識別過度使用叢集組件的工作負載以及效能受到活動增加影響的工作負載。

用於管理儲存系統效能的 **Unified Manager** 介面

這些部分包含有關Active IQ Unified Manager提供的兩個使用者介面的信息，用於解決資料儲存容量、可用性和保護問題。這兩個 UI 是 Unified Manager Web UI 和維護控制台。

如果您想要使用 Unified Manager 中的保護功能，您也必須安裝和設定OnCommand Workflow Automation (WFA)。

Unified Manager Web UI

Unified Manager Web UI 可讓管理員監控和排除與資料儲存容量、可用性和保護相關的叢集問題。

這些部分介紹了管理員可以遵循的一些常見工作流程，以解決 Unified Manager Web UI 中顯示的儲存容量、資料可用性或保護問題。

維護控制台

Unified Manager 維護控制台可讓管理員監控、診斷和解決與 Unified Manager 伺服器本身相關的作業系統問題、版本升級問題、使用者存取問題和網路問題。如果 Unified Manager Web UI 不可用，則維護控制台是存取 Unified Manager 的唯一方法。

您可以使用此資訊存取維護控制台並使用它來解決與 Unified Manager 伺服器功能相關的問題。

叢集配置和效能資料收集活動

群集配置資料的收集間隔為15分鐘。例如，新增叢集後，需要 15 分鐘才能在 Unified Manager UI 中顯示叢集詳細資訊。對集群進行變更時也適用此間隔。

例如，如果您在叢集中的 SVM 中新增兩個新磁碟區，您將在下一個輪詢間隔（最長可達 15 分鐘）後在 UI 中看到這些新物件。

Unified Manager 每五分鐘從所有受監控的叢集收集一次目前效能統計資料。它分析這些數據以識別效能事件和潛在問題。它保留30天的五分鐘歷史性能數據和180天的一小時歷史性能數據。這使您可以查看當前月份的非常詳細的性能詳情以及長達一年的整體性能趨勢。

收集輪詢會偏移幾分鐘，以便每個叢集的資料不會同時發送，這可能會影響效能。

下表描述了 Unified Manager 執行的收集活動：

活動	時間間隔	描述
績效統計調查	每5分鐘	從每個集群收集即時性能數據。

活動	時間間隔	描述
統計分析	每5分鐘	每次統計輪詢後，Unified Manager 都會將收集的資料與使用者定義、系統定義和動態閾值進行比較。 如果超出任何效能閾值，Unified Manager 會產生事件並向指定使用者發送電子郵件（如果已設定為這樣做）。
配置輪詢	每15分鐘	從每個叢集收集詳細的清單信息，以識別所有儲存物件（節點、SVM、磁碟區等）。
總結	每小時	將最近 12 個五分鐘效能資料集合匯總為每小時平均值。 部分UI頁面採用每小時平均值，並保留180天。
預測分析和資料修剪	每天午夜後	分析群集資料以建立未來 24 小時的捲延遲和 IOPS 的動態閾值。 從資料庫中刪除任何超過 30 天的五分鐘效能資料。
資料修剪	每天凌晨 2 點後	從資料庫中刪除任何超過 180 天的事件以及超過 180 天的動態閾值。
資料修剪	每天凌晨 3:30 後	從資料庫中刪除任何超過 180 天的一小時效能資料。

什麼是資料連續性收集週期

資料連續性收集週期檢索即時叢集效能收集週期以外的效能數據，預設情況下，即時叢集效能收集週期每五分鐘運行一次。資料連續性收集使 Unified Manager 能夠填補無法收集即時資料時出現的統計資料空白。

當發生下列事件時，Unified Manager 會對歷史效能資料執行資料連續性收集輪詢：

- 叢集最初會新增到 Unified Manager。

Unified Manager 收集前 15 天的歷史效能資料。這使您可以在新增叢集後的幾個小時內查看該叢集兩週的歷史效能資訊。

此外，如果存在的話，也會報告前一期的系統定義閾值事件。

- 當前效能資料收集週期未按時完成。

如果即時效能輪詢超出了五分鐘的收集時間，則會啟動資料連續性收集週期來收集缺失的資訊。如果沒有資料連續性收集，則跳過下一個收集期。

- Unified Manager 在一段時間內無法訪問，然後又重新上線，如下：
 - 它已重新啟動。
 - 它在軟體升級或建立備份檔案時被關閉。
 - 網路中斷已修復。
- 叢集在一段時間內無法訪問，然後又重新上線，例如以下情況：
 - 網路中斷已修復。
 - 廣域網路連線速度慢延遲了效能資料的正常收集。

一個資料連續性採集週期最多可以採集24小時的歷史資料。如果 Unified Manager 停機超過 24 小時，UI 頁面上的效能資料就會出現差距。

資料連續性收集週期和即時資料收集週期不能同時運作。資料連續性收集週期必須在啟動即時效能資料收集之前完成。當資料連續性收集需要收集超過一小時的歷史資料時，您會在通知窗格頂部看到該叢集的橫幅訊息。

時間戳在收集的資料和事件中意味著什麼

收集的健康和效能資料中出現的時間戳，或作為事件偵測時間出現的時間戳，基於ONTAP叢集時間，並根據 Web 瀏覽器上設定的時區進行調整。

強烈建議您使用網路時間協定 (NTP) 伺服器來同步 Unified Manager 伺服器、ONTAP叢集和 Web 瀏覽器上的時間。



如果您發現某個特定叢集的時間戳記不正確，您可能需要檢查叢集時間是否設定正確。

在 Unified Manager GUI 中導覽效能工作流程

Unified Manager 介面提供了許多頁面用於收集和顯示效能資訊。您可以使用左側導覽面板導覽至 GUI 中的頁面，並使用頁面上的標籤和連結來檢視和設定資訊。

您可以使用以下所有頁面來監視和排除叢集效能資訊故障：

- 儀表板頁面
- 儲存與網路物件清單頁面
- 儲存物件詳細資訊頁面（包括效能資源管理器）
- 配置和設定頁面
- 活動頁面

登入使用者介面

您可以使用支援的 Web 瀏覽器登入 Unified Manager UI。

開始之前

- 網頁瀏覽器必須符合最低要求。

請參閱互通性矩陣 "mysupport.netapp.com/matrix"以取得受支援的瀏覽器版本的完整清單。

- 您必須擁有 Unified Manager 伺服器的 IP 位址或 URL。

如果您 1 小時沒有活動，您將自動退出會話。此時間範圍可在*常規* > *功能設定*下配置。

步驟

1. 在您的 Web 瀏覽器中輸入 URL，其中 URL 是 Unified Manager 伺服器的 IP 位址或完全限定網域名稱 (FQDN)：
 - 對於 IPv4：`https://URL/`
 - 對於 IPv6：`https://[URL]/`

如果伺服器使用自簽名數位證書，瀏覽器可能會顯示警告，表示該證書不受信任。您可以承認風險並繼續訪問，或者安裝憑證授權單位 (CA) 簽署的數位憑證進行伺服器驗證。。在登入畫面上，輸入您的使用者名稱和密碼。

如果使用 SAML 驗證保護登入 Unified Manager 使用者介面，您將在身分識別提供者 (IdP) 登入頁面而不是 Unified Manager 登入頁面中輸入您的憑證。

將顯示“儀表板”頁面。



如果 Unified Manager 伺服器未初始化，則新的瀏覽器視窗將顯示首次體驗精靈。您必須輸入將向其發送電子郵件警報的初始電子郵件收件者、將處理電子郵件通訊的 SMTP 伺服器，以及是否啟用 AutoSupport 以將有關 Unified Manager 安裝的資訊傳送給技術支援。完成此資訊後，將出現 Unified Manager UI。

圖形介面和導航路徑

Unified Manager 具有極大的靈活性，可讓您以多種方式完成多項任務。在 Unified Manager 中工作時，您會發現許多導覽路徑。雖然無法顯示所有可能的導航組合，但您應該熟悉一些更常見的場景。

監控集群對象導航

您可以監控 Unified Manager 管理的任何叢集中所有物件的效能。監控您的儲存物件可以讓您概覽叢集和物件的效能，並包含效能事件監控。您可以從高層次查看效能和事件，也可以進一步調查物件效能和效能事件的任何詳細資訊。

這是許多可能的集群物件導航的一個範例：

1. 在“儀表板”頁面中，查看“性能容量”面板中的詳細信息，以確定使用最多性能容量的集群，然後單擊條形圖導航到該集群的節點列表。
2. 確定具有最高效能容量使用值的節點並按一下該節點。
3. 在節點/效能資源管理器頁面中，按一下檢視和比較選單中的*此節點上的聚合*。
4. 確定使用最多效能容量的聚合並按一下該聚合。

5. 在「聚合/效能資源管理器」頁面上，按一下「檢視和比較」功能表中的「此聚合上的磁碟區」。

6. 確定使用最多 IOPS 的捲。

您應該調查這些卷，看看是否應該應用 QoS 策略或效能服務等級策略，或更改策略設置，以便這些磁碟區不會在叢集上使用如此大比例的 IOPS。

Dashboard All Clusters

Capacity
31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...licity	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.6 TB	51 days	8.0:1
sysmgr...0-1-8	33 TB	148 days	8.3:1

Performance Capacity
No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
sysmgr-fas806-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

Nodes Last updated: Nov 15, 2019, 10:48 AM

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,335 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	43%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Follower Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4...	47.51...	5.8 M...	8%
NSLM12_001	11.4...	216 L...	4.33...	5%

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate

Volume	Latency	IOPS	MB/s
suchita_vmware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmware_d...	3.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

監控叢集效能導航

您可以監控 Unified Manager 管理的所有叢集的效能。監控叢集可為您提供叢集和物件效能的概覽，並包含效能事件監控。您可以從高層次查看效能和事件，也可以進一步調查叢

集和物件效能以及效能事件的任何詳細資訊。

這是許多可能的叢集效能導航路徑的一個範例：

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 要查看有關這些聚合的性能的信息，請選擇“性能：所有聚合”視圖。
3. 確定您想要調查的聚合，然後按一下該聚合名稱以導覽至聚合/效能資源管理器頁面。
4. 或者，在「檢視與比較」功能表中選擇要與此聚合進行比較的其他對象，然後將其中一個物件新增至比較窗格。

兩個物件的統計資料將出現在計數器圖表中以供比較。

5. 在資源管理器頁面右側的比較窗格中，按一下其中一個計數器圖表中的「縮放檢視」以查看有關該聚合的效能記錄的詳細資訊。

Aggregates

Last updated: Nov 15, 2019, 1:18 PM

View: Performance: All Aggregates Search Aggregates Filter

Status	Aggregate	Type	Latency	IOPS	MB/s	Performance Capacity Used	Utilization
	aggr_evt	SSD	0.29 ms/op	3.79 IOPS	<1 MB/s	<1%	<1%
	aggr4	HDD	5.74 ms/op	14.4 IOPS	1.31 MB/s	6%	5%
	aggr3	HDD	5.06 ms/op	3.06 IOPS	<1 MB/s	6%	5%
	meg_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

TIME RANGE: Last 72 Hours

VIEW AND COMPARE: Aggregates on same Node

Aggregate	Latency	IOPS	MB/s	Perf...
aggr3	5.06 ...	3.06 ...	<1 M...	6%
aggr_evt	0.29 ...	3.79 ...	<1 M...	<1%
aggr_automation	0.27...	8.35 ...	<1 M...	<1%

Comparing 1 Additional Object

- aggr4
- aggr3

CHOOSE CHARTS: 7 Charts Selected

Events for Aggregate: aggr4

No data to display



Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4

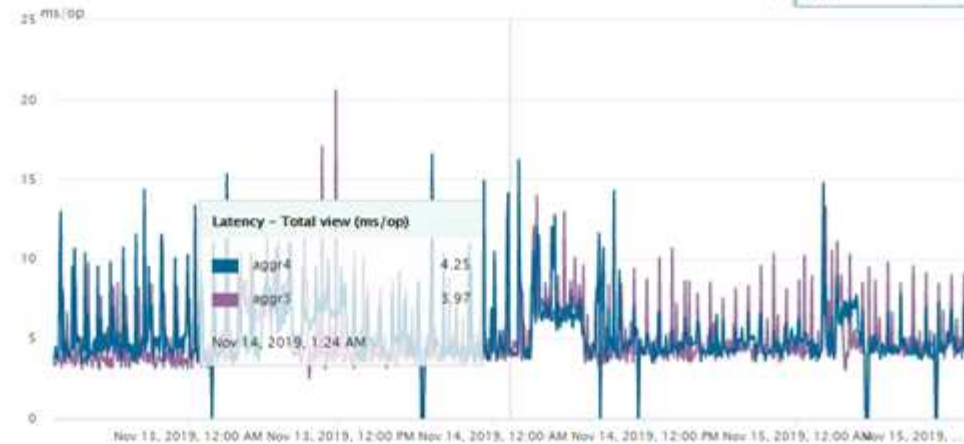
TIME RANGE: Last 72 Hours

- Critical Events
- Error Events
- Warning Events
- Information Events

No data to display

Comparing Objects

- aggr4
- aggr3



Unified Manager 事件詳細資訊頁面可讓您深入了解任何效能事件。這在調查效能事件、排除故障和微調系統效能時非常有用。

根據效能事件的類型，您可能會看到以下兩種類型的事件詳細資訊頁面之一：

- 使用者定義和系統定義的閾值策略事件的事件詳細資訊頁面
- 動態閾值策略事件的事件詳細資訊頁面

這是事件調查導航的一個例子。

1. 在左側導覽窗格中，按一下「事件管理」。
2. 從「檢視」功能表中，按一下「活動效能事件」。
3. 按一下要調查的事件的名稱，將顯示事件詳細資訊頁面。
4. 查看事件描述並查看建議的操作（如果有）以查看有關該事件的更多詳細信息，這可能有助於您解決問題。您可以按一下「分析工作負載」按鈕來顯示詳細的效能圖表，以協助進一步分析問題。

Active performance events

Search Events

Assign To Acknowledge Mark as Resolved Add Alert

Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs2:/julia_feb12_vol3	Volume
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM	Warning	New	Risk	Performance	QoS volume Peak IOP... Threshold Breached	suchita_vmwar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../ocum-c220-07	LUN

Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.

Actions

Suggested Actions to Fix The Issue

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput

- Leave the QoS configuration setting as it is.

Event Information

EVENT TRIGGER TIME	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ON CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

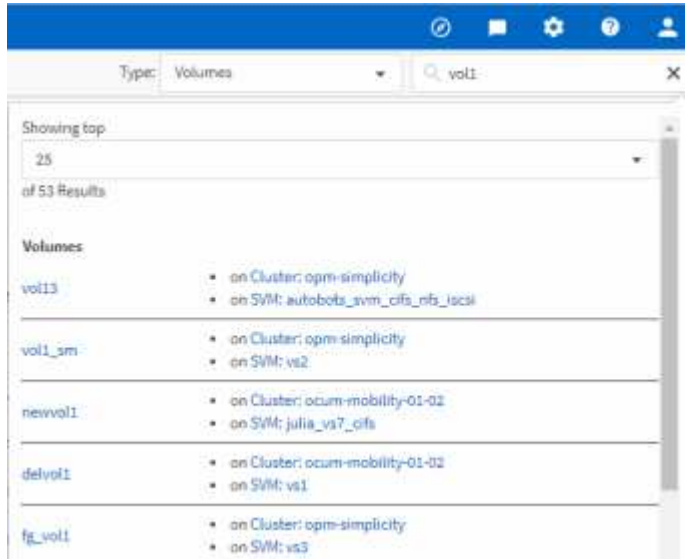
搜尋儲存對象

若要快速存取特定對象，您可以使用功能表列頂部的「搜尋所有儲存對象」欄位。這種對所有物件進行全域搜尋的方法使您能夠按類型快速定位特定物件。搜尋結果按儲存物件類型排序，您可以使用下拉式選單進行篩選。有效搜尋必須至少包含三個字元。

全域搜尋顯示結果總數，但只能存取前 25 個搜尋結果。因此，如果您知道想要快速找到的項目，則可以將全域搜尋功能視為尋找特定項目的快速工具。要獲得完整的搜尋結果，您可以使用物件庫存頁面中的搜尋及其相關的過濾功能。

您可以點擊下拉框並選擇“全部”以同時搜尋所有物件和事件。或者，您可以按一下下拉方塊來指定物件類型。在「搜尋所有儲存物件」欄位中輸入物件或事件名稱的至少三個字符，然後按「Enter」顯示搜尋結果，例如：

- 叢集：叢集名稱
- 節點：節點名稱
- 聚合：聚合名稱
- SVM：SVM 名稱
- 卷：卷名稱
- LUN：LUN 路徑



無法在全域搜尋列中搜尋 LIF 和連接埠。

在此範例中，下拉方塊已選擇磁碟區物件類型。在「搜尋所有儲存物件」欄位中輸入「vol」將顯示名稱中包含這些字元的所有磁碟區的清單。對於物件搜索，您可以按一下任何搜尋結果以導航到該物件的效能資源管理器頁面。對於事件搜索，按一下搜尋結果中的項目將導航至「事件詳細資料」頁面。

過濾庫存頁面內容

您可以在 Unified Manager 中過濾庫存頁面數據，以便根據特定條件快速定位數據。您可以使用篩選功能來縮小 Unified Manager 頁面的內容範圍，以僅顯示您感興趣的結果。這提供了一種非常有效的方法，可以僅顯示您感興趣的數據。

使用*過濾*根據您的喜好自訂網格視圖。可用的篩選選項是基於網格中查看的物件類型。如果目前套用了過濾器，則已套用的過濾器的數量將顯示在過濾器按鈕的右側。

支援三種類型的過濾參數。

範圍	驗證
字串（文字）	運算子包括*包含*、以...開頭、以...結尾*和*不包含。

範圍	驗證
數位	運算子包括*大於*、小於、在最後*和*之間。
枚舉（文本）	運算子是 is 和 is not 。

每個篩選器都需要列、運算子和值欄位；可用的篩選器反映目前頁面上可篩選的列。您最多可以套用四個濾鏡。過濾結果基於組合過濾參數。過濾結果適用於過濾搜尋中的所有頁面，而不僅僅是目前顯示的頁面。

您可以使用過濾面板新增過濾器。

1. 在頁面頂部，按一下“過濾器”按鈕。顯示過濾面板。
2. 點擊左側下拉清單並選擇一個物件；例如，“*Cluster*”或效能計數器。
3. 按一下中心下拉列表，然後選擇要使用的運算子。
4. 在最後一個清單中，選擇或輸入一個值以完成該物件的篩選。
5. 若要新增另一個過濾器，請按一下「+新增過濾器」。顯示附加的過濾欄位。使用前面步驟中所述的程序完成此過濾器。請注意，新增第四個過濾器後，*+新增過濾器*按鈕不再顯示。
6. 按一下“套用過濾器”。過濾選項應用於網格，過濾器的數量顯示在過濾器按鈕的右側。
7. 使用過濾面板透過點擊要刪除的過濾器右側的垃圾桶圖示來刪除單個過濾器。
8. 若要刪除所有過濾器，請按一下過濾面板底部的“重設”。

過濾範例

該圖顯示了帶有三個過濾器的過濾面板。當您擁有的過濾器少於四個時，將顯示“+新增過濾器”按鈕。

The screenshot shows a filter panel with three rows of filters. Each row consists of a field dropdown, an operator dropdown, a value input field, and a unit dropdown. To the right of each row is a trash icon for deletion. At the bottom left is a '+ Add Filter' button, and at the bottom right are 'Cancel' and 'Apply Filter' buttons. The filters are: 1. Mbps greater than 5 MBps; 2. Node name starts with test; 3. Type is FCP Port.

點擊“套用過濾器”後，“過濾”面板將關閉，套用過濾器，並顯示已套用的過濾器數量（  ）。

從儀表板監控叢集效能

Unified Manager 儀表板提供了幾個面板，顯示由此 Unified Manager 實例監控的所有叢集的進階效能狀態。它使您能夠評估託管叢集的整體效能，並快速記錄、定位或分配解決任何已識別的特定事件。

了解儀表板上的性能面板

Unified Manager 儀表板提供了一些面板，顯示您環境中正在監控的所有叢集的進階效能狀態。您可以選擇查看所有集群或單一集群的狀態。

除了顯示效能資訊外，大多數面板還顯示該類別中的活躍事件數以及過去 24 小時內新增的事件數。這些資訊可協助您確定需要進一步分析哪些群集以解決報告的事件。點擊事件將顯示前幾個事件，並提供指向事件管理庫存頁面的鏈接，該頁面經過篩選以顯示該類別中的事件。

以下面板提供效能狀態。

- 性能容量面板

查看所有群集時，此面板顯示每個群集的效能容量值（前 1 小時的平均值）以及效能容量達到上限的天數（基於每日成長率）。點擊長條圖將轉到該叢集的節點清單頁面。請注意，節點庫存頁面顯示過去 72 小時的平均效能容量，因此該值可能與儀表板值不符。

查看單一叢集時，此面板顯示叢集效能容量、總 IOPS 和總吞吐量值。

- 工作負載 IOPS 面板

當啟用工作負載主動管理並查看單一叢集時，此面板顯示目前在一定 IOPS 範圍內執行的工作負載總數。

- 工作負載效能面板

啟用工作負載主動管理後，此面板顯示指派給每個定義的效能服務等級的符合和不符合的工作負載總數。按一下長條圖可前往「工作負載」頁面中指派給該原則的工作負載。

- 使用概覽面板

查看所有叢集時，您可以選擇按最高 IOPS 或吞吐量（MB/s）排序以查看叢集。

查看單一叢集時，您可以選擇按最高 IOPS 或吞吐量（MB/s）排序以查看該叢集上的工作負載。

效能橫幅訊息和說明

Unified Manager 可能會在通知頁面上顯示橫幅訊息（來自通知鈴），以提醒您特定叢集的狀態問題。

橫幅訊息	描述	解決
No performance data is being collected from cluster <code>cluster_name</code> . Restart Unified Manager to correct this issue.	Unified Manager 收集服務已停止，且未從任何叢集收集效能資料。	重新啟動 Unified Manager 以解決此問題。如果此方法無法解決問題，請聯絡技術支援。

橫幅訊息	描述	解決
More than x hour(s) of historical data is being collected from cluster <code>cluster_name</code> . Current data collections will start after all historical data is collected.	資料連續性收集週期目前正在運行，以檢索即時叢集效能收集週期之外的效能資料。	<p>無需採取任何行動。資料連續性收集週期完成後，將收集當前效能資料。</p> <p>當新增叢集或 Unified Manager 由於某種原因無法收集目前效能資料時，將執行資料連續性收集週期。</p>

修改效能統計收集間隔

效能統計資訊的預設收集間隔為5分鐘。如果您發現大型叢集的收集未在預設時間內完成，則可以將此間隔變更為 10 或 15 分鐘。此設定會影響此 Unified Manager 實例所監控的所有叢集的統計資訊收集。

開始之前

您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。

橫幅訊息指出了效能統計資料收集未按時完成的問題 `Unable to consistently collect from cluster <cluster_name>` 或者 `Data collection is taking too long on cluster <cluster_name>`。

僅當因統計資訊收集問題而需要時才應變更收集間隔。請勿因任何其他原因更改此設定。



將此值從預設設定 5 分鐘變更為其他值可能會影響 Unified Manager 報告的效能事件的數量和頻率。例如，當超過策略 30 分鐘時，系統定義的效能閾值會觸發事件。當使用 5 分鐘收集時，必須超過該政策連續六次收集。對於 15 分鐘的收集，政策必須僅超出兩個收集期。

叢集設定頁面底部的訊息指示目前統計資料收集間隔。

步驟

1. 使用 SSH 以維護使用者身分登入 Unified Manager 主機。
 - 顯示 Unified Manager 維護控制台提示。
2. 鍵入標示為「效能輪詢間隔配置」的選單選項的編號，然後按 Enter。
3. 如果出現提示，請再次輸入維護使用者密碼。
4. 鍵入要設定的新輪詢間隔的數字，然後按 Enter。

如果您將 Unified Manager 收集間隔變更為 10 或 15 分鐘，且您目前已連線至外部資料提供者（例如 Graphite），則必須變更資料提供者傳輸間隔，使其等於或大於 Unified Manager 收集間隔。


使用工作負載分析器排除工作負載故障

工作負載分析器提供了一種在單一頁面上查看單一工作負載的重要健康和效能標準的方法，以協助進行故障排除。透過查看工作負載的所有當前和過去事件，您可以更好地了解工

作負載現在可能存在效能或容量問題的原因。

使用此工具還可以幫助您確定儲存是否是導致應用程式效能問題的原因，或者該問題是否是由網路或其他相關問題引起的。

您可以從使用者介面中的多個位置啟動此功能：

- 從左側導覽功能表上的「工作負載分析」選擇
- 在事件詳細資料頁面中點選「分析工作負載」按鈕
- 在任何工作負載清單頁面（磁碟區、LUN、工作負載、NFS 共用或 SMB/CIFS 共用）中，按一下更多圖標 ，然後*分析工作負載*
- 在虛擬機器頁面中，按一下任意資料儲存物件上的「分析工作負載」按鈕

當您從左側導覽功能表啟動工具時，您可以輸入要分析的任何工作負載的名稱，並選擇要排除故障的時間範圍。當您從任何工作負載或虛擬機器清單頁面啟動該工具時，工作負載的名稱將自動填寫，並且工作負載的資料將以預設的 2 小時時間範圍顯示。從事件詳情頁面啟動工具時，會自動填入工作負載的名稱，並顯示 10 天的資料。

工作負載分析器顯示哪些數據

工作負載分析器頁面顯示有關可能影響工作負載的任何當前事件的資訊、可能修復導致事件的問題的建議以及用於分析效能和容量歷史記錄的圖表。

在頁面頂部，您可以指定要分析的工作負載（磁碟區或 LUN）的名稱以及要查看統計資料的時間範圍。如果您想查看更短或更長的時間段，您可以隨時變更時間範圍。

頁面的其他區域顯示分析結果以及效能和容量圖表。



LUN 的工作負載圖表不提供與卷圖表相同級別的統計信息，因此在分析這兩種類型的工作負載時您會注意到差異。

• 活動摘要區

顯示一段時間內發生的事件的數量和類型的簡要概述。當有來自不同影響領域（例如效能和容量）的事件時，會顯示此訊息，以便您可以選擇感興趣的事件類型的詳細資訊。按一下事件類型以查看事件名稱清單。

如果該時間範圍內只有一個事件，則會針對某些事件列出修復該問題的建議清單。

• 事件時間表

顯示指定時間範圍內發生的所有事件。將遊標停留在每個事件上即可查看事件名稱。

如果您透過點擊事件詳細資料頁面上的「分析工作負載」按鈕到達此頁面，則所選事件的圖示將會變得更大，以便您識別該事件。

• 性能圖表區域

根據您選擇的時間範圍顯示延遲、吞吐量（IOPS 和 MB/s）和利用率（節點和聚合）的圖表。如果您想進行進一步的分析，可以按一下「查看效能詳細資料」連結來顯示工作負載的效能資源管理器頁面。

◦ *延遲*顯示所選時間範圍內工作負載的延遲。此圖表有三種視圖，您可以查看：

- *總*延遲
- *細分*延遲（按讀取、寫入和其他流程細分）
- *集群組件*延遲（按集群組件細分）

看"[集群組件及其爭用的原因](#)"有關此處顯示的集群組件的說明。 吞吐量*顯示所選時間範圍內工作負載的 IOPS 和 MB/s 吞吐量。此圖表有四個視圖，可讓您查看： 總*吞吐量 細分*吞吐量（按讀取、寫入和其他流程細分） 雲端吞吐量（用於將資料寫入雲端和從雲端讀取資料的 MB/s；適用於將容量分層到雲端的工作負載） *帶預測的 IOPS（預測在時間範圍內預期的上限和下限值圖表 IOPS 輸出值 (QoS)最大和最小吞吐量閾值設定（如果已配置），因此您可以看到系統可能在何處使用 QoS 策略有意限制吞吐量。 *利用率*顯示在選定時間範圍內運行工作負載的聚合和節點的利用率。從這裡您可以看到您的聚合或節點是否被過度利用，這可能導致高延遲。分析FlexGroup磁碟區時，利用率圖表上列出了多個節點和多個聚合。

• 容量圖表區域

顯示過去一個月工作負載的資料容量和快照容量圖表。

對於卷，您可以按一下查看容量詳細資料連結以顯示工作負載的運行狀況詳細資訊頁面，以便進行進一步的分析。LUN 不提供此鏈接，因為沒有 LUN 的“健康詳情”頁面。


- *容量視圖*顯示分配給工作負載的總可用空間和邏輯使用空間（經過所有NetApp優化後）。
- **Snapshot View** 顯示為 Snapshot 副本保留的總空間以及目前正在使用的空間量。請注意，LUN 不提供快照視圖。
- *雲層視圖*顯示本機效能層中正在使用的容量以及雲層中正在使用的容量。這些圖表包括容量滿載之前剩餘時間的估計值。此資訊基於歷史使用情況，需要至少 10 天的資料。當剩餘容量少於 30 天時，Unified Manager 會將儲存空間標識為「幾乎已滿」。

我什麼時候應該使用工作負載分析器

您通常會使用工作負載分析器來排除使用者報告的延遲問題，更徹底分析報告的事件或警報，或探索您發現正在執行異常的工作負載。

如果使用者聯絡您並告知他們正在使用的應用程式運行非常緩慢，您可以檢查應用程式運行的工作負載的延遲、吞吐量和利用率圖表，以查看儲存是否是導致效能問題的原因。您也可以使用容量圖表來查看容量是否較低，因為ONTAP系統的容量使用率超過 85% 可能會導致效能問題。這些圖表將幫助您確定問題是由儲存還是網路或其他相關問題引起的。

如果 Unified Manager 產生了效能事件，並且您想要更徹底地檢查問題的原因，則可以從事件詳細資訊頁面啟動工作負載分析器，方法是點擊 **分析工作負載** 按鈕來研究工作負載的一些延遲、吞吐量和容量趨勢。

如果您在查看任何工作負載清單頁面（磁碟區、LUN、工作負載、NFS 共用或 SMB/CIFS 共用）時發現工作負載運行異常，您可以按一下「更多」圖標 ，然後*分析工作負載*開啟工作負載分析頁面，進一步檢查工作負載。

使用工作負載分析器

有多種方法可以從使用者介面啟動工作負載分析器。這裡我們描述如何從左側導覽窗格啟動該工具。

步驟

1. 在左側導覽窗格中，按一下「工作負載分析」。

將顯示“工作負載分析”頁面。

2. 如果您知道工作負載名稱，請輸入該名稱。如果您不確定全名，請輸入至少 3 個字符，系統將顯示與該字串相符的工作負載清單。
3. 如果您想查看超過預設 2 小時的統計數據，請選擇時間範圍，然後按一下「套用」。
4. 查看摘要區域以了解該時間範圍內發生的事件。
5. 查看效能和容量圖表，了解任何指標何時出現異常，並查看是否有任何事件與異常條目一致。

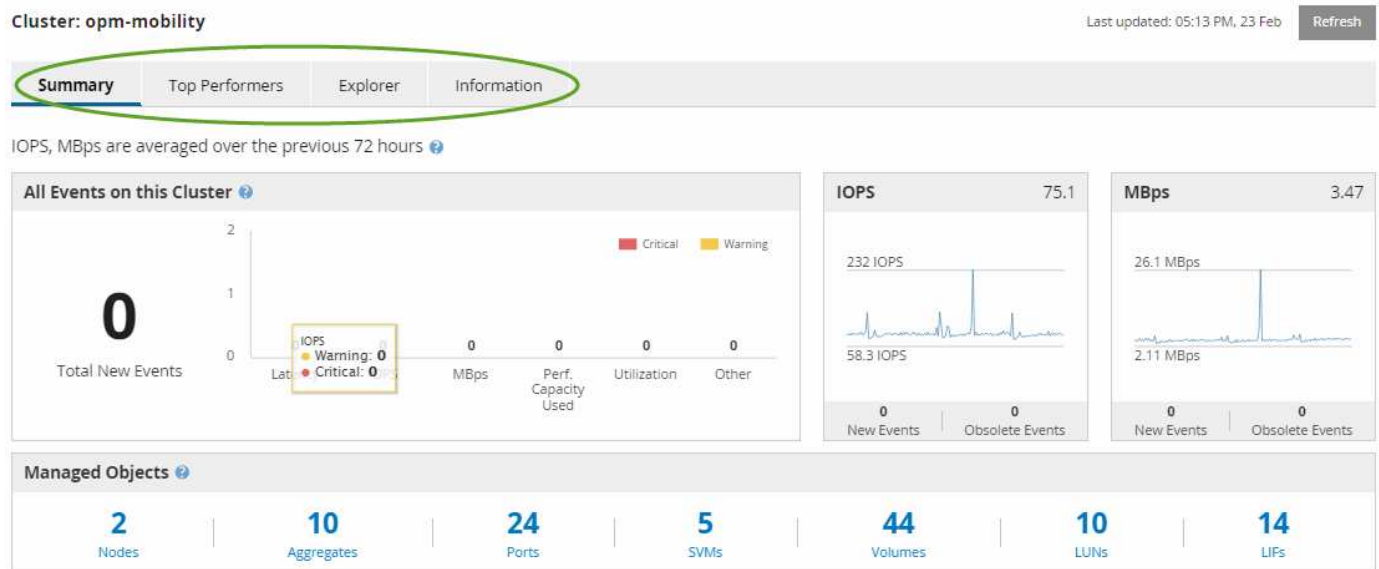
從效能叢集登入頁面監控叢集效能

效能群集登入頁面顯示由 Unified Manager 實例監控的選定群集的進階效能狀態。此頁面可讓您評估特定叢集的整體效能，並快速記錄、定位或指派已識別的任何特定於叢集的事件以供解決。

了解性能集群登陸頁面

效能集群登入頁面提供了所選集群的高級效能概述，重點關注集群內前 10 個物件的效能狀態。效能問題顯示在頁面頂部的「此叢集上的所有事件」面板中。

效能群集登入頁面提供了由 Unified Manager 實例管理的每個群集的進階概述。此頁面為您提供有關事件和效能的信息，並使您能夠監控和排除叢集故障。下圖顯示了名為 opm-mobility 的叢集的效能叢集登入頁面的範例：



叢集摘要頁面上的事件計數可能與效能事件清單頁面上的事件計數不符。這是因為，當違反組合閾值策略時，「群集摘要」頁面可以在「延遲」和「利用率」欄中分別顯示一個事件，而當違反組合策略時，「效能事件清單」頁面僅顯示一個事件。



如果叢集已從 Unified Manager 的管理中刪除，則狀態 已刪除 將顯示在頁面頂部的叢集名稱右側。

性能集群登陸頁面

效能集群登入頁面顯示所選集群的高階效能狀態。透過此頁面，您可以存取所選叢集上儲存物件的每個效能計數器的完整詳細資訊。

效能群集登入頁麵包含四個選項卡，將群集詳細資料分為四個資訊區域：

- 摘要頁面
 - 叢集事件窗格
 - MB/s 和 IOPS 效能圖表
 - 管理物件窗格
- 最佳表演者頁面
- 資源管理器頁面
- 資訊頁面

效能集群摘要頁面

效能群集摘要頁面提供群集的活動事件、IOPS 效能和 MB/s 效能的摘要。此頁面還包括叢集中儲存物件的總數。

叢集效能事件窗格

叢集效能事件窗格顯示叢集的效能統計資料和所有活動事件。這在監控叢集以及所有與叢集相關的效能和事件時最有用。

此群集窗格上的所有事件

此叢集上的所有事件窗格顯示前 72 小時內所有活動的叢集效能事件。最左側顯示「總活動事件」；此數字代表此叢集中所有儲存物件的所有新事件和已確認事件的總數。您可以點擊「總活動事件」連結導覽至「事件清單」頁面，該頁面經過過濾以顯示這些事件。

群集的總活動事件長條圖顯示活動嚴重事件和警告事件的總數：

- 延遲（節點、聚合、SVM、磁碟區、LUN 和命名空間的總延遲）
- IOPS（叢集、節點、聚合、SVM、磁碟區、LUN 和命名空間的總數）
- MB/s（叢集、節點、聚合、SVM、磁碟區、LUN、命名空間、連接埠和 LIF 的總數）
- 已使用的效能容量（節點和聚合的總容量）
- 利用率（節點、聚合和連接埠的總數）
- 其他（卷的緩存未命中率）

此清單包含由使用者定義的閾值策略、系統定義的閾值策略和動態閾值觸發的活動效能事件。

圖表資料（垂直計數器條）顯示為紅色 (■) 表示關鍵事件，黃色 (■) 表示警告事件。將遊標放在每個垂直計數器條上以查看事件的實際類型和數量。您可以按一下「刷新」來更新計數器面板資料。

您可以透過點擊圖例中的「嚴重」和「警告」圖示來顯示或隱藏「總活動事件」效能圖中的嚴重事件和警告事件。如果隱藏某些事件類型，圖例圖示將顯示為灰色。

櫃檯面板

計數器面板顯示前 72 小時的叢集活動和效能事件，並包含以下計數器：

- **IOPS** 計數器面板

IOPS 表示叢集的運作速度，以每秒輸入/輸出運算元表示。此計數器面板提供了過去 72 小時內叢集 IOPS 健康狀況的進階概述。您可以將遊標放在圖形趨勢線上以查看特定時間的 IOPS 值。

- **MB/s** 計數器面板

MB/s 表示每秒有多少資料以兆位元組為單位傳輸到叢集和從叢集傳輸出去。此計數器面板提供了過去 72 小時內叢集 MB/s 健康狀況的進階概覽。您可以將遊標放在圖形趨勢線上以查看特定時間的 MB/s 值。

圖表右上角灰色條中的數字是過去 72 小時內的平均值。趨勢線圖底部和頂部顯示的數字是過去 72 小時內的最小值和最大值。圖表下方的灰色條包含過去 72 小時內活動事件（新事件和已確認事件）和過時事件的數量。

計數器面板包含兩種類型的事件：

- 積極的

表示效能事件目前處於活動狀態（新的或已確認）。導致該事件的問題尚未自行修正或尚未解決。儲存物件的效能計數器仍然高於效能閾值。

- 過時的

表示該事件不再有效。導致該事件的問題已自行修正或已解決。儲存物件的效能計數器不再高於效能閾值。

對於*活動事件*，如果有事件，您可以將遊標放在事件圖示上，然後按一下事件編號以連結到相應的事件詳細資訊頁面。如果有多個事件，您可以按一下「檢視所有事件」以顯示「事件清單」頁面，該頁面經過篩選以顯示所選物件計數器類型的所有事件。

管理物件窗格

「效能摘要」標籤中的「管理物件」窗格提供了叢集的儲存物件類型和數量的頂級概覽。此窗格可讓您追蹤每個叢集中物件的狀態。

管理物件計數是截至上一個收集期間的時間點資料。每隔 15 分鐘就會發現新物體。

按一下任何物件類型的連結數字將顯示該物件類型的物件效能清單頁面。物件清單頁面經過過濾，僅顯示此叢集上的物件。

管理對像有：

- 節點

集群中的物理系統。

- 聚合

一組多個獨立磁碟冗餘陣列 (RAID) 群組，可以作為單一單元進行管理以進行保護和配置。

- 連接埠

節點上的實體連接點，用於連接網路上的其他設備。

- 儲存虛擬機

透過唯一網路位址提供網路存取的虛擬機器。SVM 可以從不同的命名空間提供數據，並且可以與叢集的其餘部分分開管理。

- 卷

透過一個或多個支援的存取協定保存可存取使用者資料的邏輯實體。此計數包括FlexVol捲和FlexGroup磁碟區；但不包括FlexGroup組成部分。

- LUN

光纖通道 (FC) 邏輯單元或 iSCSI 邏輯單元的識別碼。邏輯單元通常對應於儲存卷，並在電腦作業系統中表示為裝置。

- 網路介面

代表節點的網路存取點的邏輯網路介面。此計數包括所有介面類型。

最佳表演者頁面

根據您選擇的效能計數器，「最佳效能者」頁面顯示具有最高效能或最低效能的儲存物件。例如，在儲存虛擬機器類別中，您可以顯示具有最高 IOPS、最高延遲或最低 MB/s 的 SVM。此頁面還顯示任何表現最佳者是否有任何活躍的表現事件（新的或已確認的）。

「最佳表現者」頁面最多顯示每個物件的 10 個。請注意，Volume 物件包括FlexVol磁碟區和FlexGroup磁碟區。

- 時間範圍

您可以選擇一個時間範圍來查看表現最佳的物件；所選的時間範圍適用於所有儲存物件。可用時間範圍：

- 最後一小時
- 過去 24 小時
- 過去 72 小時（預設）
- 過去 7 天

- 公制

點擊“Metric”選單以選擇不同的計數器。計數器選項對於物件類型來說是唯一的。例如，Volumes 物件的可用計數器有 **Latency**、**IOPS** 和 **MB/s**。變更計數器會根據所選計數器重新載入具有最佳表現者的面板資料。

可用計數器：



- 延遲

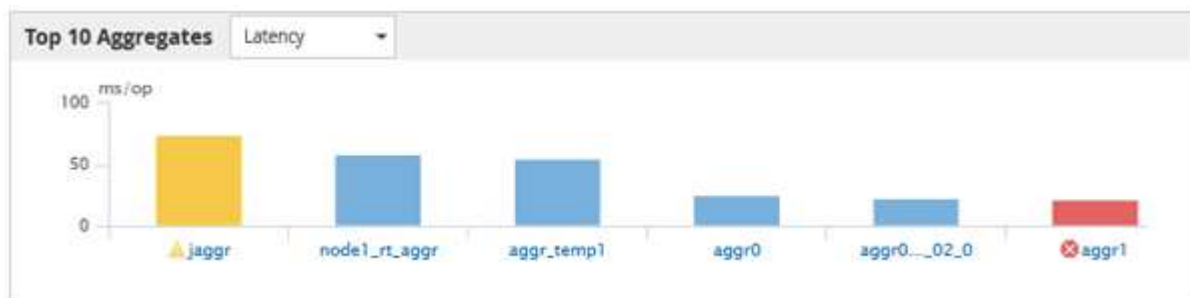
- 每秒輸入/輸出次數
- MB/秒
- 已使用的效能容量（針對節點和聚合）
- 利用率（針對節點和聚合）

- 種類

按一下「排序」功能表可為選定的物件和計數器選擇升序或降序排序。選項為*從高到低*和*從低到高*。這些選項使您能夠查看效能最高或效能最低的物件。



- 櫃檯酒吧

圖表中的計數器條顯示每個物件的效能統計數據，以該項目的長條表示。長條圖採用顏色編碼。如果計數器未突破性能閾值，則計數器條顯示為藍色。如果閾值突破處於活動狀態（新事件或已確認事件），則長條圖將以該事件的顏色顯示：警告事件以黃色顯示（），關鍵事件顯示為紅色（）。閾值違規進一步透過警告和嚴重事件的嚴重性事件指示圖示來指示。



對於每個圖表，X 軸顯示所選物件類型的最佳表現。Y 軸顯示適用於所選計數器的單位。按一下每個垂直長條圖元素下方的物件名稱連結以導覽至所選物件的效能登入頁面。

- 嚴重程度事件指示器

嚴重性事件*指示圖示顯示在活動嚴重事件的物件名稱左側（）或警告（）頂級表演者圖表中的事件。按一下「*嚴重性事件」指示器圖示可查看：

- 一項活動

導航至該活動的事件詳細資訊頁面。

- 兩個或更多事件

導航至事件清單頁面，該頁面經過過濾以顯示所選物件的所有事件。

- 匯出按鈕

創建一個`.csv`包含計數器欄中顯示的資料的檔案。您可以選擇為您正在查看的單一叢集或資料中心中的所有叢集建立檔案。

使用「效能清單」頁面監控效能

物件清單效能頁面顯示物件類型類別中所有物件的效能資訊、效能事件和物件健康狀況。





這為您提供了叢集內每個物件（例如所有節點或所有磁碟區）效能狀態的概覽。

物件庫存效能頁面提供了物件狀態的進階概述，使您能夠評估所有物件的整體效能並比較物件效能資料。您可以透過搜尋、排序和篩選來優化物件庫存頁面的內容。這在監控和管理物件效能時非常有用，因為它使您能夠快速找到具有效能問題的物件並開始故障排除過程。

Nodes - Performance / All Nodes

Last updated: Jan 17, 2019, 7:54 AM 

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		↓		⚙			
<input type="checkbox"/>	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
<input type="checkbox"/>		ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
<input checked="" type="checkbox"/>		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
<input type="checkbox"/>		ocum-mobility-01	0.018 ms/op	< 1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
<input type="checkbox"/>		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

預設情況下，效能清單頁面上的物件會根據物件效能關鍵性進行排序。具有新的關鍵效能事件的物件列在最前面，具有警告事件的物件列在後面。這提供了必須解決的問題的直接視覺指示。所有性能數據均基於 72 小時平均值。

您可以透過點選物件名稱列中的物件名稱，輕鬆地從物件庫存績效頁面導覽至物件詳細資料頁面。例如，在效能/所有節點庫存頁面上，您可以點選*節點*列中的節點物件。物件詳細資訊頁面提供有關所選物件的深入資訊和詳細信息，包括活動事件的並排比較。

查看所有儲存物件的效能清單頁面

您可以使用效能清單頁面查看有關每個可用儲存物件（例如叢集、聚合、磁碟區等）的效能資訊摘要。您可以連結到性能對象詳細資訊頁面以查看特定對象的詳細資訊。

預設情況下，視圖頁面中的物件會根據事件嚴重性進行排序。發生嚴重事件的物件列在最前面，發生警告事件的物件列在後面。這提供了必須解決的問題的直接視覺指示。

您可以將這些資料從這些頁面匯出為逗號分隔的值(.csv) 文件、Microsoft Excel 文件(.xlsx) ， 或者(.pdf) 文檔，然後使用匯出的資料建立報表。此外，您可以自訂頁面，然後使用「計畫報告」按鈕安排定期建立和透過電子郵件傳送報告。

這些頁面上的所有欄位都可以在自訂檢視和報表中使用的。一些欄位連結到相關頁面，以便提供更詳細的視圖。

效能：所有叢集視圖

效能：所有叢集視圖顯示由 Unified Manager 實例監控的每個叢集的效能事件、資料和設定資訊概覽。此頁面使您能夠監控叢集的效能，並解決效能問題和閾值事件。

您可以使用*指派效能閾值策略*和*清除效能閾值策略*按鈕為物件庫存頁面上的任何物件指派效能閾值策略或清除閾值策略。

以下是「效能：所有叢集」視圖中的一些重要欄位。

- 集群 FQDN：集群的完全限定域名 (FQDN)。

- IOPS：叢集每秒的輸入/輸出運算元。
- MB/s：叢集上的吞吐量，以每秒 MiB 為單位。
- 容量欄位：可用容量和總容量（以 GiB 為單位）。
- 主機名稱或 IP 位址：叢集管理 LIF 的主機名稱或 IP 位址（IPv4 或 IPv6）。
- 作業系統版本：叢集上安裝的ONTAP軟體版本。



如果叢集中的節點上安裝了不同版本的ONTAP軟體，則列出最低版本號。您可以從「效能：所有節點」視圖查看每個節點上安裝的ONTAP版本。

- 閾值策略：在此儲存物件上有效的使用者定義的效能閾值策略或策略。您可以將遊標放在包含省略號 (...) 的政策名稱上，以查看完整的策略名稱或已指派的策略名稱清單。指派效能閾值策略和清除效能閾值策略按鈕保持停用狀態，直到您透過點選最左側的複選框選擇一個或多個物件。

效能：所有磁碟區視圖

效能：所有磁碟區視圖顯示由 Unified Manager 實例監控的每個FlexVol volume和FlexGroup磁碟區的效能事件、計數器資料和設定資訊概覽。這使您能夠快速監控磁碟區的效能，並解決效能問題和閾值事件。

如果要分析特定物件的延遲和吞吐量，請按一下更多選項按鈕；然後*分析工作負載*，您可以在工作負載分析頁面上查看效能和容量圖表。如果您擁有系統管理員的有效憑證，則可以在系統管理員上查看詳細資訊。



對於資料保護 (DP) 卷，僅顯示使用者產生的流量的計數器值。此頁面上不顯示根卷。

以下是「效能：所有磁碟區」視圖中的一些重要欄位。

- 樣式：FlexVol或FlexGroup。
- 延遲：對於FlexVol卷，這是卷對所有 I/O 請求的平均回應時間，以每次操作的毫秒數表示。對於FlexGroup卷，這是所有組成捲的平均延遲。
- IOPS/TB：基於工作負載所消耗的總空間，每秒處理的輸入/輸出運算元（以 TB 為單位）。此計數器測量給定的儲存容量可以提供多少效能。
- IOPS：對於FlexVol磁碟區，這是磁碟區每秒的輸入/輸出運算元。對於FlexGroup卷，這是所有組成捲的 IOPS 的總和。
- MB/s：對於FlexVol卷，這是磁碟區上的吞吐量，以每秒兆位元組為單位。對於FlexGroup卷，這是所有組成捲的 MB/s 的總和。
- 容量欄位：可用容量和總容量（以 GiB 為單位）。

請參閱以下連結以了解更多資訊：

- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)
- ["Unified Manager 監控的工作負載類型"](#)
- ["查看應用於特定磁碟區或 LUN 的 QoS 原則群組設置"](#)
- ["了解 Unified Manager 將資料分層到雲端的建議"](#)
- ["查看效能圖表以比較同一 QoS 策略群組中的磁碟區或 LUN"](#)

效能：所有聚合視圖

效能：所有聚合視圖顯示由 Unified Manager 實例監控的每個聚合的效能事件、資料和設定資訊概覽。此頁面使您能夠監控聚合的效能，並解決效能問題和閾值事件。

以下是「效能：所有聚合」視圖中的一些重要欄位。

- 類型：聚合的類型：
 - 硬碟
 - 雜交種。結合了 HDD 和 SSD，但尚未啟用 Flash Pool。
 - 混合 (Flash Pool)。結合了 HDD 和 SSD，並且已啟用 Flash Pool。
 - 固態硬碟
 - SSD (FabricPool)。結合 SSD 和雲層
 - HDD (FabricPool)。結合 HDD 和雲層
 - VM磁碟 (SDS)。虛擬機器內的虛擬磁碟
 - VMDisk (FabricPool)。結合虛擬磁碟和雲層
 - LUN (FlexArray)
- 非活動資料報告：此聚合上是否啟用或停用非活動資料報告功能。啟用後，此聚合上的磁碟區將在「效能：所有磁碟區」檢視中顯示冷資料量。當ONTAP版本不支援非活動資料報告時，此欄位中的值為「N/A」。
- 閾值策略：在此儲存物件上有效的使用者定義的效能閾值策略或策略。您可以將遊標放在包含省略號 (...) 的政策名稱上，以查看完整的策略名稱或已指派的策略名稱清單。指派效能閾值策略和清除效能閾值策略按鈕保持停用狀態，直到您透過點選最左側的複選框選擇一個或多個物件。請參閱以下連結以了解更多資訊：
 - ["為儲存物件指派效能閾值策略"](#)
 - ["從儲存物件中刪除效能閾值策略"](#)

效能：所有節點視圖

效能：所有節點視圖顯示 Unified Manager 實例所監控的每個節點的效能事件、資料和設定資訊概覽。這使您能夠快速監控節點的效能，並排除效能問題和閾值事件的故障。



Flash Cache Reads 傳回節點上由快取滿足的讀取操作的百分比，而不是從磁碟傳回的。只有在節點中安裝了 Flash Cache 模組時，才會顯示 Flash Cache 資料。

在「報告」功能表中，當 Unified Manager 及其管理的叢集安裝在沒有外部網路連線的網站時，會提供「硬體清單報告」選項。此按鈕產生一個 .csv 文件，其中包含叢集和節點資訊的完整清單；例如硬體型號和序號、磁碟類型和數量、已安裝的許可證等。此報告功能有助於在未連接到NetApp Active IQ平台的安全性網站內續約。您可以使用*指派效能閾值策略*和*清除效能閾值策略*按鈕為物件庫存頁面上的任何物件指派效能閾值策略或清除閾值策略。

請參閱以下連結以了解更多資訊：

- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)
- ["產生合約續約的硬體清單報告"](#)

效能：所有儲存虛擬機器視圖

效能：所有儲存虛擬機器視圖顯示由 Unified Manager 執行個體監控的每個儲存虛擬機器 (SVM) 的效能事件、資料和設定資訊概覽。這使您能夠快速監控 SVM 的效能，並解決效能問題和閾值事件。此頁面上的「延遲」欄位會報告所有 I/O 請求的平均回應時間，以每次操作的毫秒數表示。



此頁面上列出的 SVM 僅包括資料 SVM 和叢集 SVM。Unified Manager 不使用或顯示管理員或節點 SVM。

請參閱以下連結以了解更多資訊：

- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)

效能：所有 LUN 視圖

效能：所有 LUN 視圖顯示由 Unified Manager 實例監控的每個 LUN 的效能事件、資料和設定資訊概覽。這使您能夠快速監控 LUN 的效能，並排除效能問題和閾值事件的故障。

如果要分析特定物件的延遲和吞吐量，請點擊更多圖標 ，然後*分析工作負載*，您可以在*工作負載分析*頁面查看效能和容量圖表。

請參閱以下連結以了解更多資訊：

- ["監控一致性組關係中的 LUN"](#)
- ["配置 LUN"](#)
- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)
- ["查看同一 QoS 策略群組中的磁碟區或 LUN"。](#)
- ["查看應用於特定磁碟區或 LUN 的 QoS 原則群組設置"](#)
- ["使用 API 預配 LUN"](#)

效能：所有 NVMe 命名空間視圖

效能：所有 NVMe 命名空間視圖顯示由 Unified Manager 實例監控的每個 NVMe 命名空間的效能事件、資料和設定資訊概覽。這使您能夠快速監控命名空間的效能和健康狀況，並解決問題和閾值事件。

報告的資訊包括：命名空間的目前狀態。* 離線 - 不允許對命名空間進行讀取或寫入存取。* 線上 - 允許對命名空間進行讀寫存取。* NVFail - 由於NVRAM故障，命名空間自動離線。* 空間錯誤 - 命名空間已耗盡空間。

請參閱以下連結以了解更多資訊：

- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)

效能：所有網路介面視圖

效能：所有網路介面檢視顯示此 Unified Manager 實例監控的每個網路介面 (LIF) 的效能事件、資料和設定資訊

概覽。此頁面使您能夠快速監控介面的效能，並解決效能問題和閾值事件。以下是「效能：所有網路介面」視圖中的一些重要欄位。

- IOPS：每秒的輸入/輸出運算元。IOPS 不適用於 NFS LIF 和 CIFS LIF，並且對於這些類型顯示為 N/A。
- 延遲：所有 I/O 請求的平均回應時間，以每次操作的毫秒數表示。延遲不適用於 NFS LIF 和 CIFS LIF，並且對於這些類型顯示為 N/A。
- 主位置：介面的主位置，顯示為節點名稱和連接埠名稱，以冒號 (:) 分隔。如果位置顯示有省略號 (...), 您可以將遊標放在位置名稱上以查看完整位置。
- 目前位置：介面的目前位置，顯示為節點名稱和連接埠名稱，以冒號 (:) 分隔。如果位置顯示有省略號 (...), 您可以將遊標放在位置名稱上以查看完整位置。
- 角色：介面角色：資料、叢集、節點管理或叢集間。



此頁面上列出的介麵包括資料 LIF、叢集 LIF、節點管理 LIF 和叢集間 LIF。Unified Manager 不使用或顯示系統 LIF。

效能：所有連接埠視圖

效能：所有連接埠視圖顯示 Unified Manager 實例正在監控的每個連接埠的效能事件、資料和設定資訊概覽。這使您能夠快速監控連接埠的效能，並排除效能問題和閾值事件的故障。對於連接埠角色，顯示網路連接埠功能，即資料或叢集。FCP埠不能擁有角色，角色顯示為N/A。



僅顯示實體連接埠的效能計數器值。不顯示 VLAN 或介面組的計數器值。

請參閱以下連結以了解更多資訊：

- ["為儲存物件指派效能閾值策略"](#)
- ["從儲存物件中刪除效能閾值策略"](#)

效能：QoS 策略群組視圖

QoS 策略群組檢視顯示 Unified Manager 正在監控的叢集上可用的 QoS 策略群組。這包括傳統的 QoS 策略、自適應 QoS 策略和使用效能服務等級分配的 QoS 策略。

以下是效能：QoS 策略群組檢視中的一些重要欄位。

- QoS 策略群組：QoS 策略群組的名稱。對於已匯入 Unified Manager 9.7 或更高版本的 NetApp 服務等級管理器 (NSLM) 1.3 策略，此處顯示的名稱包括 SVM 名稱以及在 NSLM 中定義效能服務等級時名稱中沒有的其他資訊。例如，名稱「NSLM_vs6_Performance_2_0」表示這是在 SVM「vs6」上建立的 NSLM 系統定義的「效能」PSL 策略，預期延遲為「2 ms/op」。
- SVM：QoS 策略群組所屬的儲存虛擬機器 (SVM)。您可以按一下儲存虛擬機器名稱來導覽至該儲存虛擬機器的詳細資訊頁面。請注意，如果已在管理儲存虛擬機器上建立了 QoS 策略，則此欄位為空，因為此儲存虛擬機器類型代表叢集。
- 最小吞吐量：策略群組保證提供的最小吞吐量（以 IOPS 為單位）。對於自適應策略，這是根據儲存物件分配的大小分配給磁碟區或 LUN 的每 TB 的最小預期 IOPS。
- 最大吞吐量：策略群組不得超過的吞吐量（以 IOPS 和/或 MB/s 為單位）。當此欄位為空時，表示 ONTAP 中定義的最大吞吐量是無限的。對於自適應策略，這是分配給磁碟區或 LUN 的每 TB 的最大（峰值）可能 IOPS，基於儲存物件分配的大小或儲存物件使用的大小。

- 絕對最小 IOPS：對於自適應策略，這是絕對最小 IOPS 值，當預期 IOPS 小於此值時，用作覆蓋。
- 區塊大小：為 QoS 自適應策略指定的區塊大小。
- 最小分配：使用「分配空間」或「已使用空間」來決定最大吞吐量（峰值）IOPS。
- 預期延遲：儲存輸入/輸出操作的預期平均延遲。
- 共用：對於傳統的QoS策略，策略群組中定義的吞吐量值是否在多個物件之間共用。
- 關聯對象：指派給 QoS 策略群組的工作負載數量。您可以點選展開按鈕（▼）來查看有關該策略組的更多詳細資訊。
- 分配容量：QoS 策略群組中的物件目前正在使用的空間量。
- 關聯物件：指派給 QoS 策略群組的工作負載數量，分為磁碟區和 LUN。您可以按一下該數字以導覽至提供有關所選卷或 LUN 的更多詳細資訊的頁面。

更多資訊請參閱以下主題["使用 QoS 策略群組資訊管理效能"](#)。

優化績效清單頁面內容

效能物件的清單頁面包含可協助您最佳化物件清單資料內容的工具，讓您能夠快速輕鬆地找到特定資料。

效能物件庫存頁面中包含的資訊可能非常廣泛，通常跨越多個頁面。這種綜合數據非常適合監控、追蹤和提高效能；但是，定位特定數據需要工具來使您能夠快速找到您正在尋找的數據。因此，效能物件庫存頁面包含搜尋、排序和篩選功能。此外，搜尋和過濾可以協同工作以進一步縮小搜尋結果。

在對象庫存效能頁面上搜尋

您可以在物件清單效能頁面上搜尋字串。使用位於頁面右上角的「搜尋」欄位可以根據物件名稱或策略名稱快速定位資料。這使您能夠快速找到特定物件及其關聯數據，或快速找到策略並查看關聯的策略物件數據。

步

1. 根據您的搜尋要求，執行以下選項之一：

要找到這個...	輸入此...
特定對象	將物件名稱輸入到*搜尋*欄位中，然後按一下*搜尋*。將顯示您搜尋的對象及其相關資料。
使用者定義的效能閾值策略	將全部或部分政策名稱輸入到*搜尋*欄位中，然後按一下*搜尋*。將顯示指派給您搜尋的策略的物件。

在物件清單效能頁面上排序

您可以按任意列升序或降序對物件清單效能頁面上的所有資料進行排序。這使您能夠快速找到物件庫存數據，這在檢查效能或開始故障排除過程時很有幫助。

選定的要排序的列由突出顯示的列標題名稱和指示名稱右側排序方向的箭頭圖示表示。向上箭頭表示升序；向下

箭頭表示降序。預設排序順序是依*狀態*（事件嚴重性）降序排列，最關鍵的效能事件列在最前面。

步

1. 您可以按一下下列名來切換列的排序順序（升序或降序）。

根據所選列，物件清單效能頁面內容按升序或降序排序。

過濾物件清單效能頁面中的數據

您可以篩選物件清單效能頁面中的數據，以便根據特定條件快速找到數據。您可以使用篩選來縮小物件清單效能頁面的內容，以僅顯示您指定的結果。這提供了一種非常有效的方法，可以僅顯示您感興趣的性能數據。

您可以使用篩選面板根據您的喜好自訂網格視圖。可用的篩選選項是基於網格中查看的物件類型。如果目前套用了過濾器，則已套用的過濾器的數量將顯示在過濾器按鈕的右側。

支援三種類型的過濾參數。

範圍	驗證
字串（文字）	運算子包括*包含*、以...開頭、以...結尾*和*不包含*。
數位	運算子包括*大於*、小於、在最後*和*之間。
枚舉（文本）	運算子是 is 和 is not 。

每個篩選器都需要列、運算子和值欄位；可用的篩選器反映目前頁面上可篩選的列。您最多可以套用四個濾鏡。過濾結果基於組合過濾參數。過濾結果適用於過濾搜尋中的所有頁面，而不僅僅是目前顯示的頁面。

您可以使用過濾面板新增過濾器。

1. 在頁面頂部，按一下“過濾器”按鈕。顯示過濾面板。
2. 點擊左側下拉清單並選擇一個物件；例如，“Cluster”或效能計數器。
3. 按一下中心下拉列表，然後選擇要使用的運算子。
4. 在最後一個清單中，選擇或輸入一個值以完成該物件的篩選。
5. 若要新增另一個過濾器，請按一下「+新增過濾器」。顯示附加的過濾欄位。使用前面步驟中所述的程序完成此過濾器。請注意，新增第四個過濾器後，*+新增過濾器*按鈕不再顯示。
6. 按一下“套用過濾器”。過濾選項應用於網格，過濾器的數量顯示在過濾器按鈕的右側。
7. 使用過濾面板透過點擊要刪除的過濾器右側的垃圾桶圖示來刪除單個過濾器。
8. 若要刪除所有過濾器，請按一下過濾面板底部的“重設”。

過濾範例

該圖顯示了帶有三個過濾器的過濾面板。當您擁有的過濾器少於四個時，將顯示“+新增過濾器”按鈕。

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				<input type="button" value="Cancel"/> <input type="button" value="Apply Filter"/>

點擊“套用過濾器”後，“過濾”面板將關閉，套用過濾器，並顯示已套用的過濾器數量（ 3 ）。

了解 Unified Manager 將資料分層到雲端的建議

效能：所有磁碟區視圖顯示與非活動（冷）磁碟區上儲存的使用者資料大小相關的資訊。在某些情況下，Unified Manager 會識別某些卷，這些卷可以透過將非活動資料分層到啟用FabricPool的聚合的雲層（雲端提供者或StorageGRID）而受益。



FabricPool是在ONTAP 9.2 中引入的，因此如果您使用的是 9.2 之前的ONTAP軟體版本，則 Unified Manager 對分層資料的建議需要升級您的ONTAP軟體。此外， **auto** ONTAP 9.4 中引入了分層策略，並且 **all** 分層策略是在ONTAP 9.6 中引入的，因此如果建議使用自動分層策略，則必須升級到ONTAP 9.4 或更高版本。

效能：所有磁碟區視圖上的以下三個欄位提供有關是否可以透過將非活動資料移至雲層來提高儲存系統的磁碟使用率並節省效能層空間的資訊。

- 分層保單

分層策略決定磁碟區上的資料是否保留在效能層，或是否將部分資料從效能層移至雲層。

此欄位中的值表示在磁碟區上設定的分層策略，即使該磁碟區目前不駐留在FabricPool聚合上。只有當磁碟區位於FabricPool聚合上時，分層策略才會生效。

- 冷數據

冷資料顯示非活動（冷）磁碟區上儲存的使用者資料的大小。

只有在使用ONTAP 9.4 或更高版本的軟體時，此處才會顯示值，因為它要求部署磁碟區的聚合具有 **inactive data reporting parameter** 設定為 **enabled**，並且已達到最低冷卻天數閾值（對於使用 **snapshot-only** 或者 **auto** 分層策略）。否則，該值將被列為“`N/A`”。

- 雲端推薦

在擷取有關磁碟區上的資料活動的足夠資訊後，Unified Manager 可能會確定不需要採取任何行動，或者您可以透過將非活動資料分層到雲層來節省效能圖層上的空間。



冷資料欄位每 15 分鐘更新一次，但對磁碟區執行冷資料分析時雲端建議欄位每 7 天更新一次。因此，不同領域的冷數據的具體數量可能有所不同。雲端推薦欄位顯示運行分析的日期。

啟用非活動資料報告後，冷資料欄位將顯示非活動資料的確切數量。如果沒有非活動資料報告功能，Unified Manager 將使用效能統計資料來確定磁碟區上的資料是否為非活動狀態。在這種情況下，非活動資料量不會顯示在「冷資料」欄位中，但當您將遊標停留在單字「Tier」上以查看雲建議時，它會顯示出來。

您將看到的雲端建議是：

- 學習。尚未收集足夠的數據來提出建議。
- 等級。分析已確定該磁碟區包含非活動（冷）數據，並且您應該配置該磁碟區以將該資料移至雲層。在某些情況下，這可能會要求您先將磁碟區移至啟用FabricPool的聚合。在其他情況下，如果磁碟區已經位於FabricPool聚合上，您只需變更分層策略。
- 無動作。該磁碟區具有非常少的非活動數據，該磁碟區已設定為FabricPool聚合上的「自動」分層策略，或該磁碟區是資料保護磁碟區。當磁碟區處於離線狀態或在MetroCluster配置中使用時，也會顯示此值。

若要移動磁碟區、變更磁碟區分層策略或聚合非活動資料報告設置，請使用ONTAP System Manager、ONTAP CLI 指令或這些工具的組合。

如果您以應用程式管理員或儲存管理員角色登入 Unified Manager，則將遊標停留在單字 **Tier** 上時，雲端推薦中會出現 **Configure Volume** 連結。按一下此按鈕可開啟系統管理員中的磁碟區頁面以進行建議的變更。

使用效能資源管理器頁面監視效能

效能資源管理器頁面顯示有關叢集中每個物件的效能的詳細資訊。此頁面提供了所有叢集物件效能的詳細視圖，可讓您選擇和比較不同時間段內特定物件的效能資料。

您還可以評估所有物件的整體效能，並以並排格式比較物件效能資料。

了解根對象

根物件是與其他物件進行比較的基線。這使您能夠查看和比較來自其他物件的資料與根物件的數據，提供效能數據分析，幫助您排除故障並提高物件效能。

根物件名稱顯示在比較窗格的頂部。附加物件顯示在根物件下方。儘管您可以新增至比較窗格的附加物件的數量沒有限制，但只允許一個根物件。根物件的資料會自動顯示在計數器圖表窗格中的圖表中。

您無法變更根物件；它始終設定為您正在查看的物件頁面。例如，如果您開啟 Volume1 的 Volume Performance Explorer 頁面，則 Volume1 是根對象，無法變更。如果您想與不同的根物件進行比較，那麼您必須點擊物件的連結並開啟其登入頁面。



僅顯示根物件的事件和閾值。

應用篩選來減少網格中相關物件的列表

透過過濾，您可以在網格中顯示更小、定義更明確的物件子集。例如，如果網格中有 25 個卷，則透過過濾，您可以只查看吞吐量小於 90 MBps 或延遲大於 1 ms/op 的捲。

指定相關對象的時間範圍

效能資源管理器頁面上的時間範圍選擇器可讓您指定物件資料比較的時間範圍。指定時間

範圍可最佳化效能資源管理器頁面的內容，以僅顯示您指定的時間範圍內的物件資料。

細化時間範圍提供了一種有效的方法，可以僅顯示您感興趣的性能數據。您可以選擇預先定義的時間範圍或指定自訂時間範圍。預設時間範圍是前 72 小時。

選擇預定義的時間範圍

選擇預先定義的時間範圍是您在查看叢集物件效能資料時自訂和集中資料輸出的快速有效方法。選擇預先定義的時間範圍時，最多可獲得 13 個月的數據。

步驟

1. 在「效能資源管理器」頁面的右上角，按一下「時間範圍」。
2. 從「時間範圍選擇」面板的右側，選擇一個預先定義的時間範圍。
3. 按一下“應用範圍”。

指定自訂時間範圍

透過「效能資源管理器」頁面，您可以指定效能資料的日期和時間範圍。在細化叢集物件資料時，指定自訂時間範圍比使用預定義時間範圍具有更大的彈性。

您可以選擇一小時到 390 天之間的時間範圍。13 個月等於 390 天，因為每個月算 30 天。指定日期和時間範圍可提供更多詳細信息，並使您能夠放大特定的性能事件或一系列事件。指定時間範圍也有助於解決潛在的效能問題，因為指定日期和時間範圍可以更詳細地顯示效能事件周圍的資料。使用*時間範圍*控制項選擇預先定義的日期和時間範圍，或指定您自己的自訂日期和時間範圍（最長 390 天）。預先定義時間範圍的按鈕從*過去一小時*到*過去 13 個月*不等。

選擇「過去 13 個月」選項或指定超過 30 天的自訂日期範圍將顯示一個對話框，提醒您超過 30 天的時間段內顯示的效能資料是使用每小時平均值而不是 5 分鐘資料輪詢繪製的。因此，可能會出現時間軸視覺粒度的損失。如果您按一下對話方塊中的「不再顯示」選項，則當您選擇「過去 13 個月」選項或指定大於 30 天的自訂日期範圍時，不會出現該訊息。如果時間範圍包含距今超過 30 天的時間/日期，則摘要資料也適用於較小的時間範圍。

選擇時間範圍（自訂或預定義）時，30 天或更短的時間範圍是根據 5 分鐘間隔資料樣本。超過 30 天的時間範圍是基於一小時間隔的資料樣本。

From							To						
April 2015							April 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	01	02	03	04	29	30	31	01	02	03	04
05	06	07	08	09	10	11	05	06	07	08	09	10	11
12	13	14	15	16	17	18	12	13	14	15	16	17	18
19	20	21	22	23	24	25	19	20	21	22	23	24	25
26	27	28	29	30	01	02	26	27	28	29	30	01	02
03	04	05	06	07	08	09	03	04	05	06	07	08	09

Time: 6:00 am Time: 6:00 am

Last Hour
Last 24 Hours
Last 72 Hours
Last 7 Days
Last 30 Days
Last 13 Months
Custom Range

Cancel Apply Range

1. 按一下「時間範圍」下拉框，顯示「時間範圍」面板。

- 若要選擇預先定義的時間範圍，請按一下「時間範圍」面板右側的「最後...」按鈕之一。選擇預先定義的時間範圍時，最多可獲得 13 個月的數據。您選擇的預定義時間範圍按鈕將會反白顯示，並且相應的日期和時間將顯示在行事曆和時間選擇器中。
- 若要選擇自訂日期範圍，請按一下左側「從」行事曆中的開始日期。按一下 < 或 > 可在日曆中向前或向後導覽。若要指定結束日期，請按一下右側「至」行事曆中的日期。請注意，預設結束日期是今天，除非您指定其他結束日期。時間範圍面板右側的「自訂範圍」按鈕會反白顯示，表示您已選擇自訂日期範圍。
- 若要選擇自訂時間範圍，請按一下「從」行事曆下方的「時間」控制項並選擇開始時間。若要指定結束時間，請按一下右側「至」日曆下方的「時間」控件，然後選擇結束時間。時間範圍面板右側的「自訂範圍」按鈕會反白顯示，表示您已選擇自訂時間範圍。
- 或者，您可以在選擇預定義日期範圍時指定開始時間和結束時間。選擇前面所述的預定義日期範圍，然後按前面描述選擇開始和結束時間。選定的日期在日曆中突出顯示，您指定的開始和結束時間顯示在*時間*控制項中，並且*自訂範圍*按鈕突出顯示。
- 選擇日期和時間範圍後，按一下*套用範圍*。此時間範圍的效能統計資料顯示在圖表和事件時間軸中。

定義用於比較圖表的相關物件列表

您可以在計數器圖表窗格中定義相關物件的列表，以進行資料和效能比較。例如，如果您的儲存虛擬機器 (SVM) 遇到效能問題，您可以比較 SVM 中的所有磁碟區以確定哪個磁碟區可能導致該問題。


您可以將相關物件網格中的任何物件新增至比較和計數器圖表窗格。這使您可以查看和比較多個物件以及根物件的資料。您可以在相關物件網格中新增和刪除物件；但是，比較窗格中的根物件是不可刪除的。



在比較窗格中新增許多物件可能會對效能產生負面影響。為了保持效能，您應該選擇有限數量的圖表進行資料比較。

步驟

- 在物件網格中，找到要新增的對象，然後按一下「新增」按鈕。

*新增*按鈕變為灰色，並且該物件被新增至比較窗格中的附加物件清單中。物件的資料被加入到計數器圖表窗格中的圖表中。物件的眼睛圖示的顏色 () 與圖表中物件資料趨勢線的顏色相符。

- *可選*：*隱藏或顯示選定物件的資料*：

要做到這一點...	採取此行動...
隱藏選取的對象	點選所選物件的眼睛圖示 () 在比較窗格中。該物件的資料被隱藏，並且該物件的眼睛圖示變為灰色。
顯示隱藏的對象	按一下比較窗格中所選物件的灰色眼睛圖示。 眼睛圖示恢復其原始顏色，並且物件資料被重新添加到計數器圖表窗格中的圖表中。

- *可選*：*從*比較*窗格中刪除選取的物件*：

要做到這一點...	採取此行動...
移除選取的對象	將滑鼠懸停在比較窗格中選取物件的名稱上以顯示刪除物件按鈕 (X)，然後按一下該按鈕。該物件將從比較窗格中刪除，並且其資料將從計數器圖表中清除。
移除所有選取的對象	按一下比較窗格頂部的刪除所有物件的按鈕 (X)。所有選取的物件及其資料都將被刪除，只留下根物件。

了解計數器圖表

計數器圖表窗格中的圖表可讓您查看和比較根物件和從相關物件網格中新增的物件的效能資料。這可以幫助您了解效能趨勢並隔離和解決效能問題。

預設顯示的計數器圖表是事件、延遲、IOPS 和 MBps。您可以選擇顯示的選用圖表包括利用率、已使用效能容量、可用 IOPS、IOPS/TB 和快取未命中率。此外，您還可以選擇查看延遲、IOPS、MBps 和已使用效能容量圖表的總值或細分值。

效能資源管理器預設顯示某些計數器圖表；無論儲存物件是否全部支援它們。當計數器不受支援時，計數器圖表為空，且訊息 `Not applicable for <object>` 將顯示。

圖表顯示根物件和您在比較窗格中選擇的所有物件的效能趨勢。各圖表資料排列如下：

- **X軸**

顯示指定的時間段。如果您未指定時間範圍，則預設為前 72 小時。

- **Y軸**

顯示選取物件或物件獨有的計數器單位。

趨勢線顏色與比較窗格中顯示的物件名稱顏色相符。您可以將遊標放在任何趨勢線上的某個點上，以查看該點的時間和值的詳細資訊。

如果要調查圖表中的特定時間段，可以使用以下方法之一：

- 使用 < 按鈕展開計數器圖表窗格以跨越頁面寬度。
- 使用遊標（當它變成放大鏡時）選擇圖表中時間範圍的一部分來聚焦和放大該區域。您可以按一下「重設圖表縮放」將圖表恢復到預設時間範圍。
- 使用「縮放視圖」按鈕顯示包含擴展詳細資訊和閾值指標的大型單一計數器圖表。



有時，趨勢線會出現缺口。差距意味著 Unified Manager 無法從儲存系統收集效能數據，或者 Unified Manager 可能已關閉。

效能計數器圖表的類型

有標準效能圖表顯示所選儲存物件的計數器值。每個細分計數器圖表顯示分為讀取、寫入和其他類別的總值。此外，當圖表以縮放視圖顯示時，一些細分計數器圖表會顯示更多詳細資訊。

下表顯示了可用的效能計數器圖表。

可用圖表	圖表描述
活動	顯示與根物件的統計圖表相關的嚴重、錯誤、警告和資訊事件。除了性能事件之外，還顯示健康事件，以提供性能可能受到影響的原因的完整情況。
延遲 - 總計	響應應用程式請求所需的毫秒數。請注意，平均延遲值是 I/O 加權的。
延遲 - 細分	「延遲總計」中顯示相同的訊息，但效能資料分為讀取、寫入和其他延遲。只有當選取的物件是 SVM、節點、聚合、磁碟區、LUN 或命名空間時，此圖表選項才適用。
延遲 - 集群組件	「延遲總計」中顯示相同的訊息，但效能數據依集群組件分為延遲。此圖表選項僅當選取物件為體積時才適用。
IOPS - 總計	每秒處理的輸入/輸出運算元。當顯示某個節點時，選擇「總計」將顯示透過此節點移動的資料的 IOPS，這些資料可能駐留在本地或遠端節點上，而選擇「總計（本地）」將顯示僅駐留在目前節點上的資料的 IOPS。
IOPS - 細分	<p>IOPS Total 顯示相同的訊息，但效能資料分為讀取、寫入和其他 IOPS。只有當選取的物件是 SVM、節點、聚合、磁碟區、LUN 或命名空間時，此圖表選項才適用。</p> <p>當在縮放檢視中顯示時，磁碟區圖表會顯示 QoS 最小和最大吞吐量值（如果在 ONTAP 中配置）。</p> <p>當顯示某個節點時，選擇「細分」將顯示透過此節點移動的資料的 IOPS 細分，這些資料可能會駐留在本地或遠端節點上，而選擇「細分（本地）」將顯示僅駐留在目前節點上的資料的 IOPS 細分。</p>
IOPS - 協議	IOPS Total 顯示相同的訊息，但效能資料分為 CIFS、NFS、FCP、NVMe 和 iSCSI 協定流量的單獨圖表。此圖表選項僅當選取的物件是 SVM 時才適用。

可用圖表	圖表描述
IOPS/TB - 總計	<p>根據工作負載所佔用的總空間，每秒處理的輸入/輸出操作數（以 TB 為單位）。此計數器也稱為 I/O 密度，用於衡量給定儲存容量可以提供多少效能。如果在 ONTAP 中配置，則在縮放檢視中顯示磁碟區圖表會顯示 QoS 預期值和峰值吞吐量值。</p> <p>此圖表選項僅當選取物件為體積時才適用。</p>
MB/s - 總計	<p>每秒傳輸到物件和從物件傳輸的資料（兆位元組數）。</p>
MB/s - 細分	<p>MB/s 圖表中顯示相同的訊息，但吞吐量資料分為磁碟讀取、快閃記憶體讀取、寫入和其他。當在縮放檢視中顯示時，磁碟區圖表會顯示 QoS 最大吞吐量值（如果在 ONTAP 中配置）。</p> <p>只有當選取的物件是 SVM、節點、聚合、磁碟區、LUN 或命名空間時，此圖表選項才適用。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>只有在節點中安裝了 Flash Cache 模組時，才會顯示 Flash Cache 資料。</p> </div>
已使用的效能容量 - 總計	<p>節點或聚合所消耗的效能容量百分比。</p>
已使用性能容量 - 明細	<p>效能容量所使用的資料分為使用者協定和系統後台進程。此外，還顯示了可用的效能容量。</p>
可用 IOPS - 總計	<p>此物件上目前可用（免費）的每秒輸入/輸出操作數。此數字是從 Unified Manager 計算的物件可以執行的總 IOPS 中減去目前使用的 IOPS 的結果。僅當選取的物件是節點或聚合時，此圖表選項才適用。</p>
利用率 - 總計	<p>正在使用的物件的可用資源百分比。利用率表示節點的節點利用率、聚合的磁碟利用率和連接埠的頻寬利用率。此圖表選項僅當選定的物件是節點、聚合或連接埠時才適用。</p>
快取未命中率 - 總計	<p>來自客戶端應用程式的讀取請求中從磁碟返回而不是從快取返回的百分比。此圖表選項僅當選取物件為體積時才適用。</p>

選擇要顯示的效能圖表

透過「選擇圖表」下拉列表，您可以選擇要在「計數器圖表」窗格中顯示的效能計數器圖表的類型。這使您能夠根據效能要求查看特定的資料和計數器。

步驟

1. 在「計數器圖表」窗格中，按一下「選擇圖表」下拉清單。
2. 新增或刪除圖表：

到...	這樣做...
新增或刪除單一圖表	按一下要顯示或隱藏的圖表旁的複選框
新增所有圖表	點擊“全選”
刪除所有圖表	點擊*取消全選*

您選擇的圖表將顯示在計數器圖表窗格中。請注意，當您新增圖表時，新圖表將插入到「計數器圖表」窗格中，以符合「選擇圖表」下拉清單中列出的圖表的順序。選擇其他圖表可能需要額外滾動。

展開計數器圖表窗格

您可以展開計數器圖表窗格，以便圖表更大且更易讀。

定義計數器的比較物件和時間範圍後，您可以查看更大的計數器圖表窗格。您可以使用效能資源管理器視窗中間的 < 按鈕來展開窗格。

步

1. 展開或縮小*計數器圖表*窗格。

到...	這樣做...
擴展計數器圖表窗格以適合頁面寬度	點擊 < 按鈕
將計數器圖表窗格縮小到頁面的右半部分	點擊 > 按鈕

將計數器圖表焦點變更為較短的時間段

您可以使用滑鼠縮小時間範圍，以在計數器圖表窗格或計數器圖表縮放檢視視窗中專注於特定時間段。這使您能夠更細緻、更微觀地查看效能資料、事件和閾值的時間軸的任何部分。

開始之前

遊標必須變成放大鏡才能表示此功能處於活動狀態。



當使用此功能時，它會改變時間軸以顯示與更精細的顯示相對應的值，*時間範圍*選擇器上的時間和日期範圍不會從圖表的原始值變化。

步驟

1. 若要放大特定時間段，請使用放大鏡點擊並拖曳滑鼠以反白您想要詳細查看的區域。

您選擇的時間段內的計數器值填入計數器圖表。

- 若要返回*時間範圍*選擇器中設定的原始時間段，請點選*重設圖表縮放*按鈕。

計數器圖表以其原始狀態顯示。

在事件時間軸中查看事件詳細信息

您可以在效能資源管理器的事件時間軸窗格中查看所有事件及其相關詳細資訊。這是一種快速有效的方法，可以查看指定時間範圍內根物件上發生的所有健康和效能事件，這在解決效能問題時很有幫助。

事件時間軸窗格顯示在選定時間範圍內在根物件上發生的關鍵、錯誤、警告和資訊事件。每個事件嚴重程度都有自己的時間表。單一事件和多個事件由時間線上的事件點表示。您可以將遊標放在事件點上以查看事件詳細資訊。為了增加多個事件的視覺粒度，您可以減少時間範圍。這會將多個事件分散為單一事件，使您能夠單獨查看和調查每個事件。

事件時間線上的每個效能事件點與事件時間線下方顯示的計數器圖表趨勢線中的相應峰值垂直排列。這提供了事件和整體表現之間的直接視覺關聯。健康事件也會顯示在時間線上，但這些類型的事件不一定與表現圖表之一中的峰值一致。

步驟

- 在「事件時間軸」窗格上，將遊標放在時間線上的事件點上，以查看該事件點的事件摘要。

彈出對話方塊顯示有關事件類型、事件發生的日期和時間、狀態和事件持續時間的資訊。

- 查看一個或多個事件的完整事件詳情：

要做到這一點...	點擊此處...
查看單一事件的詳細信息	在彈出對話框中*查看事件詳情*。
查看多個事件的詳細信息	在彈出對話框中*查看事件詳情*。  按一下多個事件對話方塊中的單一事件將顯示對應的事件詳細資訊頁面。

計數器圖表縮放視圖

計數器圖表提供縮放視圖，使您能夠放大指定時間段內的效能詳細資訊。這使您能夠以更高的粒度查看效能詳細資訊和事件，這在解決效能問題時非常有用。

當以縮放視圖顯示時，某些細分圖表會提供比圖表未以縮放視圖顯示時顯示的資訊更多的資訊。例如，如果在ONTAP中設定了磁碟區和 LUN 的 QoS 策略值，則 IOPS、IOPS/TB 和 MBps 細分圖縮放檢視頁面將顯示這些值。



對於系統定義的效能閾值策略，*策略*清單中只有「節點資源過度利用」和「QoS 吞吐量限制突破」策略可用。其他系統定義的閾值策略目前無法使用。

顯示計數器圖表縮放視圖

計數器圖表縮放視圖為所選計數器圖表及其相關時間軸提供了更精細的細節。這會放大計數器圖表數據，使您能夠更清晰地了解效能事件及其根本原因。

您可以顯示任何計數器圖表的計數器圖表縮放檢視。

步驟

1. 按一下「縮放檢視」以在新瀏覽器視窗中開啟選定的圖表。
2. 如果您正在查看細分圖表，然後按一下“縮放檢視”，細分圖表將以縮放檢視顯示。如果您想要變更檢視選項，可以在「縮放檢視」中選擇「總計」。

在縮放視圖中指定時間範圍

計數器圖表縮放檢視視窗中的「時間範圍」控制項可讓您為所選圖表指定日期和時間範圍。這使您能夠根據預設的時間範圍或您自己的自訂時間範圍快速找到特定資料。

您可以選擇一小時到 390 天之間的時間範圍。13 個月等於 390 天，因為每個月算 30 天。指定日期和時間範圍可提供更多詳細信息，並使您能夠放大特定的性能事件或一系列事件。指定時間範圍也有助於解決潛在的效能問題，因為指定日期和時間範圍可以更詳細地顯示效能事件周圍的資料。使用*時間範圍*控制項選擇預先定義的日期和時間範圍，或指定您自己的自訂日期和時間範圍（最長 390 天）。預先定義時間範圍的按鈕從*過去一小時*到*過去 13 個月*不等。

選擇「過去 13 個月」選項或指定超過 30 天的自訂日期範圍將顯示一個對話框，提醒您超過 30 天的時間段內顯示的效能資料是使用每小時平均值而不是 5 分鐘資料輪詢繪製的。因此，可能會出現時間軸視覺粒度的損失。如果您按一下對話方塊中的「不再顯示」選項，則當您選擇「過去 13 個月」選項或指定大於 30 天的自訂日期範圍時，不會出現該訊息。如果時間範圍包含距今超過 30 天的時間/日期，則摘要資料也適用於較小的時間範圍。

選擇時間範圍（自訂或預定義）時，30 天或更短的時間範圍是根據 5 分鐘間隔資料樣本。超過 30 天的時間範圍是基於一小時間隔的資料樣本。

From							To						
April 2015							April 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	01	02	03	04	29	30	31	01	02	03	04
05	06	07	08	09	10	11	05	06	07	08	09	10	11
12	13	14	15	16	17	18	12	13	14	15	16	17	18
19	20	21	22	23	24	25	19	20	21	22	23	24	25
26	27	28	29	30	01	02	26	27	28	29	30	01	02
03	04	05	06	07	08	09	03	04	05	06	07	08	09

Time: 6:00 am

Time: 6:00 am

- Last Hour
- Last 24 Hours
- Last 72 Hours
- Last 7 Days
- Last 30 Days
- Last 13 Months
- Custom Range

Cancel Apply Range

1. 按一下「時間範圍」下拉框，顯示「時間範圍」面板。
2. 若要選擇預先定義的時間範圍，請按一下「時間範圍」面板右側的「最後...」按鈕之一。選擇預先定義的時間範圍時，最多可獲得 13 個月的數據。您選擇的預定義時間範圍按鈕將會反白顯示，並且相應的日期和時間將顯示在行事曆和時間選擇器中。

3. 若要選擇自訂日期範圍，請按一下左側「從」行事曆中的開始日期。按一下 < 或 > 可在日曆中向前或向後導覽。若要指定結束日期，請按一下右側「至」行事曆中的日期。請注意，預設結束日期是今天，除非您指定其他結束日期。時間範圍面板右側的「自訂範圍」按鈕會反白顯示，表示您已選擇自訂日期範圍。
4. 若要選擇自訂時間範圍，請按一下「從」行事曆下方的「時間」控制項並選擇開始時間。若要指定結束時間，請按一下右側「至」日曆下方的「時間」控件，然後選擇結束時間。時間範圍面板右側的「自訂範圍」按鈕會反白顯示，表示您已選擇自訂時間範圍。
5. 或者，您可以在選擇預定義日期範圍時指定開始時間和結束時間。選擇前面所述的預定義日期範圍，然後按前面描述選擇開始和結束時間。選定的日期在日曆中突出顯示，您指定的開始和結束時間顯示在*時間*控制項中，並且*自訂範圍*按鈕突出顯示。
6. 選擇日期和時間範圍後，按一下*套用範圍*。此時間範圍的效能統計資料顯示在圖表和事件時間軸中。

在計數器圖表縮放視圖中選擇效能閾值

在計數器圖表縮放視圖中套用閾值可提供效能閾值事件發生的詳細視圖。這使您能夠應用或刪除閾值，並立即查看結果，這在決定下一步是否進行故障排除時很有幫助。

在計數器圖表縮放視圖中選擇閾值可讓您查看有關效能閾值事件的精確資料。您可以套用計數器圖表縮放視圖的*策略*區域下出現的任何閾值。

每次只能將一個策略套用到計數器圖表縮放檢視中的物件。

步

1. 選擇或取消選擇  與政策相關的。

所選閾值將應用於計數器圖表縮放視圖。臨界閾值顯示為紅線；警告閾值顯示為黃線。

按集群組件查看卷延遲


您可以使用磁碟區效能資源管理器頁面查看磁碟區的詳細延遲資訊。延遲 - 總計數器圖表顯示磁碟區上的總延遲，延遲 - 細分計數器圖表有助於確定讀寫延遲對磁碟區的影響。

此外，「延遲 - 群集組件」圖表顯示了每個群集組件的延遲的詳細比較，以幫助確定每個組件對卷的總延遲的貢獻。將顯示以下集群組件：

- 網路
- QoS 限制最大值
- QoS 限制最小值
- 網路處理
- 集群互連
- Data Processing
- 聚合操作
- 大量啟用設定
- MetroCluster資源
- 雲延遲

- 同步SnapMirror

步驟

1. 在您選擇的磁碟區的「磁碟區效能資源管理器」頁面中，從延遲圖表的下拉式功能表中選擇「叢集元件」。
顯示延遲 - 叢集組件圖表。
2. 若要查看圖表的較大版本，請選擇「縮放檢視」。
顯示集群組件比較圖。您可以透過取消選擇或選擇  與每個集群組件相關聯的。
3. 若要查看特定值，請將遊標移到圖表區域以查看彈出視窗。


按協定查看 SVM IOPS 流量

您可以使用效能/SVM 資源管理器頁面查看 SVM 的詳細 IOPS 資訊。IOPS - 總計計數器圖表顯示 SVM 上的總 IOPS 使用情況，而 IOPS - 細分計數器圖表有助於確定讀取、寫入和其他 IOPS 對 SVM 的影響。

此外，IOPS - 協定圖表顯示了 SVM 上使用的每種協定的 IOPS 流量的詳細比較。可用的協定如下：

- CIFS
- NFS
- FCP
- iSCSI
- NVMe光纖通道

步驟

1. 在您選擇的 SVM 的「效能/SVM 資源管理器」頁面中，從 IOPS 圖表的下拉式功能表中選擇「協定」。
顯示 IOPS - 協定圖表。
2. 若要查看圖表的較大版本，請選擇「縮放檢視」。
顯示IOPS高階協定比較圖。您可以透過取消選擇或選擇  與協議相關。
3. 若要查看具體值，請將遊標移到任一圖表的圖表區域以查看彈出視窗。

查看捲和 LUN 延遲圖表以驗證效能保證

您可以查看已訂閱「效能保證」計畫的捲和 LUN，以驗證延遲是否未超過您所保證的水平。

延遲效能保證是每次操作一毫秒的值，不應超過該值。它基於每小時平均值，而不是預設的五分鐘效能收集期。

步驟

1. 在「效能：所有磁碟區」檢視或「效能：所有 LUN」檢視中，選擇您感興趣的磁碟區或 LUN。
2. 在您選擇的磁碟區或 LUN 的效能資源管理器頁面中，從 查看統計資料 選擇器中選擇 每小時平均值。

隨著五分鐘收集的數據被每小時平均值取代，延遲圖表中的水平線將顯示更平滑的線。

3. 如果同一聚合上還有其他磁碟區處於效能保證之下，則可以新增這些磁碟區以在同一圖表中查看其延遲值。

查看所有 SAN 陣列叢集的效能

您可以使用效能：所有叢集視圖來顯示所有 SAN 陣列叢集的效能狀態。

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。

您可以在「效能：所有叢集」視圖中查看所有 SAN 陣列叢集的概述信息，並在「叢集/效能資源管理器」頁面中查看詳細資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 確保「個性」列顯示在*健康：所有群集*視圖中，或使用*顯示/隱藏*控制項新增它。

此列顯示您的所有 SAN 陣列叢集的「所有 SAN 陣列」。

3. 要查看有關這些集群的性能信息，請選擇“性能：所有集群”視圖。

查看全 SAN 陣列叢集的效能資訊。

4. 要查看有關這些叢集的效能的詳細信息，請按一下所有 SAN 陣列叢集的名稱。
5. 按一下“資源管理器”標籤。
6. 在*叢集/效能資源管理器*頁面上，從*檢視和比較*選單中選擇*此叢集上的節點*。

您可以比較此叢集上兩個節點的效能統計數據，以確保兩個節點上的負載幾乎相同。如果兩個節點之間存在很大差異，您可以將第二個節點新增至圖表中，並比較較長時間範圍內的值以識別任何配置問題。

根據僅駐留在本機節點上的工作負載查看節點 IOPS

節點 IOPS 計數器圖表可以突出顯示操作僅透過本地節點使用網路 LIF 對遠端節點上的磁碟區執行讀取/寫入操作的位置。IOPS - 「總計（本地）」和「細分（本地）」圖表顯示僅駐留在目前節點上的本機磁碟區中的資料的 IOPS。

這些計數器圖表的「本地」版本與效能容量和使用率的節點圖表類似，因為它們也僅顯示駐留在本機磁碟區上的資料的統計資料。

透過將這些計數器圖表的「本機」版本與這些計數器圖表的常規總版本進行比較，您可以看到是否有大量流量透過本機節點移動以存取遠端節點上的磁碟區。如果有太多操作透過本地節點到達遠端節點上的捲，這種情況可能會導致效能問題，可能表現為節點利用率高。在這些情況下，您可能想要將磁碟區移至本機節點，或在遠端節點上建立 LIF，以便可以連接存取該磁碟區的主機的流量。

步驟

1. 在所選節點的「效能/節點資源管理器」頁面中，從 IOPS 圖表的下拉式選單中選擇「總計」。

顯示 IOPS - 總計圖表。

2. 按一下「縮放檢視」可在新瀏覽器標籤中顯示圖表的較大版本。
3. 返回「效能/節點資源管理器」頁面，從 IOPS 圖表的下拉式選單中選擇「總計（本機）」。

顯示 IOPS - 總計（本地）圖表。

4. 按一下「縮放檢視」可在新瀏覽器標籤中顯示圖表的較大版本。
5. 查看兩個圖表並排查看，並確定 IOPS 值看起來差異很大的區域。
6. 將遊標移到這些區域上，以比較特定時間點的本地和總 IOPS。

物件登陸頁的元件

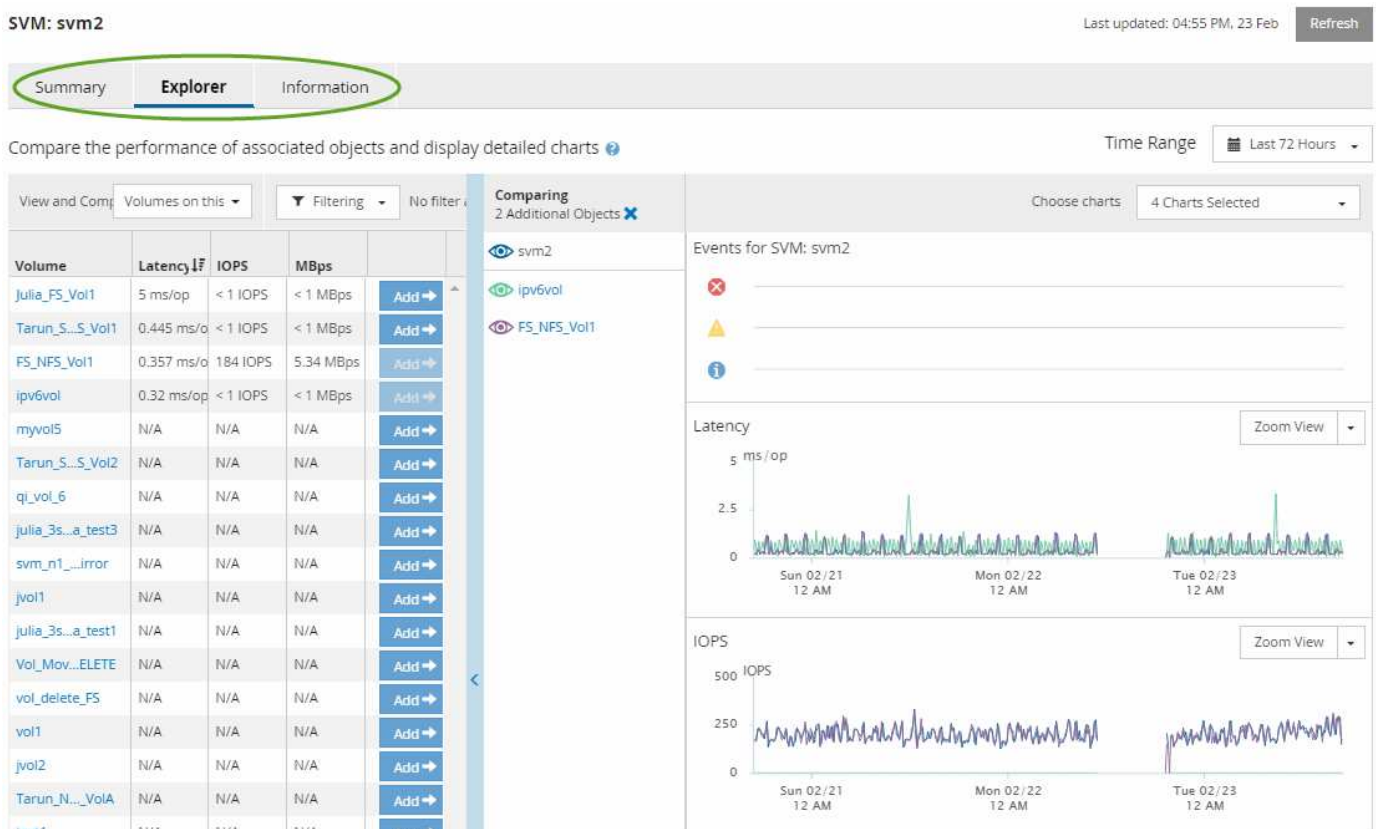
物件登陸頁面提供有關所有關鍵、警告和資訊事件的詳細資訊。它們提供了所有叢集物件效能的詳細視圖，使您能夠選擇和比較不同時間段內的單一物件。

物件登入頁面可讓您檢查所有物件的整體效能，並以並排格式比較物件效能資料。這在評估效能和排除事件故障時非常有用。



計數器摘要面板和計數器圖表中顯示的數據是基於五分鐘的採樣間隔。頁面左側的物件清單網格中顯示的資料是基於一小時的採樣間隔。

下圖顯示了顯示資源管理器資訊的物件登入頁面的範例：



根據正在檢視的儲存對象，對象登入頁面可以具有以下選項卡，提供有關該對象的效能資料：

- 總結

顯示三個或四個計數器圖表，其中包含前 72 小時內每個物件的事件和效能，包括顯示該期間高值和低值的趨勢線。

- 探險家

顯示與目前物件相關的儲存物件網格，可讓您將目前物件的效能值與相關物件的效能值進行比較。此標籤包含最多 11 個計數器圖表和一個時間範圍選擇器，可讓您執行各種比較。

- 資訊

顯示有關儲存物件的非效能配置屬性的值，包括已安裝的ONTAP軟體版本、HA 合作夥伴名稱以及連接埠和 LIF 的數量。

- 最佳表現者

對於叢集：根據您選擇的效能計數器，顯示具有最高效能或最低效能的儲存物件。

- 故障轉移規劃

對於節點：顯示如果節點的 HA 夥伴發生故障，對節點效能造成的影響的估計。

- 細節

對於磁碟區：顯示選定磁碟區工作負載的所有 I/O 活動和操作的詳細效能統計資料。此標籤適用於FlexVol磁碟區、FlexGroup磁碟區和 FlexGroups 的組成部分。

摘要頁面

摘要頁面顯示計數器圖表，其中包含前 72 小時內每個物件的事件和效能的詳細資訊。資料不會自動刷新，但截至上次頁面載入時是最新資料。摘要頁面中的圖表回答了「我需要進一步了解嗎？」這個問題

圖表和計數器統計

摘要圖表提供了過去 72 小時內的快速、進階概覽，並幫助您識別可能需要進一步調查的問題。

摘要頁面計數器統計資訊以圖表形式顯示。

您可以將遊標放在圖表中的趨勢線上，以查看特定時間點的計數器值。摘要圖表也顯示以下計數器在前 72 小時內的活動嚴重和警告事件的總數：

- 延遲

所有 I/O 請求的平均回應時間；以每次操作的毫秒數表示。

顯示所有物件類型。

- 每秒輸入/輸出次數

平均運轉速度；以每秒的輸入/輸出操作表示。

顯示所有物件類型。

- **MB/秒**

平均吞吐量；以每秒兆位元組表示。

顯示所有物件類型。

- 已使用的性能容量

節點或聚合所消耗的效能容量百分比。

僅對節點和聚合顯示。

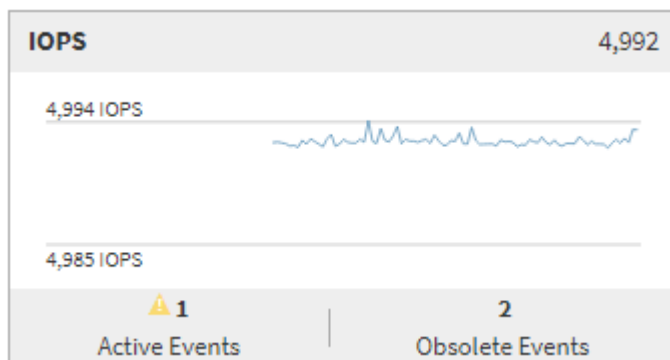
- 利用率

節點和聚合的物件利用率百分比，或連接埠的頻寬利用率。

僅顯示節點、聚合和連接埠。

將遊標定位在活動事件的事件計數上會顯示事件的類型和數量。關鍵事件以紅色顯示 (■)，警告事件顯示為黃色 (■)。

圖表右上角灰色條中的數字是過去 72 小時內的平均值。趨勢線圖底部和頂部顯示的數字是過去 72 小時內的最小值和最大值。圖表下方的灰色條包含過去 72 小時內活動事件（新事件和已確認事件）和過時事件的數量。



- 延遲計數器圖表

延遲計數器圖表提供了前 72 小時內物件延遲的進階概覽。延遲是指所有 I/O 請求的平均回應時間；以每個操作的毫秒數表示，即所考慮的叢集儲存元件中的資料包或區塊所經歷的服務時間、等待時間或兩者。

*頂部（計數器值）：*標題中的數字顯示前 72 小時的平均值。

*中（表現圖）：*圖表底部的數字顯示最低延遲，圖表頂部的數字顯示前 72 小時內的最高延遲。將遊標放在圖形趨勢線上以查看特定時間的延遲值。

*底部（事件）：*懸停時，彈出視窗顯示事件的詳細資訊。點擊圖表下方的“活動事件”鏈接，導航至“事件清單”頁面以查看完整的事件詳細資訊。

- **IOPS 計數器圖表**

IOPS 計數器圖表提供了前 72 小時內物件 IOPS 健康狀況的進階概覽。IOPS 表示儲存系統每秒輸入/輸出操作次數的速度。

*頂部（計數器值）：*標題中的數字顯示前 72 小時的平均值。

*中間（性能圖）：*圖表底部的數字顯示最低 IOPS，圖表頂部的數字顯示前 72 小時內的最高 IOPS。將遊標放在圖形趨勢線上以查看特定時間的 IOPS 值。

*底部（事件）：*懸停時，彈出視窗顯示事件的詳細資訊。點擊圖表下方的“活動事件”鏈接，導航至“事件清單”頁面以查看完整的事件詳細資訊。

• MB/s 計數器圖表

MB/s 計數器圖表顯示物件 MB/s 效能，並指示每秒有多少資料以兆位元組為單位傳輸到物件和從物件傳輸出去。MB/s 計數器圖表提供了前 72 小時內物件 MB/s 健康狀況的進階概覽。

*頂部（計數器值）：*標題中的數字顯示前 72 小時內的平均 MB/s 數。

*中（表現圖）：*圖表底部的值顯示最低的 MB/s 數，圖表頂部的值顯示前 72 小時內最高的 MB/s 數。將遊標放在圖形趨勢線上，即可查看特定時間的 MB/s 值。

*底部（事件）：*懸停時，彈出視窗顯示事件的詳細資訊。點擊圖表下方的“活動事件”鏈接，導航至“事件清單”頁面以查看完整的事件詳細資訊。

• 性能容量已用計數器圖表

已用性能容量計數器圖表顯示物件所消耗的性能容量百分比。

*頂部（計數器值）：*標題中的數字顯示前 72 小時內平均使用的效能容量。

*中（性能圖）：*圖表底部的值顯示最低使用的性能容量百分比，圖表頂部的值顯示前 72 小時內最高的使用的性能容量百分比。將遊標放在圖形趨勢線上，即可查看特定時間內已使用的效能容量值。

*底部（事件）：*懸停時，彈出視窗顯示事件的詳細資訊。點擊圖表下方的“活動事件”鏈接，導航至“事件清單”頁面以查看完整的事件詳細資訊。

• 利用率計數器圖表

利用率計數器圖表顯示物件利用率百分比。利用率計數器圖表提供了前 72 小時內物件或頻寬利用率百分比的進階概覽。

*頂部（計數器值）：*標題中的數字顯示前 72 小時的平均使用率百分比。

*中間（效能圖）：*圖表底部的數值顯示最低利用率百分比，圖表頂部的數值顯示前 72 小時內的最高利用率百分比。將遊標放在圖形趨勢線上即可查看特定時間的使用率值。

*底部（事件）：*懸停時，彈出視窗顯示事件的詳細資訊。點擊圖表下方的“活動事件”鏈接，導航至“事件清單”頁面以查看完整的事件詳細資訊。

活動

事件歷史記錄表（如適用）列出了該物件上發生的最新事件。按一下事件名稱可在「事件詳細資料」頁面上顯示該事件的詳細資料。

效能資源管理器頁面的元件

透過「效能資源管理器」頁面，您可以比較叢集中類似物件的效能 - 例如，叢集中的所有磁碟區。這在排除效能事件故障和微調物件效能時非常有用。您也可以將物件與根物件進行比較，根物件是進行其他物件比較的基線。

您可以按一下「切換到健康視圖」按鈕來顯示此物件的健康詳細資料頁面。在某些情況下，您可以了解有關此物件的儲存配置設定的重要信息，這可能有助於解決問題。

效能資源管理器頁面顯示叢集物件及其效能資料的清單。此頁面以表格形式顯示相同類型的所有群集物件（例如，磁碟區及其特定於物件的效能統計資料）。此視圖提供了叢集物件效能的有效概覽。



如果表格中的任何儲存格中出現“N/A”，則表示該計數器的值不可用，因為此時該物件上沒有 I/O。

效能資源管理器頁面包含以下元件：

- 時間範圍

使您能夠選擇物件資料的時間範圍。

您可以選擇預先定義的範圍，或指定您自己的自訂時間範圍。

- 查看並比較

使您能夠選擇在網格中顯示哪種類型的相關物件。

可用的選項取決於根物件類型及其可用資料。您可以按一下「檢視和比較」下拉清單來選擇物件類型。您選擇的物件類型將顯示在清單中。

- 過濾

使您能夠根據自己的喜好縮小接收的資料量。

您可以建立適用於物件資料的篩選器 - 例如，IOPS 大於 4。您最多可以同時新增四個濾鏡。

- 比較

顯示您選擇與根物件進行比較的物件清單。

比較窗格中物件的資料顯示在計數器圖表中。

- 查看統計數據

對於捲和 LUN，您可以選擇是否在每個收集週期（預設 5 分鐘）後顯示統計信息，或者是否以每小時平均值的形式顯示統計信息。此功能可讓您查看支援 NetApp 「效能保證」計畫的延遲圖表。

- 反圖表

顯示每個物件效能類別的圖形資料。

通常，預設僅顯示三到四個圖表。選擇圖表組件可讓您顯示其他圖表或隱藏特定圖表。您也可以選擇顯示或

隱藏事件時間軸。

- 事件時間表

顯示您在時間範圍元件中選擇的時間線上發生的效能和健康事件。

使用 QoS 策略群組資訊管理效能

Unified Manager 可讓您查看您正在監控的所有叢集上可用的服務品質 (QoS) 策略群組。這些策略可能已使用 ONTAP 軟體 (系統管理員或 ONTAP CLI) 或 Unified Manager 效能服務等級策略定義。Unified Manager 也顯示哪些磁碟區和 LUN 指派了 QoS 原則群組。

有關調整 QoS 設定的更多信息，請參閱 ["績效管理概述"](#)

儲存 QoS 如何控制工作負載吞吐量

您可以建立服務品質 (QoS) 策略群組來控制其包含的工作負載的每秒 I/O (IOPS) 或吞吐量 (MB/s) 限制。如果工作負載位於沒有設定限制的策略群組 (例如預設策略群組) 中，或設定的限制無法滿足您的需求，您可以增加限制或將工作負載移至具有所需限制的新策略群組或現有策略群組。

「傳統」QoS 策略群組可以指派給單一工作負載；例如單一磁碟區或 LUN。在這種情況下，工作負載可以使用全部吞吐量限制。QoS 策略群組也可以指派給多個工作負載；在這種情況下，吞吐量限制在工作負載之間「共用」。例如，分配給三個工作負載的 QoS 限制為 9,000 IOPS，這將限制合併後的 IOPS 不能超過 9,000 IOPS。

「自適應」QoS 策略群組也可以指派給單一工作負載或多個工作負載。但是，即使指派給多個工作負載，每個工作負載也會獲得完整的吞吐量限制，而不是與其他工作負載共用吞吐量值。此外，自適應 QoS 策略會根據每個工作負載的磁碟區大小自動調整吞吐量設置，從而隨著磁碟區大小的變化保持 IOPS 與 TB 的比率。例如，如果在自適應 QoS 策略中將峰值設定為 5,000 IOPS/TB，則 10 TB 卷的最大吞吐量將為 50,000 IOPS。如果稍後將磁碟區大小調整為 20 TB，自適應 QoS 會將最大值調整為 100,000 IOPS。

從 ONTAP 9.5 開始，您可以在定義自適應 QoS 策略時包含區塊大小。當工作負載使用非常大的區塊大小並最終使用大量吞吐量時，這可以有效地將策略從 IOPS/TB 閾值轉換為 MB/s 閾值。

對於共享群組 QoS 策略，當策略群組中所有工作負載的 IOPS 或 MB/s 超過設定的限制時，策略群組會限制工作負載以限制其活動，這會降低策略群組中所有工作負載的效能。如果動態效能事件是由策略群組限制產生的，則事件描述會顯示所涉及的策略群組的名稱。

在「效能：所有磁碟區」檢視中，您可以按 IOPS 和 MB/s 對受影響的磁碟區進行排序，以查看哪些工作負載的使用率最高，可能導致該事件。在效能/磁碟區資源管理器頁面中，您可以選擇其他磁碟區或磁碟區上的 LUN，以與受影響的工作負載 IOPS 或 MBps 吞吐量使用情況進行比較。

透過將過度使用節點資源的工作負載分配給更嚴格的策略群組設置，策略群組可以限制工作負載以限制其活動，從而減少該節點上資源的使用。但是，如果您希望工作負載能夠使用更多的節點資源，則可以增加策略群組的值。

您可以使用 System Manager、ONTAP 指令或 Unified Manager 效能服務等級來管理原則群組，包含下列任務：

- 建立策略組
- 在策略群組中新增或刪除工作負載
- 在策略組之間移動工作負載
- 更改策略群組的吞吐量限制
- 將工作負載移動到不同的聚合和/或節點

查看所有叢集上可用的所有 QoS 策略群組

您可以顯示 Unified Manager 正在監控的叢集上可用的所有 QoS 策略群組的清單。這包括傳統 QoS 策略、自適應 QoS 策略以及由 Unified Manager 效能服務等級策略管理的 QoS 策略。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「QoS 策略群組」。

預設顯示「效能：傳統 QoS 策略群組」視圖。
2. 查看每個可用的傳統 QoS 策略群組的詳細配置設定。
3. 點選展開按鈕 (▼) 來查看有關該策略組的更多詳細資訊。
4. 在「檢視」功能表中，選擇其中一個附加選項以檢視所有自適應 QoS 原則群組或檢視使用 Unified Manager 效能服務等級所建立的所有 QoS 原則群組。

查看同一 QoS 策略群組中的磁碟區或 LUN

您可以顯示已指派給相同 QoS 政策群組的磁碟區和 LUN 的清單。

對於在多個磁碟區之間「共用」的傳統 QoS 策略群組，這有助於查看某些磁碟區是否過度使用了為策略群組定義的吞吐量。它還可以幫助您決定是否可以將其他磁碟區新增至策略群組而不會對其他磁碟區產生負面影響。

對於自適應 QoS 原則和 Unified Manager 效能服務等級原則，這有助於查看使用策略群組的所有磁碟區或 LUN，以便您可以看到如果變更 QoS 原則的設定設置，哪些物件會受到影響。


步驟

1. 在左側導覽窗格中，按一下「儲存」>「QoS 策略群組」。

預設顯示「效能：傳統 QoS 策略群組」視圖。
2. 如果您對傳統政策組感興趣，請留在此頁面。否則，請選擇其中一個附加檢視選項以顯示所有自適應 QoS 原則群組或由 Unified Manager 效能服務等級所建立的所有 QoS 原則群組。
3. 在您感興趣的 QoS 策略中，按一下展開按鈕 (▼) 來查看更多詳細資訊。

View Adaptive QoS Policy Groups

Schedule Report

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
▼ julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
▲ julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2
Details Allocated Capacity  Associated Objects 2 Volumes 0 LUNs Events None							
▼ julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
▼ julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

4. 按一下磁碟區或 LUN 連結以查看使用此 QoS 策略的物件。

磁碟區或 LUN 的效能清單頁面顯示使用 QoS 策略的物件的排序清單。

查看應用於特定磁碟區或 LUN 的 QoS 原則群組設置

您可以查看已套用至磁碟區和 LUN 的 QoS 原則群組，並且可以連結至效能/QoS 策略群組視圖以顯示每個 QoS 原則的詳細設定。

查看應用於磁碟區的 QoS 策略的步驟如下所示。查看 LUN 的此資訊的步驟類似。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。

預設顯示“健康狀況：所有磁碟區”視圖。

2. 在「檢視」功能表中，選擇「效能：QoS 策略群組中的磁碟區」。

3. 找到您要查看的磁碟區並向右捲動，直到您看到 **QoS 策略群組** 列。

4. 按一下 QoS 策略群組名稱。

根據傳統 QoS 策略、自適應 QoS 策略或使用 Unified Manager 效能服務等級所建立的 QoS 策略，將顯示對應的服務品質頁面。

5. 查看 QoS 策略組的詳細設定。

6. 點選展開按鈕 (▼) 來查看有關該策略組的更多詳細資訊。

查看效能圖表以比較同一 QoS 策略群組中的磁碟區或 LUN

您可以查看同一 QoS 策略群組中的磁碟區和 LUN，然後比較單一 IOPS、MB/s 或 IOPS/TB 圖表上的效能以識別任何問題。

比較同一 QoS 策略群組中磁碟區的效能的步驟如下所示。查看 LUN 的此資訊的步驟類似。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。

預設顯示“健康狀況：所有磁碟區”視圖。

2. 在「檢視」功能表中，選擇「效能：QoS 策略群組中的磁碟區」。
3. 按一下要查看的磁碟區的名稱。

將顯示該磁碟區的效能資源管理器頁面。

4. 在檢視和比較選單中，選擇*相同 QoS 策略群組中的磁碟區*。

下表列出了共享相同 QoS 策略的其他磁碟區。

5. 按一下「新增」按鈕將這些磁碟區新增至圖表中，以便您可以比較圖表中所有選定磁碟區的 IOPS、MB/s、IOPS/TB 和其他效能計數器。

您可以變更時間範圍以查看除預設的 72 小時之外的不同時間間隔內的效能。

不同類型的 QoS 策略如何在吞吐量圖表中顯示

您可以在效能資源管理器和工作負載分析 IOPS、IOPS/TB 和 MB/s 圖表中查看已套用於磁碟區或 LUN 的 ONTAP 定義的服務品質 (QoS) 策略設定。圖表中顯示的資訊會根據應用於工作負載的 QoS 策略的類型而不同。

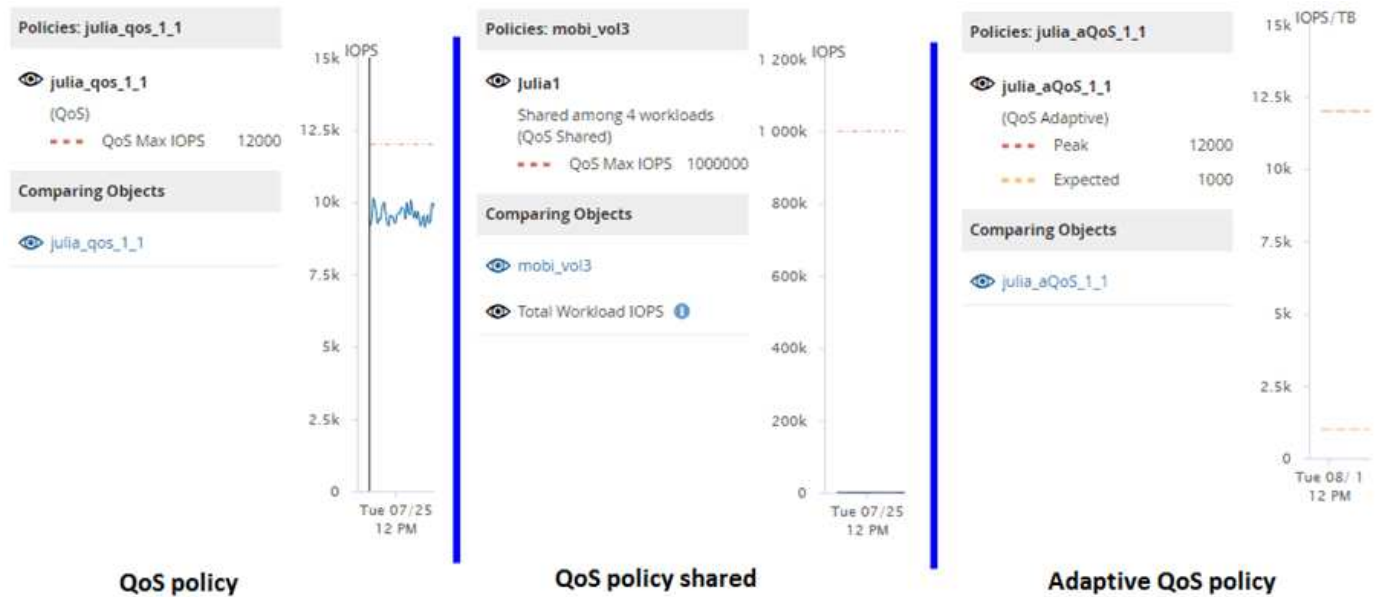
吞吐量最大值（或“峰值”）設定定義了工作負載可以消耗的最大吞吐量，從而限制了對系統資源競爭工作負載的影響。吞吐量最小值（或「預期」）設定定義了工作負載必須具備的最小吞吐量，以便關鍵工作負載能夠滿足最小吞吐量目標，而不管競爭工作負載的需求如何。

IOPS 和 MB/s 的共享和非共享 QoS 策略使用術語「最小值」和「最大值」來定義下限和上限。ONTAP 9.3 中引入的 IOPS/TB 自適應 QoS 策略使用術語「預期」和「峰值」來定義下限和上限。

雖然 ONTAP 允許您建立這兩種類型的 QoS 策略，但根據它們如何應用於工作負載，QoS 策略將以三種方式顯示在效能圖表中。

保單類型	功能	Unicum Manager 介面中的指示器
指派給單一工作負載的 QoS 共用策略，或指派給單一工作負載或多個工作負載的 QoS 非共用策略	每個工作負載可以使用指定的吞吐量設定	顯示“ (QoS) ”
指派給多個工作負載的 QoS 共用策略	所有工作負載共享指定的吞吐量設定	顯示“ (QoS 共享) ”
分配給單一工作負載或多個工作負載的自適應 QoS 策略	每個工作負載可以使用指定的吞吐量設定	顯示“ (QoS 自適應) ”

下圖顯示了計數器圖表中三個選項的顯示方式的範例。



當已在 IOPS 中定義的正常 QoS 策略出現在工作負載的 IOPS/TB 圖表中時，ONTAP 會將 IOPS 值轉換為 IOPS/TB 值，且 Unified Manager 會在 IOPS/TB 圖表中顯示該策略以及文字「QoS，在 IOPS 中定義」。

當已在 IOPS/TB 中定義的自適應 QoS 策略出現在工作負載的 IOPS 圖表中時，ONTAP 會將 IOPS/TB 值轉換為 IOPS 值，且 Unified Manager 在 IOPS 圖表中顯示該策略以及文字「QoS Adaptive - Used, defined in IOPS/TB」分配設定的配置方式。當分配設定設為「allocated-space」時，峰值 IOPS 是根據磁碟區的大小計算的。當分配設定設為「已使用空間」時，峰值 IOPS 是根據磁碟區中儲存的資料量計算的，同時考慮儲存效率。



IOPS/TB 圖表僅當磁碟區使用的邏輯容量大於或等於 128 GB 時才顯示效能資料。當所選時間範圍內已使用容量低於 128 GB 時，圖表中會顯示缺口。

在效能資源管理器中查看工作負載 QoS 最小和最大設置

您可以在效能資源管理器圖表中查看磁碟區或 LUN 上 ONTAP 定義的服務品質 (QoS) 策略設定。吞吐量最大設定限制了競爭工作負載對系統資源的影響。吞吐量最小設定可確保關鍵工作負載滿足最低吞吐量目標，而不管競爭工作負載的需求如何。

只有在 ONTAP 中配置了 QoS 吞吐量「最小」和「最大」IOPS 和 MB/s 設定時，它們才會顯示在計數器圖表中。吞吐量最小設定僅在運行 ONTAP 9.2 或更高版本軟體的系統上可用，僅在 AFF 系統上可用，目前只能為 IOPS 設定。

自適應 QoS 策略從 ONTAP 9.3 開始可用，並使用 IOPS/TB 而不是 IOPS 來表示。這些策略會根據每個工作負載的磁碟區大小自動調整 QoS 策略值，從而隨著磁碟區大小的變化保持 IOPS 與 TB 的比率。您只能將自適應 QoS 策略群組套用至磁碟區。QoS 術語「預期」和「峰值」用於自適應 QoS 策略，而不是最小值和最大值。

當工作負載吞吐量在前一小時的每個效能收集期間超過定義的 QoS 最大政策設定時，Unified Manager 會產生 QoS 政策違規警告事件。在每個收集期間，工作負載吞吐量可能僅在短時間內超過 QoS 閾值，但 Unified Manager 會在圖表上顯示收集期間的「平均」吞吐量。因此，您可能看到 QoS 事件，而工作負載的吞吐量可能尚未超過圖表中顯示的策略閾值。

步驟

1. 在所選磁碟區或 LUN 的「效能資源管理器」頁面中，執行下列操作以查看 QoS 上限和下限設定：

如果你想...	這樣做...
查看 IOPS 上限 (QoS 最大值)	在 IOPS 總計或細分圖表中，按一下「縮放檢視」。
查看 MB/s 上限 (QoS 最大值)	在 MB/s 總計或細分圖表中，按一下 縮放檢視。
查看 IOPS 下限 (QoS 最小值)	在 IOPS 總計或細分圖表中，按一下「縮放檢視」。
查看 IOPS/TB 上限 (QoS 峰值)	對於卷，在 IOPS/TB 圖表中，按一下 縮放檢視。
查看 IOPS/TB 底線 (預期的 QoS)	對於卷，在 IOPS/TB 圖表中，按一下 縮放檢視。

虛線水平線表示 ONTAP 中設定的最大或最小吞吐量值。您也可以查看 QoS 值變更的實施時間。

2. 若要查看與 QoS 設定相比的特定 IOPS 和 MB/s 值，請將遊標移到圖表區域以查看彈出視窗。

如果您注意到某些磁碟區或 LUN 具有非常高的 IOPS 或 MB/s 並且正在給系統資源帶來壓力，則可以使用 System Manager 或 ONTAP CLI 調整 QoS 設置，以便這些工作負載不會影響其他工作負載的效能。

有關調整 QoS 設定的更多信息，請參閱 ["績效管理概述"](#)

使用效能容量和可用 IOPS 資訊管理效能

效能容量 表示在不超過資源有用效能的情況下，您可以從資源中獲得多少吞吐量。當使用現有的效能計數器檢視時，效能容量是在延遲成為問題之前從節點或聚合獲得最大利用率的點。

Unified Manager 從每個叢集中的節點和聚合收集效能容量統計資料。已使用的效能容量 是目前正在使用的效能容量的百分比，可用性能容量 是仍可用的效能容量的百分比。

雖然效能容量可用提供了仍然可用的資源百分比，但 可用 IOPS 告訴您在達到最大效能容量之前可以新增至資源的 IOPS 數量。透過使用此指標，您可以確保可以為資源新增預定數量的 IOPS 的工作負載。

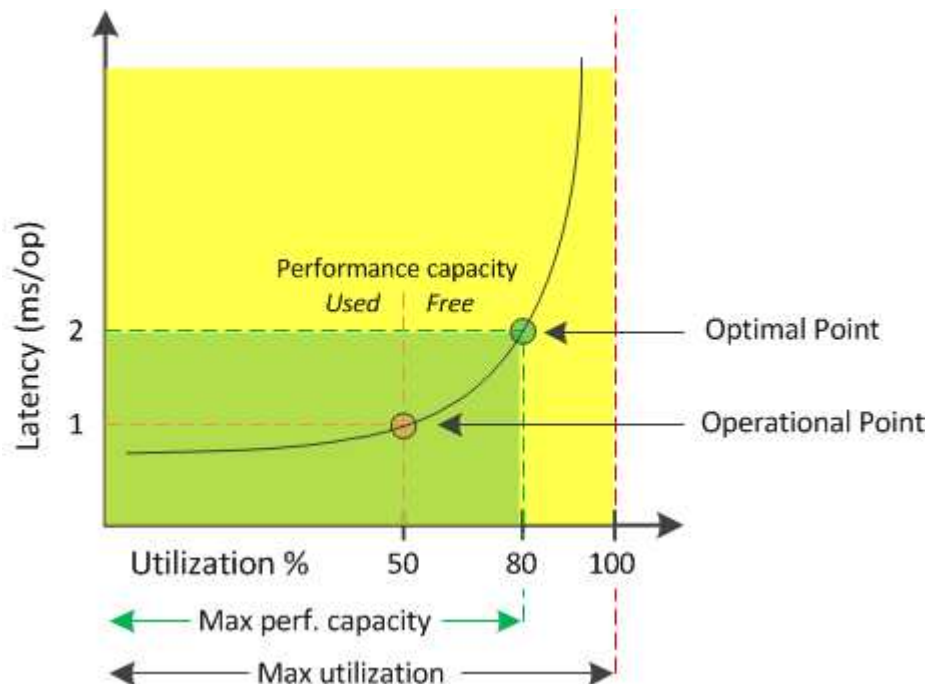
監控效能容量資訊有以下好處：

- 協助工作流程配置和平衡。
- 幫助您防止節點過載或將其資源推到最佳點之外，從而減少故障排除的需要。
- 幫助您更精確地確定可能需要額外儲存設備的位置。

所用性能容量

效能容量使用計數器可協助您確定節點或聚合的效能是否已達到工作負載增加時效能可能下降的程度。它也可以顯示在特定時間段內某個節點或聚合是否被過度使用。使用的效能容量與利用率類似，但前者提供了更多有關特定工作負載的實體資源可用性能能力的見解。

最佳使用效能容量是節點或聚合具有最佳利用率和延遲（回應時間）並且有效利用的點。下圖顯示了聚合的延遲與利用率曲線範例。



在此範例中，_操作點_ 標識聚合目前以 50% 的利用率運行，延遲為 1.0 ms/op。根據從聚合中捕獲的統計數據，Unified Manager 確定此聚合是否有額外的效能容量可用。在這個例子中，_最佳點_ 被確定為聚合利用率為 80% 且延遲為 2.0 ms/op 的點。因此，您可以向此聚合添加更多磁碟區和 LUN，以便更有效率地利用您的系統。

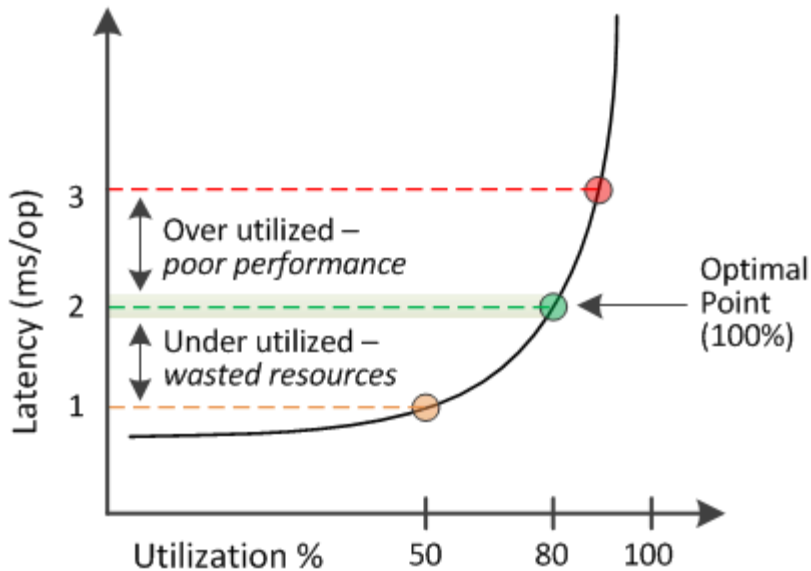
效能容量使用計數器預計會比「利用率」計數器更大，因為效能容量會增加對延遲的影響。例如，如果節點或聚合的使用率為 70%，則效能容量值可能在 80% 到 100% 範圍內，具體取決於延遲值。

然而，在某些情況下，儀表板頁面上的使用率計數器可能會更高。這是正常現象，因為儀表板會在每個收集週期刷新目前計數器值；它不像 Unified Manager 使用者介面中的其他頁面那樣顯示一段時間內的平均值。效能容量使用計數器最適合用作一段時間內平均性能的指標，而利用率計數器最適合用於確定資源的瞬時使用情況。

性能容量使用值的意義

效能容量使用值可協助您識別目前過度利用或未充分利用的節點和聚合。這使您能夠重新分配工作負載，以提高儲存資源的效率。

下圖顯示了資源的延遲與利用率曲線，並以彩色點標示了目前操作點可能所在的三個區域。



- 效能容量使用百分比等於 100 處於最佳點。
目前資源正在有效利用。
- 效能容量使用百分比高於 100 表示節點或聚合體利用率過高，且工作負載的效能不佳。
不應為資源添加任何新的工作負載，並且可能需要重新分配現有的工作負載。
- 效能容量使用百分比低於 100 表示節點或聚合未充分利用，且資源未有效利用。
可以為資源增加更多工作負載。



與利用率不同，效能容量使用百分比可以高於 100%。沒有最大百分比，但當資源過度利用時，其百分比通常會在 110% 到 140% 的範圍內。百分比越高，表示資源有嚴重問題。

可用的 IOPS 是什麼

可用 IOPS 計數器標識在資源達到其限制之前可以加到節點或聚合的剩餘 IOPS 數。

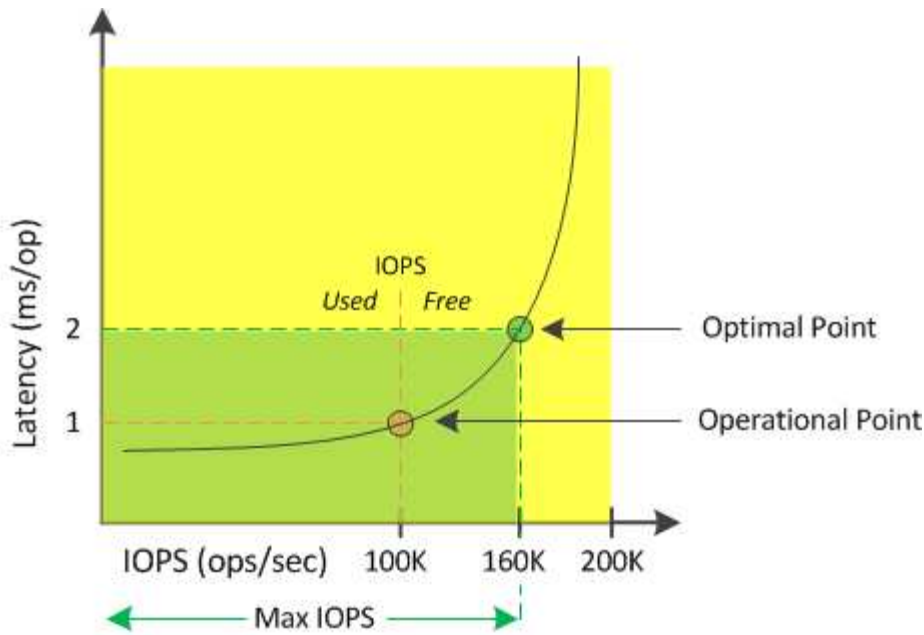
節點可以提供的總 IOPS 取決於節點的物理特性 - 例如 CPU 數量、CPU 速度和 RAM 數量。聚合可以提供的總 IOPS 取決於磁碟的實體屬性 - 例如 SATA、SAS 或 SSD 磁碟。

聚合中所有磁碟區的總 IOPS 可能與聚合的總 IOPS 不符。以下知識庫文章對此進行了討論：[KB"為什麼聚合中所有磁碟區 IOP 的總和與聚合 IOP 不符？"](#)

雖然效能容量可用計數器提供了仍可用的資源百分比，但可用 IOPS 計數器會告訴您在達到最大效能容量之前可以新增至資源的確切 IOPS（工作負載）數量。

例如，如果您使用一對 FAS2520 和 FAS8060 儲存系統，則效能容量可用值為 30% 表示您有一些可用的效能容量。但是，該值無法顯示您可以向這些節點部署多少工作負載。可用 IOPS 計數器可能顯示 FAS8060 上有 500 個可用 IOPS，但 FAS2520 上只有 100 個可用 IOPS。

下圖顯示了節點的延遲與 IOPS 曲線範例。



資源所能提供的最大IOPS數是效能容量使用計數器為100%（最優點）時的IOPS數。操作點表示該節點目前以100K IOPS 運行，延遲為 1.0 ms/op。根據從節點捕獲的統計數據，Unified Manager 確定該節點的最大 IOPS 為 160K，這意味著有 60K 空間或可用的 IOPS。因此，您可以為該節點添加更多工作負載，以便更有效率地使用您的系統。



當資源中的使用者活動最少時，可用的 IOPS 值是根據每個 CPU 核心約 4,500 IOPS 的通用工作負載來計算的。這是因為 Unified Manager 缺乏資料來準確估計所服務的工作負載的特性。

查看節點和聚合效能容量使用值

您可以監控叢集中所有節點或所有聚合的效能容量使用值，也可以查看單一節點或聚合的詳細資訊。

效能容量使用值顯示在儀表板、效能清單頁面、最佳表現頁面、建立閾值策略頁面、效能資源管理器頁面和詳細圖表中。例如，「效能：所有聚合」頁面提供了「已使用效能容量」列，用於查看所有聚合的效能容量已使用值。

Aggregates Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering: No filter applied Search Aggregates Data Search

Assign Threshold Policy Clear Threshold Policy

Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS
⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS

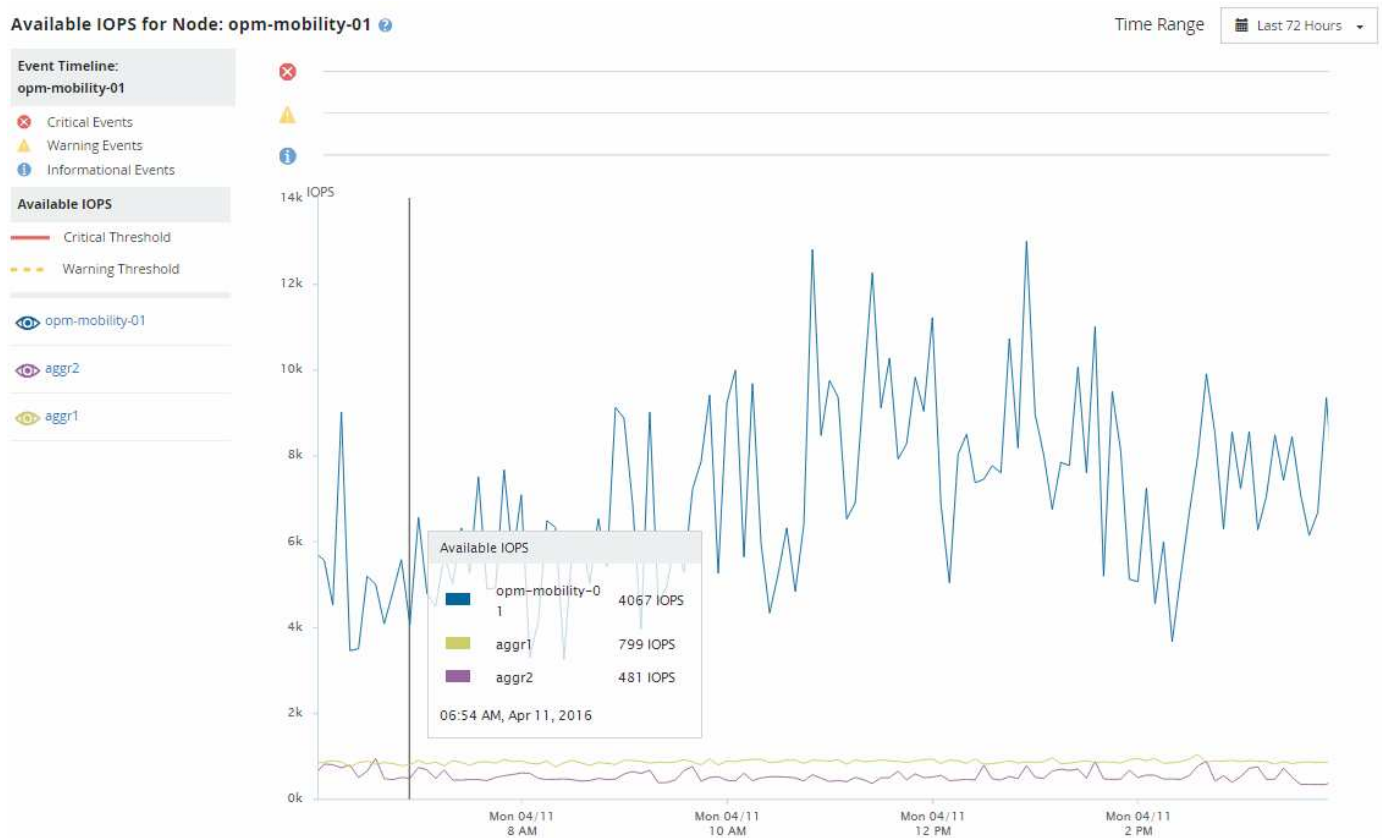
監視效能容量使用計數器可讓您識別以下內容：

- 任何叢集上的任何節點或聚合是否具有高效能容量使用值
- 任何叢集上的任何節點或聚合是否有活動的效能容量使用事件
- 叢集中效能容量使用值最高和最低的節點和聚合
- 延遲和利用率計數器值與具有高效能容量使用值的節點或聚合結合使用
- 如果其中一個節點發生故障，HA 對中節點的效能容量使用值將受到怎樣的影響
- 具有高效能容量使用值的聚合上最繁忙的捲和 LUN

查看節點並聚合可用 IOPS 值

您可以監控叢集中所有節點或所有聚合的可用 IOPS 值，也可以查看單一節點或聚合的詳細資訊。

可用的 IOPS 值顯示在效能清單頁面和節點和聚合的效能資源管理器頁面圖表中。例如，在節點/效能資源管理器頁面中檢視節點時，您可以從清單中選擇「可用 IOPS」計數器圖表，以便比較該節點和該節點上的多個聚合的可用 IOPS 值。



監控可用的 IOPS 計數器可讓您識別：

- 具有最大可用 IOPS 值的節點或聚合有助於確定未來工作負載的部署位置。
- 具有最小可用 IOPS 值的節點或聚合，用於確定您應該監控的潛在未來效能問題的資源。
- 聚合上可用 IOPS 值較小的最繁忙的捲和 LUN。

查看效能容量計數器圖表以識別問題

您可以在效能資源管理器頁面上查看節點和聚合的效能容量使用圖表。這使您能夠查看特定時間範圍內選定節點和聚合的詳細效能容量資料。

標準計數器圖表顯示所選節點或聚合的效能容量使用值。細分計數器圖表顯示根據使用者協定與後台系統程序劃分的根物件的總效能容量值。此外，還顯示了可用的效能容量。

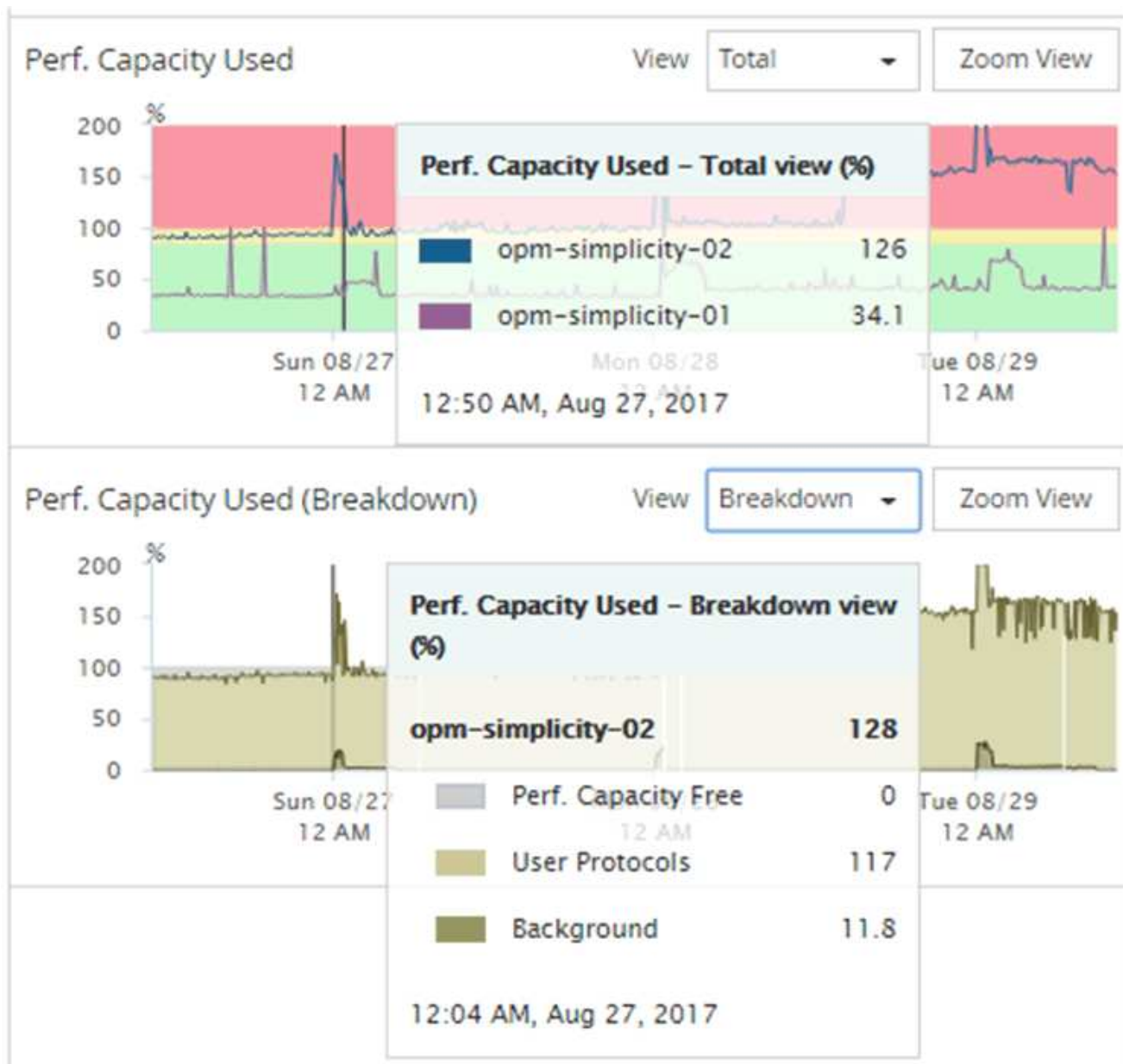


由於一些與系統和資料管理相關的後台活動被識別為使用者工作負載並歸類為使用者協議，因此當這些進程運行時，使用者協議百分比可能會顯得人為地高。這些進程通常在叢集使用率較低的午夜左右運行。如果您發現午夜左右使用者協定活動激增，請驗證叢集備份作業或其他背景活動是否已配置為在該時間執行。

步驟

1. 從節點或聚合*登陸*頁面中選擇*資源管理器*標籤。
2. 在 **Counter Charts** 窗格中，按一下 **Choose charts**，然後選擇 *Perf。已使用容量*圖表。
3. 向下捲動直到您可以查看圖表。

標準圖表的顏色顯示物件何時處於最佳範圍（黃色）、物件何時未被充分利用（綠色）以及物件何時過度利用（紅色）。細分圖表僅顯示根物件的詳細效能容量詳細資訊。



4. 如果您想以全尺寸格式查看任一圖表，請按一下「縮放檢視」。

透過這種方式，您可以在單獨的視窗中開啟多個計數器圖表，以將相同時間範圍內的效能容量使用值與 IOPS 或 MBps 值進行比較。

效能容量使用效能閾值條件

您可以建立使用者定義的效能閾值策略，以便在節點或聚合的效能容量使用值超過定義的效能容量使用閾值設定時觸發事件。

此外，可以為節點配置「效能容量使用接管」閾值策略。此閾值策略將 HA 對中兩個節點的效能容量使用統計資料相加，以確定當另一個節點發生故障時，其中一個節點是否會缺乏足夠的容量。由於故障轉移期間的工作負載是兩個夥伴節點工作負載的組合，因此可以對兩個節點應用相同的效能容量使用接管策略。



這種效能容量使用等效性在節點之間通常是正確的。但是，如果透過故障轉移夥伴節點發送到其中一個節點的跨節點流量明顯增多，則在一個夥伴節點上運行所有工作負載時所使用的總效能容量與在另一個夥伴節點上運行所有工作負載時所使用的總效能容量可能會略有不同，具體取決於哪個節點發生故障。

效能容量使用條件也可以用作輔助效能閾值設置，以在定義 LUN 和磁碟區的閾值時建立組合閾值策略。效能容量使用條件適用於磁碟區或 LUN 所在的聚合或節點。例如，您可以使用下列條件建立組合閾值策略：

儲存對象	性能計數器	警告閾值	臨界閾值	期間
體積	延遲	15毫秒/操作	25 毫秒/操作	20分鐘
總計的	已使用的性能容量	80%	95%	

組合閾值策略僅當整個持續時間內同時違反兩個條件時才會產生事件。

使用效能容量使用計數器來管理效能

通常，組織希望以低於 100 的性能容量使用百分比來運營，以便有效利用資源，同時保留一些額外的性能容量來支援高峰期的需求。您可以使用閾值策略來自訂何時發送高效能容量使用值警報。

您可以根據您的性能要求制定具體的目標。例如，金融服務公司可能會保留更多的履約能力，以確保交易的及時執行。這些公司可能希望將效能容量使用門檻設定在 70% 至 80% 的範圍內。如果利潤較小的製造公司願意冒著效能風險來更好地管理 IT 成本，他們可能會選擇保留較少的效能容量。這些公司可能會將效能容量使用門檻設定在 85-95% 範圍內。

當效能容量使用值超過使用者定義的閾值策略中設定的百分比時，Unified Manager 會傳送警報電子郵件並將事件新增至事件清單頁面。這使您能夠在潛在問題影響效能之前對其進行管理。這些事件也可以用作需要在節點和聚合內進行工作負載移動和變更的指標。

了解並使用節點故障轉移規劃頁面

如果節點的高可用性 (HA) 夥伴節點發生故障，效能/節點故障轉移規劃頁面將估計對節點效能的影響。Unified Manager 根據 HA 對中節點的歷史效能進行估算。

估計故障轉移對效能的影響有助於您在以下情況下進行規劃：

- 如果故障轉移持續使接管節點的估計效能降低到不可接受的水平，您可以考慮採取糾正措施來減少故障轉移造成的效能影響。
- 在啟動手動故障轉移來執行硬體維護任務之前，您可以估計故障轉移對接管節點效能的影響，以確定執行該任務的最佳時間。

使用節點故障轉移計劃頁面確定糾正措施

根據「效能/節點故障轉移規劃」頁面中顯示的信息，您可以採取措施確保故障轉移不會導致 HA 對的效能下降到可接受的水平以下。

例如，為了減少故障轉移對效能的估計影響，您可以將某些磁碟區或 LUN 從 HA 對中的節點移至叢集中的其他節點。這樣做可確保主節點在故障轉移後能夠繼續提供可接受的效能。

節點故障轉移計劃頁面的元件

效能/節點故障轉移計畫頁面的元件顯示在網格和比較窗格中。這些部分可讓您評估節點故障轉移對接管節點效能的影響。

績效統計網格

效能/節點故障轉移規劃頁面顯示一個網格，其中包含延遲、IOPS、利用率和使用的效能容量的統計資料。



此頁面和效能/節點效能資源管理器頁面中顯示的延遲和 IOPS 值可能不匹配，因為使用不同的效能計數器來計算預測節點故障轉移的值。

在網格中，每個節點被指派以下角色之一：

- 基本的

當 HA 合作夥伴發生故障時接管該合作夥伴的節點。根物件始終是主節點。

- 夥伴

故障轉移場景中發生故障的節點。

- 預計收購

與主節點相同。此節點顯示的效能統計資料顯示了接管節點接管故障夥伴節點後的效能。



儘管故障轉移後接管節點的工作負載相當於兩個節點工作負載的總和，但估計接管節點的統計資料並不是主節點和合作夥伴節點統計資料的總和。例如，如果主節點的延遲為 2 ms/op，則合作夥伴節點的延遲為 3 ms/op，則估計接管節點的延遲可能為 4 ms/op。此值是 Unified Manager 執行的計算。

如果您希望合作夥伴節點成為根對象，可以按一下其名稱。顯示「效能/節點效能資源管理器」頁面後，您可以按一下「故障轉移計畫」標籤來查看此節點故障場景下效能如何變化。例如，如果 Node1 是主節點，Node2 是合作夥伴節點，則可以按一下 Node2 使其成為主節點。透過這種方式，您可以看到估計的效能如何根據哪個節點發生故障而變化。

比較窗格

以下清單描述了比較窗格中預設顯示的元件：

- 事件圖表

它們以與效能/節點效能資源管理器頁面中相同的格式顯示。它們僅屬於主節點。

- 反圖表

它們顯示網格中顯示的效能計數器的歷史統計資料。在每個圖表中，估計接管節點的圖形顯示了在任何給定

時間發生故障轉移時的估計效能。

例如，假設利用率圖表顯示 2 月 8 日上午 11 點預計接管節點的利用率為 73%。如果當時發生故障轉移，接管節點的利用率將達到 73%。

歷史統計資料可以幫助您找到啟動故障轉移的最佳時間，以最大限度地減少接管節點過載的可能性。您僅可以在接管節點的預測效能可接受時安排故障轉移。

預設情況下，根物件和夥伴節點的統計資料都會顯示在比較窗格中。與效能/節點效能資源管理器頁面不同，此頁面不顯示*新增*按鈕供您新增物件進行統計比較。

您可以按照與在效能/節點效能資源管理器頁面中相同的方式自訂比較窗格。以下列表顯示了自訂圖表的範例：

- 按一下節點名稱可在計數器圖表中顯示或隱藏該節點的統計資料。
- 按一下「縮放檢視」可在新視窗中顯示特定計數器的詳細圖表。

將閾值策略與節點故障轉移計劃頁面結合使用

您可以建立節點閾值策略，以便當潛在故障轉移導致接管節點的效能降低到不可接受的水平時，您可以在「效能/節點故障轉移計畫」頁面中收到通知。

如果連續六個收集期（30 分鐘）超出閾值，則名為「節點 HA 對過度利用」的系統定義效能閾值策略將產生警告事件。如果 HA 對中節點的組合效能容量使用量超過 200%，則視為超出閾值。

來自系統定義的閾值策略的事件提醒您故障轉移將導致接管節點的延遲增加到不可接受的水平。當您看到此策略為特定節點產生的事件時，您可以導覽至該節點的效能/節點故障轉移規劃頁面，以查看因故障轉移而預測的延遲值。

除了使用此系統定義的閾值策略之外，您還可以使用「已使用效能容量 - 接管」計數器建立閾值策略，然後將此策略套用於選取的節點。指定低於 200% 的閾值可讓您在超出系統定義策略的閾值之前收到事件。如果您希望在產生系統定義的策略事件之前收到通知，也可以指定超出閾值的最短時間段，使其少於 30 分鐘。

例如，您可以定義一個閾值策略，當 HA 對中節點的組合效能容量使用量超過 175% 超過 10 分鐘時，就會產生警告事件。您可以將此策略應用於構成 HA 對的 Node1 和 Node2。收到節點 1 或節點 2 的警告事件通知後，您可以查看該節點的效能/節點故障轉移計畫頁面，以評估接管節點的預期效能影響。如果發生故障轉移，您可以採取糾正措施以避免接管節點過載。如果在節點的綜合效能容量使用率低於 200% 時採取措施，則即使在此期間發生故障轉移，接管節點的延遲也不會達到不可接受的水平。

使用效能容量使用明細圖表進行故障轉移規劃

詳細的「已使用效能容量 - 細分」圖表顯示了主節點和合作夥伴節點已使用效能容量。它還顯示了預計接管節點上的可用性能容量。此資訊可協助您確定如果合作夥伴節點發生故障，是否會出現效能問題。

除了顯示節點使用的總效能容量之外，細分圖表還將每個節點的值細分為使用者協定和後台進程。

- 使用者協定是從使用者應用程式到叢集的 I/O 操作。
- 後台進程是涉及儲存效率、資料複製和系統健康的內部系統進程。

透過這個額外的詳細資訊級別，您可以確定效能問題是由用戶應用程式活動還是後台系統進程（例如重複資料刪

除、RAID 重建、磁碟清理和SnapMirror副本) 引起的。

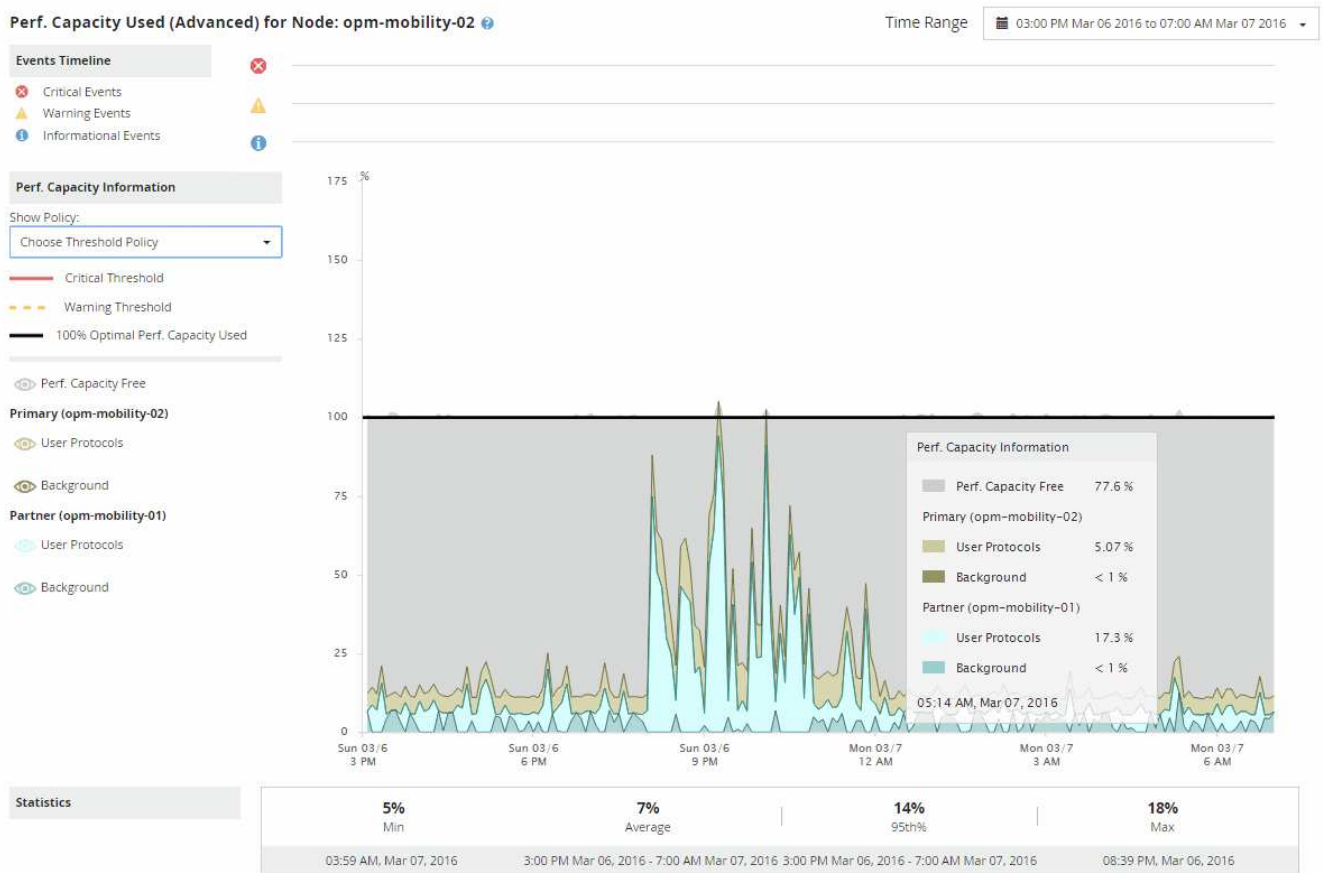
步驟

1. 前往將作為預計接管節點的節點的「效能/節點故障轉移計畫」頁面。
2. 從*時間範圍*選擇器中，選擇計數器網格和計數器圖表中顯示歷史統計資料的時間段。

將顯示包含主節點、合作夥伴節點和估計接管節點的統計資料的計數器圖表。

3. 從*選擇圖表*清單中，選擇*Perf。已使用容量*。
4. 在 **Perf** 中。容量已使用*圖表，選擇*細分*並點選*縮放檢視*。

Perf 的詳細圖表。顯示已使用容量。



5. 將遊標移到詳細圖表上，即可在彈出視窗中查看效能容量使用資訊。

穿孔。可用容量百分比是預計接管節點上可用的效能容量。它指示故障轉移後接管節點上還剩下多少效能容量。如果為 0%，故障轉移將導致接管節點上的延遲增加到不可接受的水平。

6. 考慮採取糾正措施以避免性能容量可用百分比過低。

如果您打算啟動故障轉移以進行節點維護，請選擇效能容量可用百分比不為 0 時使合作夥伴節點發生故障的時間。

收集數據並監控工作負載效能

Unified Manager 每 5 分鐘收集並分析一次工作負載活動以識別效能事件，並且每 15 分鐘偵測一次設定變更。它最多保留 30 天的 5 分鐘歷史效能和事件數據，並使用這些數據來預測所有受監控工作負載的預期延遲範圍。

Unified Manager 必須收集至少 3 天的工作負載活動才能開始分析，並且 I/O 回應時間的延遲預測才能顯示在工作負載分析頁面和事件詳細資料頁面上。在收集此活動時，延遲預測不會顯示工作負載活動發生的所有變化。在收集 3 天的活動後，Unified Manager 會在每 24 小時的凌晨 12:00 調整延遲預測，以反映工作負載活動的變化並建立更準確的動態效能閾值。

在 Unified Manager 監控工作負載的前 4 天內，如果自上次資料收集以來已超過 24 小時，則延遲圖表將不會顯示該工作負載的延遲預測。上次收集之前偵測到的事件仍然可用。



夏令時 (DST) 會改變系統時間，從而改變受監控工作負載的效能統計資料的延遲預測。Unified Manager 立即開始更正延遲預測，大約需要 15 天才能完成。在此期間，您可以繼續使用 Unified Manager，但是，由於 Unified Manager 使用延遲預測來偵測動態事件，因此某些事件可能不準確。時間變化之前偵測到的事件不受影響。

Unified Manager 監控的工作負載類型

您可以使用 Unified Manager 監控兩種類型工作負載的效能：使用者定義和系統定義。

- 使用者定義的工作負載

從應用程式到叢集的 I/O 吞吐量。這些是涉及讀寫請求的過程。磁碟區、LUN、NFS 共用、SMB/CIFS 共用和工作負載是使用者定義的工作負載。



Unified Manager 僅監控叢集上的工作負載活動。它不監控應用程式、客戶端或應用程式與叢集之間的路徑。

如果某个工作負載符合下列一項或多項條件，則該工作負載無法受到 Unified Manager 監控：

- 它是唯讀模式下的資料保護 (DP) 副本。（DP 磁碟區受到使用者產生的流量監控。）
- 它是一個離線資料克隆。
- 它是 MetroCluster 配置中的鏡像磁碟區。

- 系統定義的工作負載

與儲存效率、資料複製和系統健康相關的內部流程包括：

- 儲存效率，例如重複資料刪除
- 磁碟健康狀況，包括 RAID 重建、磁碟清理等
- 資料複製，例如 SnapMirror 副本
- 管理活動
- 文件系統健康狀況，包括各種 WAFL 活動
- 檔案系統掃描器，例如 WAFL 掃描

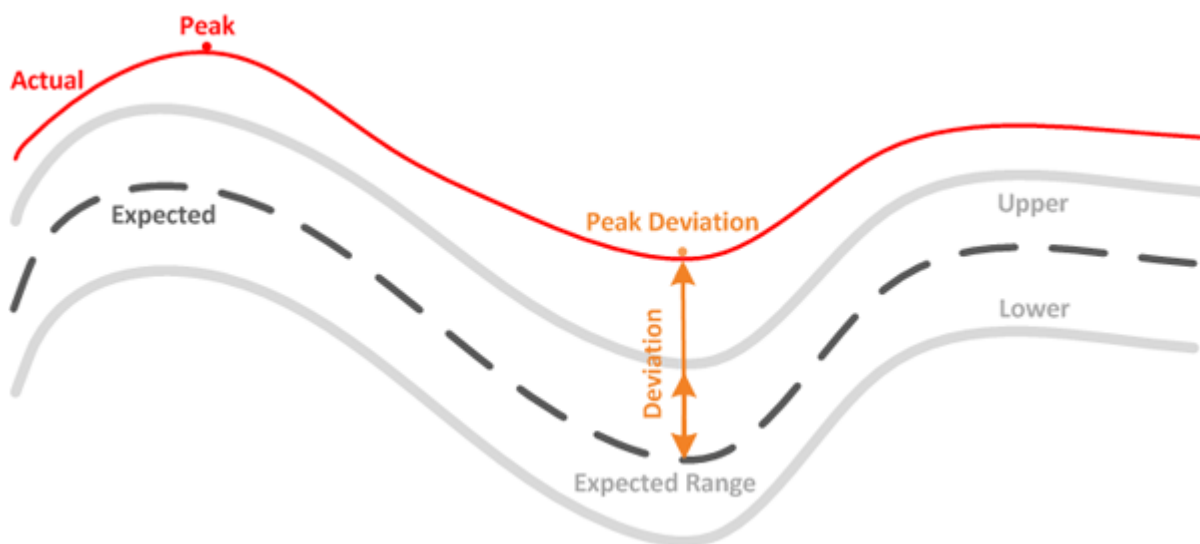
- 複製卸載，例如從 VMware 主機卸載儲存效率操作
- 系統健康狀況，例如磁碟區移動、資料壓縮等
- 未監控的捲

只有當這些工作負載所使用的叢集元件存在爭用時，系統定義的工作負載的效能資料才會顯示在 GUI 中。例如，您無法搜尋系統定義的工作負載的名稱以在 GUI 中查看其效能資料。

工作負載效能測量值


Unified Manager 根據歷史和預期統計值來衡量叢集上工作負載的效能，這些統計值形成了工作負載的延遲預測值。它將實際工作負載統計值與延遲預測進行比較，以確定工作負載效能何時過高或過低。未如預期執行的工作負載會觸發動態效能事件來通知您。

在下圖中，紅色的實際值代表該時間範圍內的實際效能統計資料。實際值已超過效能閾值，即延遲預測的上限。峰值是時間範圍內的最高實際值。偏差衡量預期值（預測）與實際值之間的變化，而峰值偏差表示預期值與實際值之間的最大變化。



下表列出了工作負載效能測量值。

測量	描述
活動	策略群組中的工作負載所使用的 QoS 限制百分比。 <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>i 如果 Unified Manager 偵測到策略群組發生變更（例如新增或刪除磁碟區或變更 QoS 限制），則實際值和預期值可能會超過設定限制的 100%。如果數值超過設定限值的 100%，則顯示為 >100%。如果值小於設定限值的 1%，則顯示為 <1%。</p> </div>
實際的	對於給定的工作負載，在特定時間測量的效能值。

測量	描述
偏差	<p>預期值與實際值之間的變化。它是實際值減去預期值與預期範圍上限值減去預期值的比率。</p> <div style="display: flex; align-items: center;">  <p>負偏差值表示工作負載效能低於預期，而正偏差值表示工作負載效能高於預期。</p> </div>
預期的	預期值是基於對給定工作負載的歷史效能資料的分析。Unified Manager 分析這些統計值以確定值的預期範圍（延遲預測）。
延遲預測（預期範圍）	延遲預測是對特定時間的上限和下限性能值的預測。對於工作負載延遲，上限值構成效能閾值。當實際值超過效能閾值時，Unified Manager 會觸發動態效能事件。
頂峰	一段時間內測得的最大值。
峰值偏差	一段時間內測得的最大偏差值。
隊列深度	在互連元件處等待的待處理 I/O 請求數。
使用率	對於網路處理、資料處理和聚合元件，一段時間內完成工作負載作業的繁忙時間百分比。例如，網路處理或資料處理元件處理 I/O 請求或聚合完成讀取或寫入請求的時間百分比。
寫入吞吐量	從本地叢集上的工作負載到MetroCluster配置中的配對叢集的寫入吞吐量，以兆位元組/秒 (MB/s) 為單位。

預期的表現範圍是多少

延遲預測是對特定時間的上限和下限性能值的預測。對於工作負載延遲，上限值構成效能閾值。當實際值超過效能閾值時，Unified Manager 會觸發動態效能事件。

例如，在上午 9:00 至下午 5:00 的正常工作時間內，大多數員工可能會在上午 9:00 至上午 10:30 之間查看電子郵件。電子郵件伺服器需求的增加意味著此時間段內後端儲存的工作負載活動也會增加。員工可能會注意到他們的電子郵件用戶端的回應時間很慢。

在中午 12 點到下午 1 點之間的午餐時間以及下午 5 點之後的工作時間結束時，大多數員工可能不會使用電腦。對電子郵件伺服器的需求通常會減少，對後端儲存的需求也會減少。或者，可以有預定的工作負載操作，例如儲存備份或病毒掃描，這些操作在下午 5:00 之後開始，並增加後端儲存的活動。

幾天內，工作負載活動的增加和減少決定了活動的預期範圍（延遲預測），並確定了工作負載的上限和下限。當物件的實際工作負載活動超出上限或下限，並在一段時間內保持超出邊界時，這可能表示該物件被過度使用或未充分使用。

延遲預測是如何形成的

Unified Manager 必須收集至少 3 天的工作負載活動，然後才能開始分析，並且 I/O 回應時間的延遲預測才能顯示在 GUI 中。所需的最低限度的資料收集並未考慮到工作負載活動發生的所有變化。在收集前 3 天的活動後，Unified Manager 會在每 24 小時的凌晨 12:00 調整延遲預測，以反映工作負載活動的變化並建立更準確的動態效能閾值。



夏令時 (DST) 會改變系統時間，從而改變受監控工作負載的效能統計資料的延遲預測。Unified Manager 立即開始更正延遲預測，大約需要 15 天才能完成。在此期間，您可以繼續使用 Unified Manager，但是，由於 Unified Manager 使用延遲預測來偵測動態事件，因此某些事件可能不準確。時間變化之前偵測到的事件不受影響。

延遲預測如何用於效能分析

Unified Manager 使用延遲預測來表示受監控工作負載的典型 I/O 延遲（回應時間）活動。當工作負載的實際延遲高於延遲預測的上限時，它會提醒您，從而觸發動態效能事件，以便您可以分析效能問題並採取糾正措施來解決它。

延遲預測為工作負載設定了效能基準。隨著時間的推移，Unified Manager 會從過去的效能測量中學習，以預測工作負載的預期效能和活動水準。預期範圍的上限確定了動態效能閾值。Unified Manager 使用基準來確定實際延遲何時高於或低於閾值，或超出其預期範圍。實際值和預期值之間的比較為工作負載建立了效能概況。

當工作負載的實際延遲超過動態效能閾值時，由於叢集組件的爭用，延遲會很高，工作負載的執行速度會比預期慢。共享相同叢集組件的其他工作負載的效能也可能比預期的要慢。

Unified Manager 分析閾值交叉事件並確定該活動是否為效能事件。如果高工作負載活動在較長時間內（例如幾個小時）保持一致，Unified Manager 會認為該活動正常，並動態調整延遲預測以形成新的動態效能閾值。

某些工作負載可能一直具有較低的活動性，其中延遲的延遲預測不會隨時間發生很大的變化。為了在效能事件分析期間最大限度地減少事件數量，Unified Manager 僅針對操作和延遲遠高於預期的低活動磁碟區觸發事件。



在此範例中，磁碟區的延遲預測為灰色，最低為每操作 3.5 毫秒 (ms/op)，最高為 5.5 ms/op。如果由於網路流量的間歇性激增或群集組件的爭用，實際延遲（藍色）突然增加到 10 ms/op，則它高於延遲預測並已超過動態效能閾值。

當網路流量減少或叢集元件不再爭用時，延遲將恢復到延遲預測範圍內。如果延遲長時間保持在 10 ms/op 或以上，您可能需要採取糾正措施來解決該事件。

Unified Manager 如何使用工作負載延遲來識別效能問題

工作負載延遲（回應時間）是叢集上的磁碟區響應來自客戶端應用程式的 I/O 請求所需的時間。Unified Manager 使用延遲來偵測效能事件並向您發出警報。

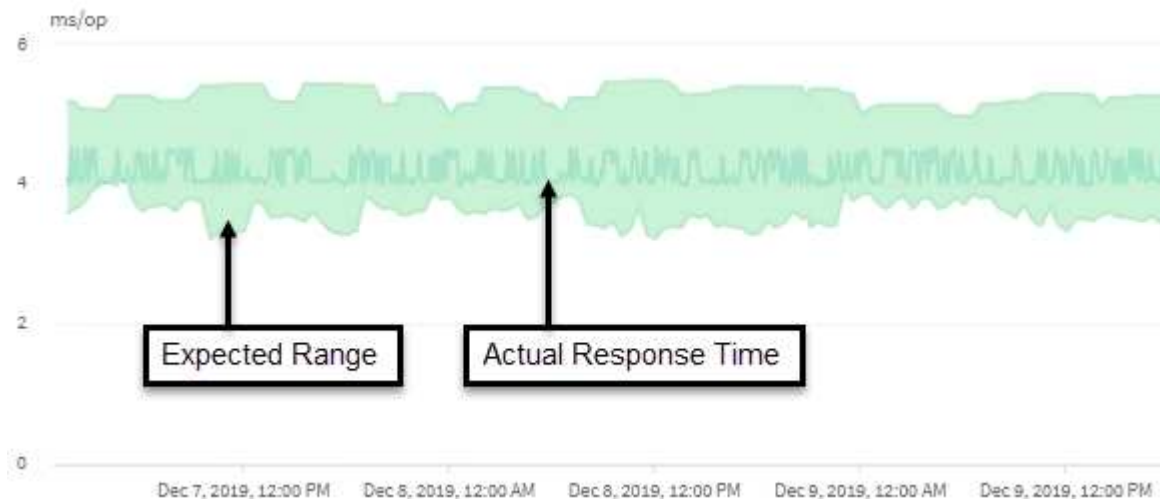
高延遲意味著應用程式對叢集上的磁碟區的請求所花費的時間比平時要長。高延遲的原因可能是叢集本身，因為一個或多個叢集元件存在爭用。高延遲也可能由叢集外部的問題引起，例如網路瓶頸、託管應用程式的用戶端問題或應用程式本身的問題。



Unified Manager 僅監控叢集上的工作負載活動。它不監控應用程式、客戶端或應用程式與叢集之間的路徑。

叢集上的操作（例如進行備份或執行重複資料刪除）會增加對其他工作負載共享的叢集元件的需求，也會導致高延遲。如果實際延遲超過預期範圍（延遲預測）的動態效能閾值，Unified Manager 會分析該事件以確定它是否是您可能需要解決的效能事件。延遲以每次操作的毫秒數 (ms/op) 來衡量。

在「工作負載分析」頁面的「總延遲」圖表上，您可以查看延遲統計資料的分析，以了解各個進程（例如讀取和寫入請求）的活動與整體延遲統計資料的比較。透過比較，您可以確定哪些操作具有最高的活動，或者特定操作是否具有影響磁碟區延遲的異常活動。在分析效能事件時，您可以使用延遲統計資料來確定事件是否由叢集上的問題引起。您也可以識別事件中涉及的特定工作負載活動或叢集元件。



此範例顯示了延遲圖表。實際反應時間（延遲）活動為藍線，延遲預測（預期範圍）為綠色。

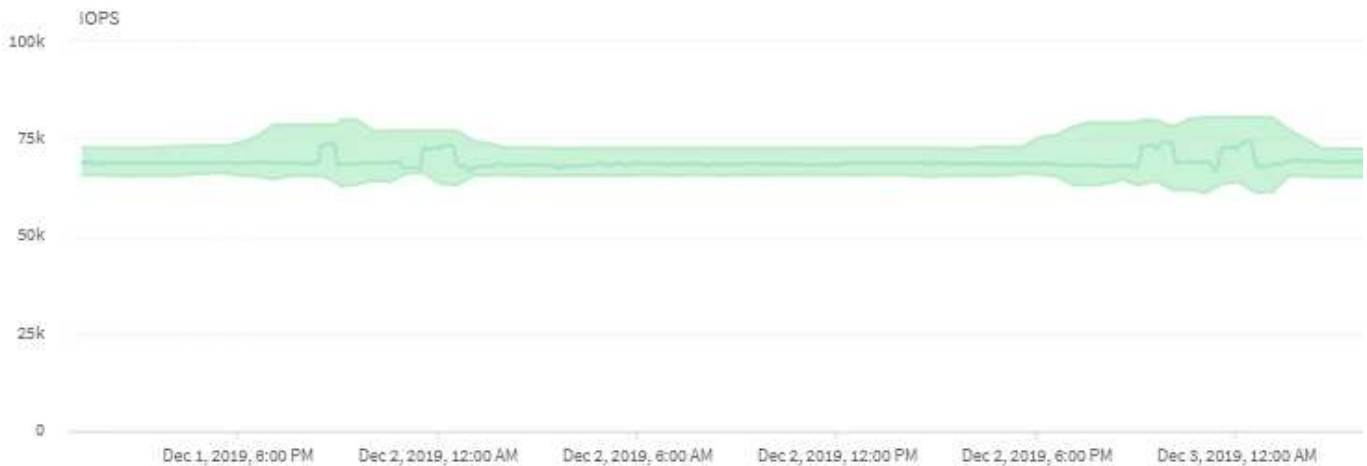


如果 Unified Manager 無法收集數據，藍線中可能會出現間隙。發生這種情況可能是因為叢集或磁碟區無法存取、Unified Manager 在此期間關閉或收集超過 5 分鐘的收集時間。

叢集操作如何影響工作負載延遲

操作（IOPS）代表叢集上所有使用者定義和系統定義的工作負載的活動。IOPS 統計資料可協助您確定叢集進程（例如進行備份或執行重複資料刪除）是否會影響工作負載延遲（回應時間）或可能導致或促成效能事件。

分析效能事件時，您可以使用 IOPS 統計資料來確定效能事件是否由叢集問題引起。您可以識別可能是效能事件主要影響因素的特定工作負載活動。IOPS 以每秒運算元 (ops/sec) 來衡量。



此範例顯示 IOPS 圖表。實際操作統計資料為藍線，操作統計資料的 IOPS 預測為綠色。



在某些情況下，當叢集過載時，Unified Manager 可能會顯示訊息 `Data collection is taking too long on Cluster cluster_name`。這意味著沒有收集足夠的統計資料供 Unified Manager 進行分析。您需要減少叢集正在使用的資源，以便收集統計資料。

MetroCluster 配置的效能監控

Unified Manager 讓您能夠監控 MetroCluster 配置中叢集之間的寫入吞吐量，以識別具有大量寫入吞吐量的工作負載。

如果這些高效能工作負載導致本機叢集上的其他磁碟區具有較高的 I/O 回應時間，Unified Manager 會觸發效能事件來通知您。



Unified Manager 將 MetroCluster 配置中的叢集視為單獨的叢集。它不區分合作夥伴群集或關聯每個群集的寫入吞吐量。

當 MetroCluster 配置中的本地叢集將其資料鏡像到其夥伴叢集時，資料將寫入 NVRAM，然後透過交換器間連結 (ISL) 傳輸到遠端聚合。Unified Manager 分析 NVRAM 以識別高寫入吞吐量過度利用 NVRAM 的工作負載，從而使 NVRAM 處於爭用狀態。

反應時間偏差超過效能門檻的工作負荷稱為 `_受害者_`，而寫入 NVRAM 的吞吐量偏差高於平常、導致爭用的工作負荷稱為 `_霸凌者_`。由於只有寫入請求鏡像到夥伴群集，因此 Unified Manager 不會分析讀取吞吐量。

您可以從下列畫面分析對應 LUN 和磁碟區的工作負載來查看 MetroCluster 配置中任何叢集的吞吐量。您可以按叢集過濾結果。從左側導覽窗格：

- 儲存 > 叢集 > 效能：所有叢集 視圖。看
- 儲存 > 磁碟區 > 效能：所有磁碟區 視圖。
- 儲存 > LUN > 效能：所有 LUN 視圖。
- 工作負載分析 > 所有工作負載

相關資訊

["效能事件分析和通知"](#)

"MetroCluster配置的效能事件分析"

"效能事件中涉及的工作負載的角色"

"識別效能事件中涉及的受害工作負載"

"識別績效事件中涉及的霸凌工作負載"

"識別效能事件中涉及的shark工作負載"

了解性能事件和警報

效能事件是與叢集上的工作負載效能相關的事件。它們可以幫助您識別響應時間較慢的工作負載。結合同時發生的健康事件，您可以確定可能導致或造成反應時間緩慢的問題。

當 Unified Manager 偵測到相同叢集元件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。

您可以設定警報，以便在發生某些嚴重程度類型的效能事件時自動發送電子郵件通知。

性能事件的來源

效能事件是與叢集上的工作負載效能相關的問題。它們可以幫助您識別響應時間較慢（也稱為高延遲）的儲存物件。結合同時發生的其他健康事件，您可以確定可能導致或造成反應時間緩慢的問題。

Unified Manager 從下列來源接收效能事件：

- 使用者定義的效能閾值策略事件

基於您設定的自訂閾值的效能問題。您可以為儲存物件（例如聚合和磁碟區）配置效能閾值策略，以便在效能計數器的閾值被突破時產生事件。

您必須定義效能閾值策略並將其指派給儲存物件以接收這些事件。

- 系統定義的效能閾值策略事件

基於系統定義的閾值的效能問題。這些閾值策略包含在 Unified Manager 的安裝中，以解決常見的效能問題。

這些閾值策略預設啟用，您可能會在新增叢集後不久看到事件。

- 動態效能閾值事件

由於 IT 基礎架構故障或錯誤，或工作負載過度利用叢集資源而導致的效能問題。這些事件的原因可能是一個簡單的問題，可以在一段時間內自行解決，或者可以透過修復或配置變更來解決。動態閾值事件表示 ONTAP 系統上的工作負載因其他工作負載對共用叢集元件的使用率較高而導致運作速度較慢。

這些閾值預設啟用，您可能會在從新叢集收集資料三天後看到事件。

效能事件嚴重性類型

每個效能事件都與一個嚴重性類型相關聯，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

發生了效能事件，如果不立即採取糾正措施，可能會導致服務中斷。

關鍵事件僅從使用者定義的閾值發送。

- 警告

群集對象的效能計數器超出正常範圍，應進行監控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。

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。

有關詳細信息，請參閱以下連結：

- ["收到事件時會發生什麼"](#)
- ["警報電子郵件包含哪些訊息"](#)
- ["添加警報"](#)
- ["新增性能事件警報"](#)

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。

系統定義的效能閾值策略的類型

Unified Manager 提供了一些標準閾值策略，用於監控叢集效能並自動產生事件。這些策略預設為啟用，當監控的效能閾值被突破時，它們會產生警告或資訊事件。



Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系統上未啟用系統定義的效能閾值策略。

如果您從任何系統定義的效能閾值策略收到不必要的事件，您可以從事件設定頁面停用單一策略的事件。

集群閾值策略

預設情況下，系統定義的叢集效能閾值策略會指派給 Unified Manager 監控的每個叢集：

- 叢集負載不平衡

識別一個節點的負載比叢集中其他節點高得多的情況，因此可能會影響工作負載延遲。

它透過比較叢集中所有節點的效能容量使用值來查看是否有任何節點超過 30% 的閾值超過 24 小時。這是一個警告事件。

- 叢集容量不平衡

識別一個聚合的已使用容量比叢集中的其他聚合高得多的情況，因此可能會影響操作所需的空間。

它透過比較叢集中所有聚合的已使用容量值來查看聚合之間是否存在 70% 的差異。這是一個警告事件。

節點閾值策略

預設情況下，系統定義的節點效能閾值策略會指派給 Unified Manager 監控的叢集中的每個節點：

- 已突破性能容量使用門檻

識別單一節點的運作效率超出其界限並因此可能影響工作負載延遲的情況。

它透過尋找使用效能容量超過 100% 且持續時間超過 12 小時的節點來實現這一點。這是一個警告事件。

- 節點 HA 對過度使用

識別 HA 對中的節點運行超出 HA 對運行效率界限的情況。

它透過查看 HA 對中兩個節點的效能容量使用值來實現這一點。如果兩個節點使用的效能容量總和超過 200% 且持續時間超過 12 小時，則控制器故障轉移將影響工作負載延遲。這是一個資訊事件。

- 節點磁碟碎片

識別聚合中的一個或多個磁碟碎片化的情況，從而降低關鍵系統服務的速度並可能影響節點上的工作負載延遲。

它透過查看節點上所有聚合的某些讀寫操作比率來實現這一點。在 SyncMirror 重新同步期間或在磁碟清理操作期間發現錯誤時也可能會觸發此策略。這是一個警告事件。



「節點磁碟碎片」策略僅分析 HDD 聚合；不分析 Flash Pool、SSD 和 FabricPool 聚合。

聚合閾值策略

系統定義的聚合效能閾值策略預設指派給 Unified Manager 監控的叢集中的每個聚合：

- 聚合磁碟過度利用

識別聚合運作超出其運作效率極限的情況，從而可能影響工作負載延遲。它透過尋找聚合中磁碟利用率超過 95% 且持續時間超過 30 分鐘的聚合來識別這些情況。然後，此多條件策略執行以下分析以幫助確定問題的原因：

- 聚合中的磁碟目前是否正在進行後台維護活動？

磁碟可能正在進行的一些後台維護活動包括磁碟重建、磁碟清理、SyncMirror 重新同步和重新奇偶校驗。

- 磁碟架光纖通道互連是否存在通訊瓶頸？
- 整體而言，可用空間是否太少？只有當三項下屬政策中的一項（或多項）也被視為違反時，才會針對該政策發出警告事件。如果僅聚合中的磁碟利用率超過 95%，則不會觸發效能事件。



「聚合磁碟過度利用」策略分析僅 HDD 聚合和 Flash Pool（混合）聚合；不分析 SSD 和 FabricPool 聚合。

工作負載延遲閾值策略

系統定義的工作負載延遲閾值策略指派給任何具有已配置效能服務等級策略且具有已定義「預期延遲」值的工作負載：

- 工作負載磁碟區/LUN 延遲閾值超出效能服務等級定義

識別超出其「預期延遲」限制並影響工作負載效能的磁碟區（檔案共用）和 LUN。這是一個警告事件。

它透過尋找前一小時內 30% 的時間內超過預期延遲值的工作負載來實現這一點。

QoS 閾值策略

系統定義的 QoS 效能閾值策略指派給任何具有配置的 ONTAP QoS 最大吞吐量策略（IOPS、IOPS/TB 或 MB/s）的工作負載。當工作負載吞吐量值比配置的 QoS 值低 15% 時，Unified Manager 會觸發一個事件：

- **QoS 最大 IOPS 或 MB/s 閾值**

識別已超出其 QoS 最大 IOPS 或 MB/s 吞吐量限制並影響工作負載延遲的捲和 LUN。這是一個警告事件。

當將單一工作負載指派給策略群組時，它會透過尋找前一小時每個收集期間內超過指派的 QoS 策略群組中定義的最大吞吐量閾值的工作負載來實現此目的。

當多個工作負載共用單一 QoS 策略時，它會透過將策略中所有工作負載的 IOPS 或 MB/s 相加並根據閾值檢查總數來實現此目的。

- **QoS 峰值 IOPS/TB 或具有區塊大小閾值的 IOPS/TB**

識別已超出其自適應 QoS 峰值 IOPS/TB 吞吐量限制（或具有區塊大小限制的 IOPS/TB）且影響工作負載延遲的磁碟區。這是一個警告事件。

它透過將自適應 QoS 策略中定義的峰值 IOPS/TB 閾值轉換為基於每個磁碟區大小的 QoS 最大 IOPS 值來實現此目的，然後尋找在前一小時的每個效能收集期間超過 QoS 最大 IOPS 的捲。



只有當叢集安裝了 ONTAP 9.3 及更高版本的軟體時，此策略才適用於磁碟區。

當自適應 QoS 策略中定義了「區塊大小」元素時，閾值將根據每個磁碟區的大小轉換為 QoS 最大 MB/s 值。然後，它會查找前一小時每個效能收集期間內超過 QoS 最大 MB/s 的捲。



只有當叢集安裝了 ONTAP 9.5 及更高版本的軟體時，此策略才適用於磁碟區。

效能事件分析和通知

效能事件會通知您因叢集元件爭用而導致的工作負載的 I/O 效能問題。Unified Manager 會分析該事件以確定所涉及的所有工作負載、存在爭用的元件以及該事件是否仍是您可能需要解決的問題。

Unified Manager 監控叢集上磁碟區的 I/O 延遲（回應時間）和 IOPS（操作）。例如，當其他工作負載過度使用叢集元件時，該元件就會發生爭用，無法以最佳水平運作以滿足工作負載需求。使用相同組件的其他工作負載的效能可能會受到影響，導致其延遲增加。如果延遲超過動態效能閾值，Unified Manager 會觸發效能事件來通知您。

事件分析

Unified Manager 使用前 15 天的效能統計資料執行以下分析，以識別事件中涉及的受害者工作負載、霸凌工作負載和叢集元件：

- 識別延遲已超過動態效能閾值（即延遲預測的上限）的受害者工作負載：
 - 對於 HDD 或 Flash Pool 混合聚合（本地層）上的捲，僅當延遲大於 5 毫秒 (ms) 且 IOPS 超過每秒 10 次操作 (ops/sec) 時才會觸發事件。
 - 對於全 SSD 聚合或 FabricPool 聚合（雲層）上的捲，僅當延遲大於 1 毫秒且 IOPS 大於 100 操作/秒時才會觸發事件。
- 識別處於爭用的集群組件。



如果叢集互連處受害工作負載的延遲大於 1 毫秒，Unified Manager 會將其視為重大事件並觸發叢集互連事件。

- 識別過度使用叢集元件並導致其發生爭用的霸凌工作負載。
- 根據群集組件的使用率或活動的偏差對所涉及的工作負載進行排序，以確定哪些霸凌者對群集組件的使用變化最大，以及哪些受害者受到的影響最大。

事件可能只會發生短暫的一瞬間，然後在其使用的元件不再爭用後自行修正。連續事件是指在五分鐘間隔內針對同一群集元件重複發生並保持活動狀態的事件。對於連續事件，Unified Manager 在兩個連續的分析間隔內偵測到相同事件後會觸發警報。

事件解決後，它將保留在 Unified Manager 中，作為磁碟區過去效能問題記錄的一部分。每個事件都有一個唯一的 ID，用於識別事件類型以及所涉及的磁碟區、叢集和叢集元件。



單一卷可以同時涉及多個事件。

事件狀態

事件可以處於以下狀態之一：

- 積極的

表示效能事件目前處於活動狀態（新的或已確認）。導致該事件的問題尚未自行修正或尚未解決。儲存物件的效能計數器仍然高於效能閾值。

- 過時的

表示該事件不再有效。導致該事件的問題已自行修正或已解決。儲存物件的效能計數器不再高於效能閾值。

事件通知

這些事件顯示在儀表板頁面和使用者介面的許多其他頁面上，並且這些事件的警報會傳送到指定的電子郵件地址。您可以在事件詳情頁面和工作負載分析頁面查看事件的詳細分析資訊並獲得解決該事件的建議。

事件交互

在事件詳情頁面和工作負載分析頁面，您可以透過以下方式與事件互動：

- 將滑鼠移到事件上會顯示一則訊息，顯示偵測到該事件的日期和時間。

如果在同一時間段內有多個事件，則訊息會顯示事件的數量。

- 點擊單一事件將顯示一個對話框，其中顯示有關該事件的更多詳細信息，包括所涉及的叢集元件。

有爭議的組件被圈出並以紅色突出顯示。您可以點擊「查看完整分析」在事件詳情頁面查看完整分析。如果同一時間段內有多個事件，對話方塊將顯示最近三個事件的詳細資訊。您可以點擊某個事件，在事件詳情頁面查看該事件的分析。

Unified Manager 如何決定事件對效能的影響

Unified Manager 使用工作負載的活動、使用率、寫入吞吐量、叢集元件使用率或 I/O 延遲（回應時間）的偏差來確定對工作負載效能的影響等級。此資訊決定了事件中每個工作負載的角色以及它們在事件詳細資訊頁面上的排名方式。

Unified Manager 將工作負載的最後分析值與預期值範圍（延遲預測）進行比較。最後分析的值與預期值範圍之間的差異可確定受事件影響最大的工作負載。

例如，假設一個叢集包含兩個工作負載：工作負載 A 和工作負載 B。工作負載 A 的延遲預測為每操作 5-10 毫秒 (ms/op)，而其實際延遲通常在 7 ms/op 左右。工作負載 B 的延遲預測為 10-20 ms/op，其實際延遲通常在 15 ms/op 左右。兩種工作負載都完全符合其延遲預測。由於叢集上的爭用，兩個工作負載的延遲都增加到 40 ms/op，超過了動態效能閾值（即延遲預測的上限），並觸發事件。對於工作負載 A，從預期值到效能閾值以上的值的延遲偏差約為 33 ms/op，而對於工作負載 B，延遲偏差約為 25 ms/op。兩種工作負載的延遲都飆升至 40 ms/op，但工作負載 A 對效能的影響更大，因為它的延遲偏差更高，為 33 ms/op。

在「事件詳細資料」頁面的「系統診斷」部分中，您可以根據叢集元件的活動、使用率或吞吐量偏差對工作負載進行排序。您也可以按延遲對工作負載進行排序。當您選擇排序選項時，Unified Manager 會分析自偵測到事件以來活動、使用率、吞吐量或延遲與預期值的偏差，以決定工作負載排序順序。對於延遲，紅點 (●) 表示受害工作負載跨越了效能閾值，以及隨後對延遲的影響。每個紅點表示延遲的更高偏差水平，這有助於您識別受事件影響最大的延遲受害者工作負載。

集群組件及其爭用的原因

當叢集元件發生爭用時，您可以識別叢集效能問題。使用該元件的工作負載的效能會變慢，且其對用戶端請求的回應時間（延遲）會增加，從而觸發 Unified Manager 中的事件。

存在爭用的組件無法達到最佳效能。它的性能已經下降，並且其他群組件和工作負載（稱為“受害者”）的性能可能會增加延遲。要使組件擺脫爭用，必須減少其工作負載或提高其處理更多工作的能力，以便效能恢復到正常水準。由於 Unified Manager 以五分鐘為間隔收集和分析工作負載效能，因此它僅偵測叢集元件何時持續過度使用。未偵測到在五分鐘間隔內僅持續很短時間的過度使用瞬態峰值。

例如，儲存聚合可能處於爭用狀態，因為其上的一個或多個工作負載正在競爭滿足其 I/O 請求。聚合上的其他工作負載可能會受到影響，導致其效能下降。為了減少聚合上的活動量，您可以採取不同的步驟，例如將一個或多個工作負載移至較不繁忙的聚合或節點，以減少目前聚合上的整體工作負載需求。對於 QoS 策略群組，您可以調整吞吐量限制，或將工作負載移至其他策略群組，這樣工作負載就不會再受到限制。

Unified Manager 監控以下叢集元件，並在它們發生爭用時提醒您：

- 網路

表示叢集上外部網路協定的 I/O 請求的等待時間。等待時間是指叢集回應 I/O 請求之前等待「傳輸就緒」事務完成所花費的時間。如果網路元件處於爭用狀態，則表示協定層的高等待時間會影響一個或多個工作負載的延遲。

- 網路處理

表示集群中涉及協定層和集群之間的 I/O 處理的軟體元件。自從偵測到該事件以來，處理網路處理的節點可能已經發生變化。如果網路處理元件存在爭用，則表示網路處理節點的高利用率正在影響一個或多個工作負載的延遲。

在主動-主動配置中使用全 SAN 陣列群集時，將顯示兩個節點的網路處理延遲值，以便您可以驗證節點是否

平等地共享負載。

- **QoS 限制最大值**

表示指派給工作負載的儲存服務品質 (QoS) 策略群組的最大吞吐量 (峰值) 設定。如果策略群組元件存在爭用，則表示策略群組中的所有工作負載都受到設定的吞吐量限制的限制，這會影響其中一個或多個工作負載的延遲。

- **QoS 限制最小值**

表示由分配給其他工作負載的 QoS 吞吐量最小 (預期) 設定導致的工作負載延遲。如果某些工作負載上設定的 QoS 最小值使用大部分頻寬來保證承諾的吞吐量，則其他工作負載將受到限制並出現更多延遲。

- **集群互連**

表示叢集節點實體連接的電纜和適配器。如果叢集互連元件處於爭用狀態，則表示叢集互連處 I/O 請求的等待時間過長會影響一個或多個工作負載的延遲。

- **Data Processing**

表示叢集中涉及叢集與包含工作負載的儲存聚合之間的 I/O 處理的軟體元件。自從偵測到事件以來，處理資料處理的節點可能已經發生變化。如果資料處理元件存在爭用，則表示資料處理節點的高利用率正在影響一個或多個工作負載的延遲。

- **音量啟動**

表示追蹤所有活動卷使用情況的進程。在有超過 1000 個磁碟區處於活動狀態的大型環境中，此流程會追蹤有多少個關鍵磁碟區需要同時透過節點存取資源。當並發活動卷的數量超過建議的最大閾值時，一些非關鍵卷將會出現此處標識的延遲。

- *** MetroCluster資源***

表示MetroCluster資源，包括NVRAM和交換器間連結 (ISL)，用於在MetroCluster配置中的叢集之間鏡像資料。如果MetroCluster元件存在爭用，則表示本地叢集上的工作負載的高寫入吞吐量或連結健康問題正在影響本地叢集上一個或多個工作負載的延遲。如果叢集不在MetroCluster配置中，則不會顯示此圖示。

- **聚合或 SSD 聚合操作**

表示運行工作負載的儲存聚合。如果聚合元件存在爭用，則表示聚合的高利用率正在影響一個或多個工作負載的延遲。聚合由所有 HDD 組成，或由 HDD 和 SSD 的混合 (Flash Pool 聚合) 組成，或由 HDD 和雲層的混合 (FabricPool聚合) 組成。「SSD 聚合」由所有 SSD (全快閃聚合) 或 SSD 和雲層 (FabricPool 聚合) 的混合組成。

- **雲延遲**

表示叢集中涉及叢集和儲存使用者資料的雲層之間的 I/O 處理的軟體元件。如果雲端延遲元件存在爭用，則表示託管在雲層上的磁碟區的大量讀取會影響一個或多個工作負載的延遲。

- **同步SnapMirror**

表示叢集中涉及在SnapMirror同步關係中將使用者資料從主磁碟區複製到輔助磁碟區的軟體元件。如果同步SnapMirror元件存在爭用，則表示SnapMirror同步操作的活動正在影響一個或多個工作負載的延遲。

效能事件中涉及的工作負載的角色

Unified Manager 使用角色來識別工作負載在效能事件中的參與情況。角色包括受害者、霸凌者和鯊魚。使用者定義的工作負載可以同時是受害者、霸凌者和鯊魚。

角色	描述
受害者	一種使用者定義的工作負載，由於其他工作負載（稱為“bullies”）過度使用叢集元件，導致其效能下降。只有使用者定義的工作負載才會被識別為受害者。Unified Manager 根據延遲偏差來識別受害工作負載，其中事件期間的實際延遲與其延遲預測（預期範圍）相比大大增加。
霸凌	使用者定義或系統定義的工作負載，其過度使用叢集元件導致其他工作負載（稱為受害者）的效能下降。Unified Manager 根據群集元件使用情況的偏差來識別霸凌工作負載，其中事件期間的實際使用情況大大超出了其預期的使用範圍。
鯊魚	與事件中涉及的所有工作負載相比，叢集元件使用率最高的使用者定義工作負載。Unified Manager 根據事件期間叢集元件的使用情況來識別 shark 工作負載。

叢集上的工作負載可以共用許多叢集元件，例如聚合以及用於網路和資料處理的 CPU。當工作負載（例如磁碟區）對叢集元件的使用率增加到該元件無法有效滿足工作負載需求的程度時，該元件就會處於爭用狀態。過度使用叢集組件的工作負載是一個惡霸。共享這些組件的其他工作負載，其表現受到霸凌的影響，是受害者。系統定義的工作負載（例如重複資料刪除或 Snapshot 副本）的活動也可能升級為「霸凌」。

當 Unified Manager 偵測到事件時，它會識別所涉及的所有工作負載和叢集元件，包括導致事件的霸凌工作負載、處於爭用的叢集元件以及由於霸凌工作負載活動增加而導致效能下降的受害工作負載。



如果 Unified Manager 無法辨識霸凌工作負載，它只會對受害工作負載和所涉及的叢集元件發出警報。

Unified Manager 可以辨識受霸凌工作負荷影響的工作負載，也能辨識這些工作負載何時成為霸凌工作負載。工作量本身就可能是一種負擔。例如，受到策略群組限制限制的高效能工作負載會導致策略群組中的所有工作負載（包括其本身）受到限制。在正在進行的績效事件中作為霸凌者或受害者的工作負荷可能會改變其角色或不再是該事件的參與者。

管理績效閾值

效能閾值策略可讓您確定 Unified Manager 產生事件的時間點，以便通知系統管理員可能影響工作負載效能的問題。這些閾值策略被稱為_使用者定義_效能閾值。

此版本支援使用者定義、系統定義和動態效能閾值。透過動態和系統定義的效能閾值，Unified Manager 可以分析工作負載活動以確定適當的閾值。使用使用者定義的閾值，您可以為許多效能計數器和許多儲存物件定義效能上限。



系統定義的效能閾值和動態效能閾值由 Unified Manager 設定，無法設定。如果您從任何系統定義的效能閾值策略收到不必要的事件，您可以從事件設定頁面停用單一策略。

使用者定義的效能閾值策略如何運作

您可以在儲存物件（例如，聚合和磁碟區）上設定效能閾值策略，以便可以向儲存管理員發送事件，通知管理員叢集正在遇到效能問題。

您可以透過以下方式為儲存物件建立效能閾值策略：

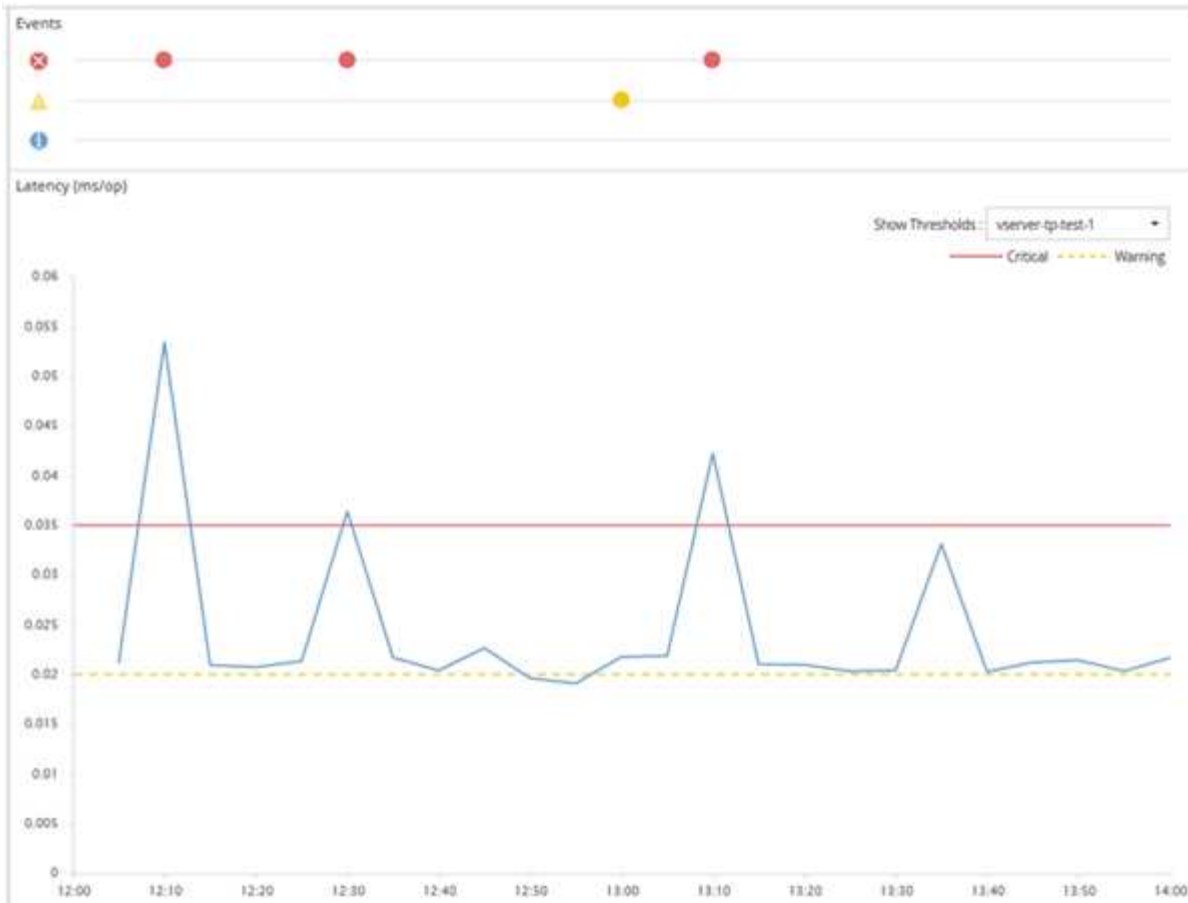
- 選擇儲存對象
- 選擇與該物件關聯的效能計數器
- 指定定義被視為警告和嚴重情況的性能計數器上限的值
- 指定一個時間段，定義計數器必須超過上限的時間

例如，您可以在磁碟區上設定效能閾值策略，以便每當該磁碟區的 IOPS 連續 10 分鐘超過每秒 750 次操作時，您都會收到關鍵事件通知。相同的閾值策略還可以指定當 IOPS 超過每秒 500 次操作持續 10 分鐘時發送警告事件。



當前版本提供了閾值，當計數器值超過閾值設定時會發送事件。您無法設定在計數器值低於閾值設定時發送事件的閾值。

這裡顯示了一個範例計數器圖表，顯示警告閾值（黃色圖示）在 1:00 被突破，並且關鍵閾值（紅色圖示）在 12:10、12:30 和 1:10 被突破：



閾值突破必須在指定的持續時間內持續發生。如果閾值因任何原因低於限制值，則後續違規將被視為新持續時間的開始。

一些叢集物件和效能計數器使您能夠建立組合閾值策略，該策略要求兩個效能計數器在生成事件之前超過其最大限制。例如，您可以使用下列條件建立閾值策略：

集群對象	性能計數器	警告閾值	臨界閾值	期間
體積	延遲	10毫秒	20毫秒	15分鐘
總計的	使用率	65%	85%	

使用兩個集群物件的閾值策略僅當同時滿足兩個條件時才會產生事件。例如，使用表中定義的閾值策略：

如果音量延遲是平均的...	並且總磁碟利用率是...	然後...
15毫秒	50%	未報告任何事件。
15毫秒	75%	報告警告事件。
25毫秒	75%	報告警告事件。
25毫秒	90%	已報告嚴重事件。

當違反績效閾值策略時會發生什麼

當計數器值超過其定義的效能閾值並持續指定的時間量時，將突破閾值並報告事件。

此事件導致啟動以下操作：

- 此事件顯示在儀表板、效能群集摘要頁面、事件頁面和特定於物件的效能清單頁面中。
- (可選) 可以向一個或多個電子郵件收件者發送有關該事件的電子郵件警報，並且可以向陷阱接收器發送 SNMP 陷阱。
- (可選) 可以執行腳本來自動修改或更新儲存物件。

第一個動作總是被執行。您可以在「警報設定」頁面中設定是否執行可選操作。您可以根據是否違反警告或嚴重閾值策略來定義獨特的操作。

在儲存物件上發生效能閾值策略違規後，不會為該策略產生進一步的事件，直到計數器值低於閾值，此時該限制的持續時間將重設。當閾值不斷被超出時，事件的結束時間會不斷更新，以反映該事件正在進行中。

閾值事件捕獲或凍結與嚴重性和策略定義相關的信息，以便唯一閾值信息隨事件一起顯示，即使將來修改閾值策略也是如此。

可以使用閾值追蹤哪些效能計數器

一些常見的效能計數器，例如 IOPS 和 MB/s，可以為所有儲存物件設定閾值。還有其他計數器可以僅為某些儲存物件設定閾值。

可用的性能計數器

儲存對象	性能計數器	描述
簇	每秒輸入/輸出次數	集群每秒處理的平均輸入/輸出操作數。
MB/秒	每秒傳輸到該集群和從該集群傳輸的平均資料兆位元組數。	節點
每秒輸入/輸出次數	節點每秒處理的平均輸入/輸出運算元。	MB/秒
每秒傳輸到該節點和從該節點傳輸的平均資料兆位元組數。	延遲	節點響應應用程式請求所需的平均毫秒數。
使用率	節點的 CPU 和 RAM 的平均使用百分比。	已使用的性能容量
節點消耗的效能容量的平均百分比。	已使用的效能容量 - 接管	節點所消耗的效能容量的平均百分比，加上其夥伴節點的效能容量。

儲存對象	性能計數器	描述
總計的	每秒輸入/輸出次數	聚合每秒處理的平均輸入/輸出運算元。
MB/秒	每秒傳輸到該聚合體和從該聚合體傳輸的平均資料兆位元組數。	延遲
聚合響應應用程式請求所需的平均毫秒數。	使用率	正在使用的聚合磁碟的平均百分比。
已使用的性能容量	聚合所消耗的性能容量的平均百分比。	儲存虛擬機
每秒輸入/輸出次數	SVM 每秒處理的平均輸入/輸出運算元。	MB/秒
每秒傳輸到和從此 SVM 的資料的平均兆位元組數。	延遲	SVM 回應應用程式請求所需的平均毫秒數。
體積	每秒輸入/輸出次數	此卷每秒處理的平均輸入/輸出操作數。
MB/秒	每秒傳輸到該磁碟區和從該磁碟區傳輸的平均資料兆位元組數。	延遲
卷響應應用程式請求所需的平均毫秒數。	快取未命中率	來自客戶端應用程式的讀取請求中，從磁碟區返回而不是從快取返回的平均百分比。
邏輯單元號	每秒輸入/輸出次數	LUN 每秒處理的平均輸入/輸出運算元。
MB/秒	每秒傳輸到該 LUN 和從該 LUN 傳輸的平均資料兆位元組數。	延遲
LUN 回應應用程式請求所需的平均毫秒數。	命名空間	每秒輸入/輸出次數
命名空間每秒處理的輸入/輸出操作的平均數。	MB/秒	每秒傳輸到該命名空間和從該命名空間傳輸的平均資料兆位元組數。
延遲	命名空間響應應用程式請求所需的平均毫秒數。	港口
頻寬利用率	正在使用的連接埠可用頻寬的平均百分比。	MB/秒

儲存對象	性能計數器	描述
每秒傳輸到該連接埠和從該連接埠傳輸的平均資料兆位元組數。	網路介面 (LIF)	MB/秒

哪些物件和計數器可以組合使用閾值策略

組合策略中只能使用部分效能指標。當指定主性能計數器和輔助性能計數器時，兩個性能計數器都必須超過其最大限制才會產生事件。

主儲存物件和計數器	二級儲存物件和計數器
卷延遲	卷 IOPS
體積 MB/s	總利用率
已使用的總性能容量	節點利用率
節點效能容量使用情況	節點效能容量使用 - 接管
LUN延遲	LUN IOPS
LUN MB/秒	總利用率
已使用的總性能容量	節點利用率
節點效能容量使用情況	節點效能容量使用 - 接管



當磁碟區組合策略應用於FlexGroup磁碟區而非FlexVol volume時，只能選擇「Volume IOPS」和「Volume MB/s」屬性作為輔助計數器。如果閾值策略包含節點或聚合屬性之一，則該策略將不會應用於FlexGroup卷，並且您將收到描述這種情況的錯誤訊息。這是因為FlexGroup磁碟區可以存在於多個節點或聚合上。

建立使用者定義的效能閾值策略

您可以為儲存物件建立效能閾值策略，以便在效能計數器超過特定值時發送通知。事件通知表明叢集正在經歷效能問題。

開始之前

您必須具有應用程式管理員角色。

您可以透過在「建立效能閾值策略」頁面上輸入閾值來建立效能閾值策略。您可以透過定義此頁面中的所有策略值來建立新策略，也可以複製現有策略並變更副本中的值（稱為_複製_）。

有效閾值為數字 0.001 到 10,000,000、百分比 0.001-100 和效能容量使用百分比 0.001-200。



當前版本提供了閾值，當計數器值超過閾值設定時會發送事件。您無法設定在計數器值低於閾值設定時發送事件的閾值。

步驟

1. 在左側導覽窗格中，選擇「事件閾值」>「效能」。

將顯示“效能閾值”頁面。

2. 根據您是想建立新策略還是想克隆類似策略並修改克隆版本來點擊相應的按鈕。

到...	點擊...
建立新策略	創造
克隆現有策略	選擇現有策略並點擊*克隆*

進入「建立效能閾值策略」或「複製效能閾值策略」頁面。

3. 透過指定要為特定儲存物件設定的效能計數器閾值來定義閾值策略：

- a. 選擇儲存物件類型並為策略指定名稱和描述。
- b. 選擇要追蹤的效能計數器並指定定義警告和嚴重事件的限制值。

您必須定義至少一個警告限值或一個臨界值。您不需要定義兩種類型的限制。

- c. 如果需要，請選擇一個輔助效能計數器，並指定警告和嚴重事件的限制值。

包括輔助計數器要求兩個計數器都超過限制值，然後才會突破閾值並報告事件。只能使用組合策略來配置某些物件和計數器。

- d. 選擇必須突破限制值才會發送事件的持續時間。

複製現有策略時，必須為該策略輸入新名稱。

4. 按一下“儲存”以儲存該策略。

您將返回到“效能閾值”頁面。頁面頂部的成功訊息確認閾值策略已創建，並提供該物件類型的庫存頁面鏈接，以便您可以立即將新策略應用於儲存物件。

如果此時您想將新的閾值策略套用至儲存對象，您可以按一下「立即前往 object_type」連結前往「庫存」頁面。

為儲存物件指派效能閾值策略

您可以將使用者定義的效能閾值策略指派給儲存對象，以便當效能計數器的值超過策略設定時，Unified Manager 會報告事件。

開始之前

您必須具有應用程式管理員角色。

您要套用於物件的效能閾值策略或策略必須存在。

一次只能將一個效能策略應用於一個物件或一組物件。

您最多可以為每個儲存物件指派三個閾值策略。將策略指派給多個物件時，如果任何物件已指派最大數量的策略，則 Unified Manager 將執行下列操作：

- 將策略應用於所有未達到其最大值的選取對象
- 忽略已達到最大策略數量的對象
- 顯示一則訊息，表示該策略未指派給所有對象

步驟

1. 從任意儲存物件的效能清單頁面中，選擇要指派閾值策略的一個或多個物件：

分配閾值給...	點擊...
單一對象	該物件左側的複選框。
多個物件	每個物件左側的複選框。
頁面上的所有對象	這 <input type="checkbox"/> 下拉框，然後選擇*選擇此頁面上的所有物件*。
所有同一類型的對象	這 <input type="checkbox"/> 下拉框，然後選擇*選擇所有物件*。

您可以使用排序和篩選功能來最佳化清單頁面上的物件列表，以便更輕鬆地將閾值策略套用到許多物件。

2. 做出選擇，然後按一下「指派效能閾值策略」。

將顯示「指派效能閾值策略」頁面，其中顯示了針對該特定類型儲存物件存在的閾值策略清單。

3. 點擊每個策略以顯示效能閾值設定的詳細信息，以驗證您是否選擇了正確的閾值策略。
4. 選擇適當的閾值策略後，按一下「指派策略」。

頁面頂部的成功訊息確認閾值策略已指派給該對象或多個對象，並提供指向警報頁面的鏈接，以便您可以為該對象和策略配置警報設定。

如果您希望透過電子郵件傳送警報或以 SNMP 陷阱的形式通知您已產生特定效能事件，則必須在警報設定頁面中設定警報設定。

查看效能閾值策略

您可以從「效能閾值」頁面查看所有目前定義的效能閾值策略。

閾值策略清單按策略名稱的字母順序排序，其中包括針對所有類型儲存物件的策略。您可以按一下列標題來按該列對策略進行排序。如果您正在尋找特定的策略，請使用過濾和搜尋機制來最佳化庫存清單中出現的閾值策略清單。

您可以將遊標停留在策略名稱和條件名稱上以查看策略的配置詳細資訊。此外，您可以使用提供的按鈕來建立、複製、編輯和刪除使用者定義的閾值策略。

步

1. 在左側導覽窗格中，選擇「事件閾值」>「效能」。

將顯示“效能閾值”頁面。

編輯使用者定義的效能閾值策略

您可以編輯現有效能閾值策略的閾值設定。如果您發現收到的某些閾值條件下的警報過多或過少，這可能會很有用。

開始之前

您必須具有應用程式管理員角色。

您無法變更現有閾值策略的策略名稱或正在監視的儲存物件的類型。

步驟

1. 在左側導覽窗格中，選擇「事件閾值」>「效能」。

顯示“效能閾值”頁面。

2. 選擇要變更的閾值策略，然後按一下「編輯」。

將顯示「編輯效能閾值策略」頁面。

3. 對閾值策略進行更改，然後按一下「儲存」。

您將返回到“效能閾值”頁面。

儲存後，變更將立即更新至使用該原則的所有儲存物件上。

根據您對策略所做變更的類型，您可能需要查看在警報設定頁面中為使用該策略的物件配置的警報設定。

從儲存物件中刪除效能閾值策略

當您不再希望 Unified Manager 監控效能計數器的值時，您可以從儲存物件中刪除使用者定義的效能閾值策略。

開始之前

您必須具有應用程式管理員角色。

每次只能從選取物件中刪除一個策略。

您可以透過在清單中選擇多個儲存物件來從多個儲存物件中刪除閾值策略。

步驟

1. 從任何儲存物件的*庫存*頁面中，選擇一個或多個應用了至少一個效能閾值策略的物件。

清除...的閾值	這樣做...
單一對象	選取該物件左側的複選框。
多個物件	選取每個物件左側的複選框。
頁面上的所有對象	點選  在列標題中。

2. 按一下“清除效能閾值策略”。

將顯示「清除閾值策略」頁面，其中顯示目前指派給儲存物件的閾值策略清單。

3. 選擇要從物件中刪除的閾值策略，然後按一下「清除策略」。

當您選擇閾值策略時，將顯示該策略的詳細信息，以便您確認已選擇適當的策略。

當效能閾值策略改變時會發生什麼

如果調整現有效能閾值策略的計數器值或持續時間，則策略變更將應用於使用該策略的所有儲存物件。新的設定會立即生效，並且 Unified Manager 開始將效能計數器值與所有新收集的效能資料的新閾值設定進行比較。

如果使用變更的閾值策略的物件存在任何活動事件，則這些事件將被標記為過時，並且閾值策略將開始作為新定義的閾值策略監視計數器。

在計數器圖表詳細視圖中查看已套用閾值的計數器時，臨界閾值線和警告閾值線反映當前閾值設定。即使您查看舊閾值設定生效時的歷史數據，原始閾值設定也不會出現在此頁面上。



由於較舊的閾值設定不會出現在計數器圖表詳細視圖中，因此您可能會看到出現在目前閾值線以下的歷史事件。

當物件移動時效能閾值策略會發生什麼變化

由於效能閾值策略被指派給儲存對象，因此如果您移動某個對象，則在移動完成後，所有指派的閾值策略仍會附加到該物件。例如，如果您將磁碟區或 LUN 移至不同的聚合，則閾值策略對於新聚合上的磁碟區或 LUN 仍然有效。

如果閾值策略（組合策略）存在輔助計數器條件（例如，如果為聚合或節點指派了附加條件），則輔助計數器條件將套用於磁碟區或 LUN 已移至的新聚合或節點。

如果對於使用變更後的閾值策略的物件存在任何新的活動事件，則這些事件將被標記為過時，並且閾值策略將開始按照新定義的閾值策略監控計數器。

磁碟區移動操作會導致 ONTAP 傳送訊息變更事件。效能資源管理器頁面和工作負載分析頁面的事件時間軸中會出現一個變更事件圖標，指示移動操作完成的時間。



如果將物件移至不同的集群，則會從該物件中刪除使用者定義的閾值策略。如果需要，您必須在移動操作完成後為物件指派閾值策略。然而，動態和系統定義的閾值策略會在物件移動到新叢集後自動套用於該物件。

HA 接管和交還期間的閾值策略功能

當在高可用性 (HA) 配置中發生接管或交還操作時，從一個節點移動到另一個節點的物件將以與手動移動操作相同的方式保留其閾值策略。由於 Unified Manager 每 15 分鐘檢查一次叢集配置更改，因此直到下次輪詢叢集配置時才能確定切換到新節點的影響。



如果接管和交還操作都發生在 15 分鐘的配置變更收集期內，您可能看不到效能統計資訊從一個節點移動到另一個節點。

聚合遷移期間的閾值策略功能

如果使用 `aggregate relocation start` 命令，單一和組合閾值策略都會保留在所有物件上，並且閾值策略的節點部分會應用於新節點。

MetroCluster 切換期間的閾值策略功能

在 MetroCluster 配置中從一個叢集移動到另一個叢集的物件不會保留其使用者定義的閾值策略設定。如果需要，您可以對已移至夥伴叢集的磁碟區和 LUN 套用閾值策略。當物件移回其原始叢集後，將自動重新套用使用者定義的閾值策略。

有關信息，請參閱["切換和切回期間的捲行為"](#)。

分析效能事件

您可以分析效能事件以確定何時偵測到它們、它們是活動的（新的或已確認的）還是過時的、所涉及的工作負載和叢集元件，以及自行解決事件的選項。

顯示有關性能事件的信息

您可以使用事件管理庫存頁面查看 Unified Manager 監控的叢集上的所有效能事件的清單。透過查看這些信息，您可以確定最關鍵的事件，然後深入了解詳細資訊以確定事件的原因。

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。

事件清單依偵測時間排序，最新事件列在最前面。您可以按一下列標題來根據該列對事件進行排序。例如，您可以按狀態列排序以按嚴重性檢視事件。如果您正在尋找特定事件或特定類型的事件，您可以使用篩選器和搜尋機制來最佳化清單中出現的事件清單。

所有來源的事件都顯示在此頁面上：

- 使用者自訂效能閾值策略
- 系統定義的效能閾值策略

- 動態效能閾值

事件類型列列出了事件的來源。您可以選擇一個事件以在事件詳細資訊頁面中查看有關該事件的詳細資訊。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。
2. 從「檢視」功能表中，選擇「活動效能事件」。

此頁面顯示過去 7 天內產生的所有新的和已確認的績效事件。

3. 找到您要分析的事件並點擊事件名稱。

將顯示事件的詳細資訊頁面。



您也可以透過點擊「效能資源管理器」頁面和警報電子郵件中的事件名稱連結來顯示活動的詳細資訊頁面。

根據使用者定義的效能閾值分析事件

從使用者定義的閾值產生的事件表示某個儲存物件（例如聚合或磁碟區）的效能計數器已超過您在策略中定義的閾值。這表示集群物件正在遇到效能問題。

您可以使用事件詳細資訊頁面來分析效能事件，並在必要時採取糾正措施，使效能恢復正常。

響應用戶定義的效能閾值事件

您可以使用 Unified Manager 調查由效能計數器超過使用者定義的警告或嚴重閾值而導致的效能事件。您也可以使用 Unified Manager 檢查叢集元件的運作狀況，以查看在元件上偵測到的最近的運作狀況事件是否導致了效能事件。

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。
- 必須有新的或過時的表演事件。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 查看*描述*，其中描述了導致該事件的閾值違規。

例如，訊息「456 ms/op 的延遲值根據 400 ms/op 的閾值設定觸發了警告事件」表示該物件發生了延遲警告事件。

3. 將遊標懸停在策略名稱上以顯示有關觸發事件的閾值策略的詳細資訊。

這包括策略名稱、正在評估的效能計數器、必須違反才能被視為嚴重或警告事件的計數器值，以及計數器必須超過該值的持續時間。

4. 記下*事件觸發時間*，以便您可以調查是否可能同時發生其他可能導致此事件的事件。

5. 請按照以下選項之一進一步調查該事件，以確定是否需要執行任何操作來解決效能問題：

選項	可能採取的調查行動
按一下來源物件名稱可顯示該物件的資源管理器頁面。	此頁面可讓您查看物件詳細資訊並將此物件與其他類似的儲存物件進行比較，以查看其他儲存物件是否在同一時間有效能問題。例如，查看同一聚合上的其他磁碟區是否也存在效能問題。
按一下叢集名稱即可顯示叢集摘要頁面。	此頁面使您能夠查看此物件所在叢集的詳細信息，以查看是否在同一時間發生了其他效能問題。

根據系統定義的效能閾值分析事件

從系統定義的效能閾值產生的事件表示某個儲存物件的效能計數器或效能計數器集已超過系統定義策略的閾值。這表示儲存物件（例如聚合或節點）正在遇到效能問題。

您可以使用事件詳細資訊頁面來分析效能事件，並在必要時採取糾正措施，使效能恢復正常。



Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系統上未啟用系統定義的閾值策略。

響應系統定義的效能閾值事件

您可以使用 Unified Manager 調查由效能計數器超過系統定義的警告閾值而導致的效能事件。您也可以使用 Unified Manager 檢查叢集元件的運作狀況，以查看在元件上偵測到的近期事件是否導致了效能事件。

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。
- 必須有新的或過時的表演事件。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 查看*描述*，其中描述了導致該事件的閾值違規。

例如，訊息「節點利用率值 90% 根據閾值設定 85% 觸發了警告事件」表示叢集物件發生了節點利用率警告事件。

3. 記下*事件觸發時間*，以便您可以調查是否可能同時發生其他可能導致此事件的事件。
4. 在*系統診斷*下，查看系統定義的策略對叢集物件執行的分析類型的簡要描述。

對於某些事件，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。對於其他類型的系統定義事件，計數器圖表顯示物件的效能。

5. 在「建議的操作」下，按一下「幫助我執行此操作」連結以查看您可以執行的建議操作，以嘗試自行解決效能事件。

回應 QoS 策略群組效能事件

當工作負載吞吐量（IOPS、IOPS/TB 或 MBps）超過定義的ONTAP QoS 策略設定且工作負載延遲受到影響時，Unified Manager 會產生 QoS 策略警告事件。這些系統定義的事件提供了在許多工作負載受到延遲影響之前糾正潛在效能問題的機會。

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。
- 必須有新的、公認的或過時的績效事件。

當工作負載吞吐量在前一小時的每個效能收集期間超過定義的 QoS 策略設定時，Unified Manager 會產生違反 QoS 策略的警告事件。在每個收集期間，工作負載吞吐量可能僅在短時間內超過 QoS 閾值，但 Unified Manager 在圖表上僅顯示收集期間的「平均」吞吐量。因此，您可能會收到 QoS 事件，而工作負載的吞吐量可能尚未超過圖表中顯示的策略閾值。

您可以使用 System Manager 或ONTAP指令來管理原則群組，包括下列任務：

- 為工作負載建立新的策略群組
- 在策略群組中新增或刪除工作負載
- 在策略組之間移動工作負載
- 更改策略群組的吞吐量限制
- 將工作負載移動到不同的聚合或節點

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 查看*描述*，其中描述了導致該事件的閾值違規。

例如，訊息「vol1_NFS1 上的 IOPS 值為 1,352 IOPS 已觸發警告事件以識別工作負載的潛在效能問題」表示在磁碟區 vol1_NFS1 上發生了 QoS 最大 IOPS 事件。

3. 請查看「事件資訊」部分，以了解有關事件發生時間和事件持續時間的更多詳細資訊。

此外，對於共用 QoS 策略吞吐量的磁碟區或 LUN，您可以看到消耗最多 IOPS 或 MBps 的前三個工作負載的名稱。

4. 在「系統診斷」部分下，查看兩個圖表：一個用於總平均 IOPS 或 MBps（取決於事件），另一個用於延遲。透過這種方式安排，您可以看到當工作負載接近 QoS 最大限制時哪些叢集元件對延遲的影響最大。

對於共用 QoS 策略事件，吞吐量圖表中顯示前三個工作負載。如果有三個以上的工作負載共享 QoS 策略，則其他工作負載將被加入到「其他工作負載」類別中。此外，延遲圖表顯示 QoS 策略中所有工作負載的平均延遲。

請注意，對於自適應 QoS 策略事件，IOPS 和 MBps 圖表顯示ONTAP根據磁碟區大小從指派的 IOPS/TB 閾值策略轉換的 IOPS 或 MBps 值。

5. 在「建議的操作」部分下，查看建議並確定應執行哪些操作以避免工作負載延遲增加。

如果需要，請按一下「幫助」按鈕以查看有關您可以執行的建議操作的更多詳細信息，以嘗試解決效能事件。

了解具有定義區塊大小的自適應 QoS 策略中的事件

自適應 QoS 策略群組根據磁碟區大小自動擴展吞吐量上限或下限，並在磁碟區大小變化時保持 IOPS 與 TB 的比率。從 ONTAP 9.5 開始，您可以在 QoS 策略中指定區塊大小，以便同時有效地套用 MB/s 閾值。

在自適應 QoS 策略中分配 IOPS 閾值僅對每個工作負載中發生的操作數量進行限制。根據產生工作負載的用戶端上設定的區塊大小，某些 IOPS 包含更多數據，因此給處理作業的節點帶來更大的負擔。

工作負載的 MB/s 值是使用下列公式產生的：

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

如果工作負載平均為 3,000 IOPS，且用戶端上的區塊大小設定為 32 KB，則該工作負載的有效 MB/s 為 96。如果相同的工作負載平均為 3,000 IOPS，且用戶端上的區塊大小設定為 48 KB，則該工作負載的有效 MB/s 為 144。您可以看到，當區塊大小較大時，節點處理的資料增加了 50%。

讓我們來看看具有定義區塊大小的以下自適應 QoS 策略，以及如何根據客戶端上設定的區塊大小觸發事件。

建立策略並將峰值吞吐量設定為 2,500 IOPS/TB，區塊大小為 32KB。對於已使用容量為 1 TB 的捲，這實際上將 MB/s 閾值設為 80 MB/s $((2500 \text{ IOPS} * 32\text{KB}) / 1000)$ 。請注意，當吞吐量值比定義的閾值低 10% 時，Unified Manager 會產生警告事件。在以下情況下會產生事件：

已用容量	當吞吐量超過此數量時會產生事件...	
	每秒輸入/輸出次數	MB/秒
1TB	2,250 IOPS	72 MB/秒
2TB	4,500 IOPS	144 MB/秒
5TB	11,250 IOPS	360MB/秒

如果磁碟區使用 2TB 可用空間，IOPS 為 4,000，且用戶端上的 QoS 區塊大小設定為 32KB，則 MB/ps 吞吐量為 128 MB/s $((4,000 \text{ IOPS} * 32 \text{ KB}) / 1000)$ 。在這種情況下不會產生任何事件，因為 4,000 IOPS 和 128 MB/s 均低於使用 2 TB 空間的捲的閾值。

如果磁碟區使用 2TB 可用空間，IOPS 為 4,000，且用戶端上的 QoS 區塊大小設定為 64KB，則 MB/s 吞吐量為 256 MB/s $((4,000 \text{ IOPS} * 64 \text{ KB}) / 1000)$ 。在這種情況下，4,000 IOPS 不會產生事件，但 256 MB/s 的 MB/s 值高於 144 MB/s 的閾值，因此會產生事件。

因此，當基於包含區塊大小的自適應 QoS 政策的 MB/s 違規觸發事件時，事件詳細資訊頁面的系統診斷部分將顯示 MB/s 圖表。如果基於自適應 QoS 政策的 IOPS 違規觸發事件，則會在系統診斷部分顯示 IOPS 圖表。如果 IOPS 和 MB/s 都發生違規，您將收到兩個事件。

有關調整 QoS 設定的更多信息，請參閱 ["績效管理概述"](#)。

響應節點資源過度利用的效能事件

當單一節點的運作超出其運作效率界限時，Unified Manager 會產生節點資源過度利用警告事件，因此可能會影響工作負載延遲。這些系統定義的事件提供了在許多工作負載受到延遲影響之前糾正潛在效能問題的機會。

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。
- 必須有新的或過時的表演事件。

Unified Manager 透過尋找效能容量使用率超過 100% 且持續超過 30 分鐘的節點，產生違反節點資源過度利用策略的警告事件。

您可以使用 System Manager 或 ONTAP 指令來修正此類效能問題，包括下列任務：

- 建立並應用 QoS 策略到任何過度使用系統資源的磁碟區或 LUN
- 降低已套用工作負載的策略群組的 QoS 最大吞吐量限制
- 將工作負載移動到不同的聚合或節點
- 透過向節點添加磁碟或升級到具有更快 CPU 和更多 RAM 的節點來增加容量

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 查看*描述*，其中描述了導致該事件的閾值違規。

例如，訊息「`Perf. simple-02 上的容量使用值為 139%，已觸發警告事件，以識別資料處理單元中的潛在效能問題。」表示節點 simple-02 上的效能容量已過度使用，並影響節點效能。

3. 在「系統診斷」部分下，查看三個圖表：一個用於節點上使用的效能容量，一個用於頂級工作負載使用的平均儲存 IOPS，一個用於頂級工作負載的延遲。以這種方式排列，您可以看到哪些工作負載是導致節點延遲的原因。

您可以將遊標移到 IOPS 圖表上來查看哪些工作負載應用了 QoS 策略，哪些工作負載沒有應用。

4. 在「建議的操作」部分下，查看建議並確定應執行哪些操作以避免工作負載延遲增加。

如果需要，請按一下「幫助」按鈕以查看有關您可以執行的建議操作的更多詳細信息，以嘗試解決效能事件。

響應集群不平衡效能事件

當叢集中某個節點的負載遠高於其他節點時，Unified Manager 會產生叢集不平衡警告事件，因此可能會影響工作負載延遲。這些系統定義的事件提供了在許多工作負載受到延遲影響之前糾正潛在效能問題的機會。

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。

Unified Manager 透過比較叢集中所有節點的效能容量使用值來查看任何節點之間是否存在 30% 的負載差異，

從而為叢集不平衡閾值策略違規產生警告事件。

這些步驟可協助您識別以下資源，以便您可以將高效能工作負載移至使用率較低的節點：

- 同一叢集中利用率較低的節點
- 新節點上利用率最低的聚合
- 當前節點上效能最高的捲

步驟

1. 顯示*事件*詳細資訊頁面以查看有關該事件的資訊。
2. 查看*描述*，其中描述了導致該事件的閾值違規。

例如，訊息「效能容量使用計數器指示叢集 Dallas-1-8 上的節點之間的負載差異為 62%，並根據系統閾值 30% 觸發了警告事件」表示其中一個節點上的效能容量被過度使用並影響節點效能。

3. 查看「建議的操作」中的文本，將高效能磁碟區從具有高效能容量使用值的節點移至具有最低效能容量使用值的節點。
4. 確定效能容量使用值最高和最低的節點：
 - a. 在「事件資訊」部分中，按一下來源叢集的名稱。
 - b. 在「叢集/效能摘要」頁面中，按一下「管理物件」區域中的「節點」。
 - c. 在「節點」庫存頁面中，按「已使用效能容量*」欄位對節點進行排序。
 - d. 確定效能容量使用值最高和最低的節點並記下這些名稱。
5. 在確定具有最高效能容量使用值的節點上使用最多 IOPS 的磁碟區：
 - a. 點選效能容量使用值最高的節點。
 - b. 在*節點/效能資源管理器*頁面中，從*檢視和比較*選單中選擇*此節點上的聚合*。
 - c. 按一下具有最高效能容量使用值的聚合。
 - d. 在*聚合/效能資源管理器*頁面中，從*檢視和比較*選單中選擇*此聚合上的磁碟區*。
 - e. 將磁碟區依 **IOPS** 欄位排序，並記下使用最多 IOPS 的磁碟區的名稱以及該磁碟區所在聚合的名稱。
6. 確定具有最低效能容量使用值的節點上利用率最低的聚合：
 - a. 按一下「儲存」>「聚合」以顯示「聚合」庫存頁面。
 - b. 選擇*效能：所有聚合*視圖。
 - c. 點擊「過濾器」按鈕並新增一個過濾器，其中「Node」等於您在步驟 4 中記下的具有最低效能容量使用值的節點的名稱。
 - d. 記下具有最低效能容量使用值的聚合的名稱。
7. 將磁碟區從過載節點移至您確定為在新節點上利用率較低的聚合。

您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 指令或這些工具的組合來執行行動操作。

幾天後，檢查您是否從該叢集收到相同的叢集不平衡事件。

根據動態效能閾值分析事件

動態閾值產生的事件表明，與預期反應時間範圍相比，工作負載的實際反應時間（延遲）太高或太低。您可以使用事件詳細資訊頁面來分析效能事件，並在必要時採取糾正措施，使效能恢復正常。



Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系統上未啟用動態效能閾值。

識別動態效能事件中涉及的受害工作負載

在 Unified Manager 中，您可以決定哪些磁碟區工作負載會因儲存元件爭用而導致回應時間（延遲）偏差最大。識別這些工作負載有助於您了解為什麼訪問它們的客戶端應用程式的運行速度比平常慢。

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。
- 必須有新的、公認的或過時的動態性能事件。

事件詳細資料頁面顯示使用者定義和系統定義的工作負載列表，按元件活動或使用情況的最大偏差或受事件影響最大的程度排序。這些值是根據 Unified Manager 在偵測和上次分析事件時識別的峰值。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 在工作負載延遲和工作負載活動圖表中，選擇*受害者工作負載*。
3. 將遊標停留在圖表上，可以查看影響組件的頂級使用者定義工作負載以及受害工作負載的名稱。

識別動態效能事件中涉及的工作負載

在 Unified Manager 中，您可以決定哪些工作負載對於爭用的叢集元件的使用偏差最大。識別這些工作負載有助於您了解叢集上的某些磁碟區響應時間（延遲）較慢的原因。

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。
- 必須有新的、公認的或過時的動態性能事件。

事件詳細資料頁面顯示使用者定義和系統定義的工作負載列表，依元件使用率最高或受事件影響最大的程度排序。這些值是根據 Unified Manager 在偵測和上次分析事件時識別的峰值。

步驟

1. 顯示事件詳細資訊頁面以查看事件的資訊。
2. 在「工作負載延遲」和「工作負載活動」圖表中，選擇「Bully Workloads」。
3. 將遊標停留在圖表上，查看影響組件的頂級使用者定義霸凌工作負載。

識別動態效能事件中涉及的shark工作負載

在 Unified Manager 中，您可以決定哪些工作負載對於爭用的儲存元件的使用偏差最大。識別這些工作負載有助於您確定是否應將這些工作負載移至使用率較低的叢集。

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。
- 有新的、已確認的或已過時的效能動態事件。

事件詳細資料頁面顯示使用者定義和系統定義的工作負載列表，依元件使用率最高或受事件影響最大的程度排序。這些值是根據 Unified Manager 在偵測和上次分析事件時識別的峰值。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 在工作負載延遲和工作負載活動圖表中，選擇 **Shark Workloads**。
3. 將遊標停留在圖表上，查看影響組件的頂級使用者定義工作負載以及 shark 工作負載的名稱。

MetroCluster配置的效能事件分析

您可以使用 Unified Manager 分析MetroCluster配置的效能事件。您可以識別事件中涉及的工作負載並查看解決該事件的建議操作。

MetroCluster效能事件可能是由於過度利用叢集之間的交換器間鏈路 (ISL) 的_bully_ 工作負載，或由於鏈路健康問題造成的。Unified Manager 獨立監控MetroCluster配置中的每個集群，而不考慮夥伴集群上的效能事件。

MetroCluster配置中兩個叢集的效能事件也會顯示在 Unified Manager 儀表板頁面上。您也可以查看 Unified Manager 的「運作狀況」頁面來檢查每個叢集的運作狀況並查看它們的關係。

分析MetroCluster配置中叢集的動態效能事件

您可以使用 Unified Manager 分析MetroCluster配置中偵測到效能事件的叢集。您可以識別叢集名稱、事件偵測時間以及所涉及的_bully_和_victim_工作負載。

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。
- MetroCluster配置必須有新的、已確認的或過時的效能事件。
- MetroCluster配置中的兩個叢集必須由同一個 Unified Manager 實例監控。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 查看事件描述以了解所涉及的工作負載的名稱以及所涉及的工作負載的數量。

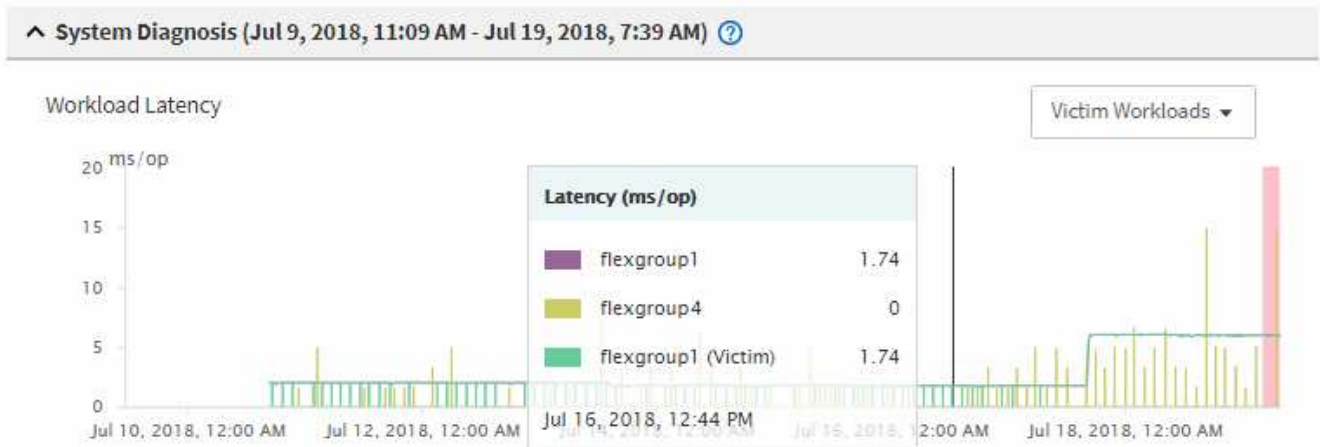
在此範例中，MetroCluster資源圖示為紅色，表示MetroCluster資源處於爭用狀態。將遊標放在圖示上即可顯示該圖示的描述。

Description: 2 victim volumes are slow due to vol_osv_siteB2_5 causing contention on MetroCluster resources



3. 記下叢集名稱和事件偵測時間，您可以使用它們來分析夥伴叢集上的效能事件。
4. 在圖表中，查看_受害者_工作負載以確認其回應時間高於效能閾值。

在此範例中，受害者工作負載顯示在懸停文字中。延遲圖表從高層次顯示了所涉及的受害工作負載的一致延遲模式。即使受害工作負載的異常延遲觸發了該事件，一致的延遲模式可能表明工作負載在其預期範圍內執行，但 I/O 的峰值增加了延遲並觸發了該事件。



如果您最近在存取這些磁碟區工作負載的用戶端上安裝了應用程式，並且該應用程式會向它們發送大量 I/O，那麼您可能會預期它們的延遲會增加。如果工作負載的延遲恢復到預期範圍內，事件狀態變為過時，並保持此狀態超過 30 分鐘，您可能可以忽略該事件。如果事件正在進行，並且保持新狀態，您可以進一步調查以確定是否有其他問題導致了該事件。

5. 在工作負載吞吐量圖表中，選擇 **Bully Workloads** 來顯示負載較大的工作負載。

存在霸凌工作負載表示該事件可能是由於本地叢集上的一個或多個工作負載過度利用 MetroCluster 資源而導致的。欺負工作負載的寫入吞吐量 (MB/s) 偏差較大。

此圖表從總體上顯示了工作負載的寫入吞吐量 (MB/s) 模式。您可以查看寫入 MB/s 模式來識別異常吞吐量，這可能表示工作負載過度利用了 MetroCluster 資源。

如果事件中不涉及任何霸凌工作負載，則該事件可能是由叢集之間的連結的健康問題或夥伴叢集上的效能問題引起的。您可以使用 Unified Manager 檢查 MetroCluster 配置中兩個叢集的運作狀況。您也可以使用 Unified Manager 檢查和分析合作夥伴叢集上的效能事件。

分析 MetroCluster 配置上的遠端叢集的動態效能事件

您可以使用 Unified Manager 分析 MetroCluster 配置中遠端叢集上的動態效能事件。此分析可協助您確定遠端叢集上的事件是否導致了其夥伴叢集上的事件。

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。
- 您必須已經分析了MetroCluster配置中本地叢集上的效能事件並取得了事件偵測時間。
- 您必須檢查涉及效能事件的本地群集及其夥伴群集的健康狀況，並取得夥伴群集的名稱。

步驟

1. 登入正在監控合作夥伴叢集的 Unified Manager 實例。
2. 在左側導覽窗格中，按一下「事件」以顯示事件清單。
3. 從*時間範圍*選擇器中，選擇*過去一小時*，然後按一下*套用範圍*。
4. 在*過濾*選擇器中，從左側下拉選單中選擇*集群*，在文字欄位中輸入合作夥伴集群的名稱，然後按一下*套用過濾器*。

如果所選群集在過去一小時內沒有發生任何事件，則表示該群集在其夥伴群集上偵測到該事件期間沒有遇到任何效能問題。

5. 如果選定群集在過去一小時內偵測到事件，則將事件偵測時間與本地群集上事件的事件偵測時間進行比較。

如果這些事件涉及導致資料處理元件爭用的霸凌工作負載，則這些霸凌者中的一個或多個可能在本地叢集上引發了該事件。您可以單擊該事件來分析它，並在事件詳細資訊頁面上查看解決該事件的建議操作。

如果這些事件不涉及霸凌工作負載，則它們不會導致本地叢集上的效能事件。

響應由 QoS 策略群組限制引起的動態效能事件

您可以使用 Unified Manager 調查服務品質 (QoS) 策略群組限制工作負載吞吐量 (MB/s) 所導致的效能事件。限制增加了策略群組中磁碟區工作負載的回應時間（延遲）。您可以使用事件資訊來確定是否需要對策略群組施加新的限制以停止限制。

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。
- 必須有新的、公認的或過時的績效事件。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 閱讀*描述*，其中顯示受限制影響的工作負載的名稱。



描述可以顯示受害者和霸凌者的相同工作負載，因為限制使工作負載成為其自身的受害者。

3. 使用文字編輯器等應用程式記錄磁碟區的名稱。

您可以稍後搜尋卷名來找到它。

4. 在「工作負載延遲」和「工作負載利用率」圖表中，選擇「Bully Workloads」。
5. 將遊標停留在圖表上，即可查看影響策略群組的主要使用者定義工作負載。

清單頂部的工作負載偏差最大，導致發生節流。活動是每個工作負載所使用的策略群組限制的百分比。

6. 在「建議的操作」區域中，按一下排名靠前的工作負載的「分析工作負載」按鈕。
7. 在工作負載分析頁面中，設定延遲圖表查看所有叢集元件，設定吞吐量圖表查看細分。

細分圖表顯示在延遲圖表和 IOPS 圖表下方。

8. 比較*延遲*圖表中的 QoS 限制，以查看事件發生時多少限制量影響了延遲。

QoS 策略群組的最大吞吐量為每秒 1,000 個作業 (op/sec)，其中的工作負載總和不能超過該吞吐量。事件發生時，策略群組中的工作負載的合併吞吐量超過 1,200 操作/秒，這導致策略群組將其活動限制回 1,000 操作/秒。

9. 將*讀取/寫入延遲*值與*讀取/寫入/其他*值進行比較。

兩個圖表都顯示讀取請求數量較多且延遲較高，但寫入請求的數量和延遲量較低。這些值可協助您確定是否存在大量吞吐量或大量操作增加了延遲。在決定對吞吐量或操作設定策略群組限制時，您可以使用這些值。

10. 使用 ONTAP 系統管理員將策略組的目前限制增加到 1,300 op/sec。
11. 一天後，返回 Unified Manager 並在工作負載分析 頁面中輸入您在步驟 3 中記錄的工作負載。
12. 選擇吞吐量細分圖表。

顯示讀取/寫入/其他圖表。

13. 在頁面頂部，將遊標指向更改事件圖示 (●) 來更改策略組限制。
14. 將*讀取/寫入/其他*圖表與*延遲*圖表進行比較。

讀寫請求相同，但節流已停止，延遲也減少了。

回應由磁碟故障引起的動態效能事件

您可以使用 Unified Manager 調查工作負載過度利用聚合所導致的效能事件。您也可以使用 Unified Manager 檢查聚合的運作狀況，以查看在聚合上偵測到的近期運作狀況事件是否導致了效能事件。

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。
- 必須有新的、公認的或過時的績效事件。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 閱讀*描述*，其中描述了事件所涉及的工作負載和爭用的叢集元件。

有多個受害卷的延遲受到爭用中的群集組件的影響。聚合體處於 RAID 重建過程中，以備用磁碟取代故障磁碟，是處於爭用的叢集元件。在「爭用中的元件」下，「聚合」圖示以紅色突出顯示，並且聚合的名稱顯示在括號中。

3. 在工作負載利用率圖表中，選擇 **Bully Workloads**。
4. 將遊標停留在圖表上，可以查看影響該組件的主要工作負載。

自偵測到事件以來峰值利用率最高的工作負載顯示在圖表頂部。最重要的工作負載之一是系統定義的工作負載磁碟健康，它表示 RAID 重建。重建是使用備用磁碟重建聚合所涉及的內部過程。磁碟運行狀況工作負載以及聚合上的其他工作負載可能會導致聚合上的爭用和相關事件。

5. 確認磁碟運作狀況工作負載的活動導致該事件後，等待約 30 分鐘以完成重建，並等待 Unified Manager 分析該事件並偵測聚合是否仍處於爭用狀態。
6. 刷新*活動詳情*。

RAID重建完成後，查看State為obsolete，表示事件已解決。

7. 在「工作負載利用率」圖表中，選擇「**Bully Workloads**」以按峰值利用率查看聚合上的工作負載。
8. 在「建議的操作」區域中，按一下排名靠前的工作負載的「分析工作負載」按鈕。
9. 在「工作負載分析」頁面中，設定時間範圍以顯示所選卷的過去 24 小時（1 天）的資料。

在事件時間軸中，紅點 (●) 表示磁碟故障事件發生的時間。

10. 在節點和聚合利用率圖表中，隱藏節點統計線，以便僅保留聚合線。
11. 將此圖表中的數據與*延遲*圖表中事件發生時的數據進行比較。

事件發生時，聚合利用率顯示大量讀寫活動，這是由 RAID 重建過程引起的，這增加了所選卷的延遲。事件發生幾個小時後，讀寫和延遲均有所減少，證實聚合不再存在爭用。

響應由 HA 接管引起的動態性能事件

您可以使用 Unified Manager 調查由高可用性 (HA) 對中的叢集節點上的高資料處理所引起的效能事件。您也可以使用 Unified Manager 檢查節點的運作狀況，以查看在節點上偵測到的任何近期運作狀況事件是否導致了效能事件。

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。
- 必須有新的、公認的或過時的績效事件。

步驟

1. 顯示*活動詳情*頁面以查看活動的資訊。
2. 閱讀*描述*，其中描述了事件所涉及的工作負載和爭用的叢集元件。

有一個受害卷的延遲受到爭用的群集組件的影響。資料處理節點從其夥伴節點接管了所有工作負載，是處於爭用的叢集元件。在「爭用中的元件」下，「Data Processing」圖示以紅色突出顯示，並且在事件發生時處理資料處理的節點的名稱顯示在括號中。

3. 在「描述」中，按一下磁碟區的名稱。

將顯示磁碟區效能資源管理器頁面。在頁面頂部的事件時間軸中，有一個更改事件圖示 (●) 表示 Unified Manager 偵測到 HA 接手開始的時間。

4. 將遊標指向 HA 接管的更改事件圖標，懸停文字將顯示有關 HA 接管的詳細資訊。

在延遲圖表中，事件表明所選卷在 HA 接管的同時由於高延遲而超過了性能閾值。

5. 按一下「縮放檢視」以在新頁面上顯示延遲圖表。
6. 在「檢視」功能表中，選擇「群集元件」以查看群集元件的總延遲。
7. 將滑鼠遊標指向 HA 接管開始的更改事件圖標，並將資料處理的延遲與總延遲進行比較。

在 HA 接手時，由於資料處理節點上的工作負載需求增加，資料處理量出現激增。CPU 使用率的增加增加了延遲並觸發了該事件。

8. 修復故障節點後，使用 ONTAP 系統管理員執行 HA 交還，將工作負載從合作夥伴節點移至已修復的節點。
9. HA 交還完成後，在 Unified Manager 中進行下一個設定發現（約 15 分鐘）後，在事件管理 庫存頁面中找到由 HA 接手觸發的事件和工作負載。

HA 接管觸發的事件現在處於過時狀態，這表示該事件已解決。資料處理組件的延遲減少了，從而降低了總延遲。選定卷現在用於資料處理的節點已解決該事件。

解決效能事件

您可以使用建議的操作來嘗試自行解決效能事件。前三個建議始終顯示，第四個建議下的操作特定於所顯示的事件類型。

*幫助我執行此操作*連結為每個建議的操作提供了附加信息，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。

確認延遲在預期範圍內

當叢集元件處於爭用狀態時，使用該元件的磁碟區工作負載可能會減少回應時間（延遲）。您可以檢查爭用組件上每個受害者工作負載的延遲，以確認其實際延遲在預期範圍內。您也可以按一下磁碟區名稱以查看該磁碟區的歷史資料。

如果效能事件處於過時狀態，則事件中涉及的每個受害者的延遲可能已恢復到其預期範圍內。

審查配置變更對工作負載效能的影響

叢集上的配置變更（例如磁碟故障、HA 故障轉移或移動磁碟區）可能會對磁碟區效能產生負面影響並導致延遲增加。

在 Unified Manager 中，您可以查看「工作負載分析」頁面，以了解最近配置變更發生的時間，並將其與操作和延遲（回應時間）進行比較，以查看所選卷工作負載的活動是否發生了變化。

Unified Manager 的效能頁面只能偵測有限數量的變更事件。健康頁面提供由配置變更引起的其他事件的警報。您可以在 Unified Manager 中搜尋該磁碟區以查看事件記錄。

從客戶端提高工作負載效能的選項

您可以檢查向涉及效能事件的磁碟區發送 I/O 的用戶端工作負載（例如應用程式或資料庫），以確定用戶端變更是否可以修正該事件。

當連接到叢集上的磁碟區的客戶端增加其 I/O 請求時，叢集必須更加努力地滿足需求。如果您知道哪些用戶端對叢集上的特定磁碟區有大量 I/O 要求，則可以透過調整存取該磁碟區的用戶端數量或減少該磁碟區的 I/O 量來提高叢集效能。您也可以對磁碟區所屬的 QoS 策略群組套用或增加限制。

您可以調查客戶端及其應用程序，以確定客戶端是否發送了比平常更多的 I/O，這可能會導致叢集元件爭議。在事件詳細資料頁面上，系統診斷部分顯示使用爭用元件的頂級磁碟區工作負載。如果您知道哪個客戶端正在存取特定卷，您可以轉到該客戶端來確定客戶端硬體或應用程式是否未按預期運行或是否比平常做更多的工作。

在MetroCluster配置中，對本地叢集上的磁碟區的寫入請求將鏡像到遠端叢集上的磁碟區。保持本地叢集上的來源磁碟區與遠端叢集上的目標磁碟區同步也會增加MetroCluster配置中兩個叢集的需求。透過減少對這些鏡像磁碟區的寫入請求，叢集可以執行更少的同步操作，從而減少對其他工作負載的效能影響。

檢查客戶端或網路問題

當連接到叢集上的磁碟區的客戶端增加其 I/O 請求時，叢集必須更加努力地滿足需求。叢集需求的增加可能會導致元件爭用，增加使用該元件的工作負載的延遲，並在 Unified Manager 中觸發事件。

在事件詳細資料頁面上，系統診斷部分顯示使用爭用元件的頂級磁碟區工作負載。如果您知道哪個客戶端正在存取特定卷，您可以轉到該客戶端來確定客戶端硬體或應用程式是否未按預期運行或是否比平常做更多的工作。您可能需要聯絡客戶管理員或應用程式供應商尋求協助。

您可以檢查網路基礎設施，以確定是否存在硬體問題、瓶頸或競爭工作負載，這些問題可能導致叢集和連接的用戶端之間的 I/O 請求執行速度比預期慢。您可能需要聯絡網路管理員尋求協助。

驗證 QoS 策略群組中的其他磁碟區是否具有異常高的活動

您可以查看服務品質 (QoS) 策略群組中活動變更最大的工作負載，以確定是否有多個工作負載導致了該事件。您也可以查看其他工作負載是否仍超出設定的吞吐量限制，或是否已回到預期的活動範圍內。

在「事件詳細資料」頁面的「系統診斷」部分中，您可以按活動尖峰偏差對工作負載進行排序，以將活動變化最大的工作負載顯示在表格頂部。這些工作負荷可能是“欺凌者”，其活動超出了設定的限制，並可能導致了該事件的發生。

您可以導覽至每個磁碟區工作負載的工作負載分析頁面來查看其 IOPS 活動。如果工作負載在某個時期的操作活動非常頻繁，則可能對該事件有所貢獻。您可以變更工作負載的政策群組設定或將工作負載移至其他策略群組。

您可以使用 ONTAP System Manager 或 ONTAP CLI 指令來管理政策群組，如下所示：

- 建立策略組。
- 在策略群組中新增或刪除工作負載。
- 在策略組之間移動工作負載。
- 更改策略群組的吞吐量限制。

行動邏輯介面 (LIF)

將邏輯介面 (LIF) 移至不太繁忙的連接埠可以幫助改善負載平衡、協助維護操作和效能調整，並減少間接存取。

間接存取會降低系統效率。當磁碟區工作負載使用不同的節點進行網路處理和資料處理時，就會發生這種情況。為了減少間接訪問，您可以重新排列 LIF，這涉及移動 LIF 以使用相同的節點進行網路處理和資料處理。您可以配置負載平衡，讓ONTAP自動將繁忙的 LIF 移動到其他端口，或者您可以手動移動 LIF。

好處	注意事項
<ul style="list-style-type: none">• 改善負載平衡。• 減少間接存取。	 <p>當移動連接到 CIFS 共享的 LIF 時，存取 CIFS 共享的用戶端將斷開連線。對 CIFS 共享的任何讀取或寫入請求都會中斷。</p>

您可以使用ONTAP指令來設定負載平衡。有關更多信息，請參閱ONTAP網絡文檔。

您可以使用ONTAP系統管理員和ONTAP CLI 指令手動移動 LIF。

在不太繁忙的時間運行儲存效率操作

您可以修改處理儲存效率操作的策略或計劃，以便在受影響的磁碟區工作負載不太繁忙時運行。

儲存效率操作可能會佔用大量叢集 CPU 資源，並成為執行作業的磁碟區的負擔。如果在執行儲存效率操作的同時受害磁碟區具有較高的活動性，則其延遲可能會增加並觸發事件。

在事件詳細資料頁面上，系統診斷部分會依活動高峰偏差顯示 QoS 策略群組中的工作負載，以識別霸凌工作負載。如果您看到表格頂部附近顯示“儲存效率”，則這些操作正在欺負受害者工作負載。透過修改效率策略或計劃以在這些工作負載不太繁忙時運行，您可以防止儲存效率操作引起叢集爭用。

您可以使用ONTAP系統管理員來管理效率策略。您可以使用ONTAP指令來管理效率策略和計畫。

什麼是儲存效率

儲存效率使您能夠以最低的成本儲存最大數量的數據，並在消耗更少空間的同時適應快速的數據成長。NetApp 的儲存效率策略是基於其核心ONTAP作業系統和隨處寫入檔案佈局 (WAFL) 檔案系統提供的內建儲存虛擬化和統一儲存基礎。

儲存效率包括使用精簡配置、Snapshot 副本、重複資料刪除、資料壓縮、FlexClone、使用SnapVault和磁碟區SnapMirror的精簡複製、RAID-DP、快閃記憶體、Flash Pool 聚合和支援FabricPool的聚合等技術，這些技術有助於提高儲存利用率並降低儲存成本。

統一儲存架構可讓您在單一平台上有效整合儲存區域網路 (SAN)、網路附加儲存 (NAS) 和二級儲存。

高密度磁碟機（例如在 Flash Pool 聚合內配置的串行高級技術附件 (SATA) 驅動器或使用 Flash Cache 和 RAID-DP 技術配置的串行高級技術附件 (SATA) 驅動器）可提高效率，而不會影響效能和彈性。

啟用FabricPool的聚合包括全 SSD 聚合或 HDD 聚合（從ONTAP 9.8 開始）作為本機效能層和指定為雲層的物件儲存。設定FabricPool可協助您根據資料是否經常被存取來管理應儲存哪個儲存層（本機層或雲端）。

精簡配置、Snapshot 副本、重複資料刪除、資料壓縮、使用SnapVault和磁碟區SnapMirror的精簡複製以及FlexClone等技術可以實現更好的節省。您可以單獨或一起使用這些技術來實現最大的儲存效率。

新增磁碟並重新分配數據

您可以向聚合添加磁碟以增加該聚合的儲存容量和效能。新增磁碟後，只有在新增的磁碟之間重新分配資料後，您才會看到讀取效能的提升。

當 Unified Manager 收到由動態閾值或系統定義的效能閾值觸發的聚合事件時，您可以使用這些說明：

- 當您收到動態閾值事件時，在事件詳細資訊頁面上，代表爭用聚合的叢集元件圖示將以紅色突出顯示。
圖示下方的括號中是聚合的名稱，用於標識可以新增磁碟的聚合。
- 當您收到系統定義的閾值事件時，在事件詳細資訊頁面上，事件描述文字會列出出現問題的聚合的名稱。
您可以在此聚合上新增磁碟並重新指派資料。

新增到聚合的磁碟必須已存在於叢集中。如果叢集沒有可用的額外磁碟，您可能需要聯絡管理員或購買更多磁碟。您可以使用ONTAP系統管理員或ONTAP命令將磁碟新增至聚合。



僅在使用 HDD 和 Flash Pool 聚合時才應重新分配資料。不要在 SSD 或 FabricPool 聚合上重新指派資料。

在節點上啟用快閃記憶體如何提高工作負載效能

您可以透過在叢集中的每個節點上啟用 Flash Cache™ 智慧資料快取來提高工作負載效能。

快閃記憶體模組（或基於 PCIe 的效能加速模組）透過充當智慧外部讀取快取來優化隨機讀取密集型工作負載的效能。此硬體與ONTAP的WAFL外部快取軟體元件協同工作。

在 Unified Manager 的「事件詳細資料」頁面上，代表爭用聚合的叢集元件圖示以紅色突出顯示。圖示下方的括號中是聚合的名稱，用於標識聚合。您可以在聚合所在的節點上啟用快閃記憶體。

您可以使用ONTAP System Manager 或ONTAP指令來查看 Flash Cache 是否已安裝或啟用，如果尚未啟用，請啟用它。以下命令指示特定節點上是否啟用了 Flash Cache：**cluster::> run local options flexscale.enable**

有關 Flash Cache 及其使用要求的更多信息，請參閱以下技術報告：

["技術報告 3832：快閃記憶體快取最佳實務指南"](#)

在儲存聚合上啟用 Flash Pool 可以如何提高工作負載效能

您可以透過在聚合上啟用 Flash Pool 功能來提高工作負載效能。Flash Pool 是包含 HDD 和 SSD 的聚合體。HDD 用於主存儲，SSD 提供高效能讀寫快取以提高整體效能。

在 Unified Manager 中，「事件詳細資料」頁面顯示存在爭用的聚合的名稱。您可以使用ONTAP系統管理員或ONTAP指令來查看是否為聚合啟用了 Flash Pool。如果您安裝了 SSD，則可以使用命令列介面來啟用它。如果您安裝了 SSD，則可以在聚合上執行以下命令以查看 Flash Pool 是否已啟用：**cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled**

在此命令中，`aggr_name`是聚合的名稱，例如爭用中的聚合。

有關 Flash Pool 及其使用要求的更多信息，請參閱《叢集模式Data ONTAP實體儲存管理指南》。

MetroCluster配置健康檢查

您可以使用 Unified Manager 透過 IP 或 FC 查看MetroCluster配置中叢集的運作狀況。健康狀況和事件可協助您確定是否存在可能影響工作負載效能的硬體或軟體問題。

如果您將 Unified Manager 設定為傳送電子郵件警報，則可以檢查電子郵件中是否存在可能導致效能事件的本機或遠端叢集的任何健康問題。在 Unified Manager GUI 中，您可以選擇 事件管理 來查看目前事件列表，然後使用篩選器僅顯示MetroCluster設定事件。

有關詳細信息，請參閱["檢查MetroCluster配置中叢集的運作狀況"](#)

MetroCluster配置驗證

透過確保正確設定MetroCluster配置，您可以防止MetroCluster透過 FC 和 IP 配置中的鏡像工作負載出現效能問題。您也可以透過變更配置或升級軟體或硬體組件來提高工作負載效能。

參考 ["MetroCluster文檔"](#)有關在MetroCluster配置中設定叢集的說明，包括光纖通道 (FC) 交換器、電纜和交換器間連結 (ISL)。它還可以幫助您配置MetroCluster軟體，以便本地和遠端叢集可以與鏡像磁碟區資料進行通訊。有關MetroCluster over IP 設定的特定信息，請參閱 ["安裝MetroCluster IP 配置"](#)。

您可以將MetroCluster配置與 ["MetroCluster文檔"](#)確定更改或升級MetroCluster配置中的組件是否可以提高工作負載效能。這個比較可以幫助您回答以下問題：

- 這些控制器是否適合您的工作負載？
- 您是否需要將 ISL 捆綁升級到更大的頻寬以處理更多的吞吐量？
- 您能否調整交換器上的緩衝區到緩衝區信用 (BBC) 來增加頻寬？
- 如果您的工作負載對固態硬碟 (SSD) 儲存具有較高的寫入吞吐量，您是否需要升級 FC 到 SAS 橋接器以適應吞吐量？

相關資訊

- 有關更換或升級MetroCluster組件的信息，請參閱 ["MetroCluster文檔"](#)。
- 有關升級控制器的信息，請參閱 ["使用切換和切回升級MetroCluster FC 配置中的控制器"](#)和 ["使用切換和切回升級MetroCluster IP 配置中的控制器"](#)

將工作負載移至不同的聚合

您可以使用 Unified Manager 來協助識別比工作負載目前所在聚合繁忙程度較低的聚合，然後您可以將選定的磁碟區或 LUN 移至該聚合。將高效能工作負載移至較不繁忙的聚合體或啟用了快閃記憶體體的聚合體，可使工作負載更有效率地運作。

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。

- 您必須記錄目前存在效能問題的聚合的名稱。
- 您必須記錄聚合接收事件的日期和時間。
- Unified Manager 必須收集並分析一個月或更長時間的效能資料。

這些步驟可協助您識別以下資源，以便您可以將高效能工作負載移至使用率較低的聚合：

- 同一集群中利用率較低的聚合
- 目前聚合中性能最高的捲

步驟

1. 確定集群中利用率最低的聚合：

- a. 在「*事件*詳細資料」頁面上，按一下聚合所在叢集的名稱。

集群詳細資訊顯示在效能/集群登陸頁面中。

- b. 在「摘要」頁面上，按一下「管理物件」窗格中的「聚合」。

顯示此叢集上的聚合清單。

- c. 按一下「使用率」列，依利用率最低的順序對聚合進行排序。

您還可以識別那些具有最大*可用容量*的聚合。這提供了您可能想要移動工作負載的潛在聚合清單。

- d. 寫下要將工作負載移到的聚合的名稱。

2. 從接收事件的聚合中辨識高效能磁碟區：

- a. 點選存在效能問題的聚合。

聚合詳細資訊顯示在效能/聚合資源管理器頁面中。

- b. 從*時間範圍*選擇器中，選擇*過去 30 天*，然後按一下*套用範圍*。

這使您能夠查看比預設 72 小時更長的效能歷史記錄週期。您想要移動持續使用大量資源的捲，而不僅僅是在過去 72 小時內。

- c. 從*檢視和比較*控制項中，選擇*此聚合上的磁碟區*。

顯示此聚合上的FlexVol磁碟區和FlexGroup組成磁碟區的清單。

- d. 按最高 MB/s 對磁碟區進行排序，然後按最高 IOPS 對磁碟區進行排序，以查看效能最高的磁碟區。

- e. 寫下要移動到不同聚合的磁碟區的名稱。

3. 將高效能磁碟區移至您確定為利用率較低的聚合。

您可以使用ONTAP System Manager、OnCommand Workflow Automation、ONTAP指令或這些工具的組合來執行行動操作。

幾天後，檢查您是否從該節點或聚合接收到相同類型的事件。

將工作負載移至其他節點

您可以使用 Unified Manager 來協助識別比目前執行工作負載的節點繁忙程度較低的其他節點上的聚合，然後您可以將選定的磁碟區移至該聚合。將高效能工作負載移至較不繁忙的節點上的聚合體，可使兩個節點上的工作負載更有效率地執行。

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。
- 您必須記錄目前存在效能問題的節點的名稱。
- 您必須記錄節點接收效能事件的日期和時間。
- Unified Manager 必須收集並分析一個月或更長時間的效能資料。

此流程可協助您識別以下資源，以便您可以將高效能工作負載移至使用率較低的節點：

- 在同一叢集中具有最大可用性能容量的節點
- 新節點上具有最大可用性能容量的聚合
- 當前節點上效能最高的捲

步驟

1. 確定叢集中具有最大可用性能容量的節點：

- a. 在「事件詳情」頁面，按一下該節點所在叢集的名稱。

叢群詳細資訊顯示在效能/叢群登陸頁面中。

- b. 在「摘要」標籤上，按一下「管理物件」窗格中的「節點」。

顯示該叢集上的節點清單。

- c. 按一下「已使用的效能容量」列，以使用率最低的百分比對節點進行排序。

這提供了您可能想要將工作負載移動到的潛在節點的清單。

- d. 寫下您想要將工作負載移動到的節點的名稱。

2. 確定新節點上利用率最低的聚合：

- a. 在左側導覽窗格中，按一下“儲存”>“聚合”，然後從“檢視”功能表中選擇“效能”>“所有聚合”。

將顯示“效能：所有聚合”視圖。

- b. 點擊“過濾”，從左側下拉選單中選擇“節點”，在文字欄位中輸入節點的名稱，然後點擊“套用篩選器”。

效能：所有聚合視圖將重新顯示此節點上可用的聚合清單。

- c. 按一下「已使用的效能容量」列，以最少使用對聚合進行排序。

這提供了您可能想要移動工作負載的潛在聚合清單。

- d. 寫下要將工作負載移到的聚合的名稱。

3. 從接收事件節點識別高效能工作負載：
 - a. 返回活動的「活動詳情」頁面。
 - b. 在「受影響的磁碟區」欄位中，按一下卷數的連結。

效能：所有磁碟區視圖顯示該節點上磁碟區的篩選清單。
 - c. 按一下「總容量」列，依已指派的可用空間對磁碟區進行排序。

這提供了您可能想要移動的潛在磁碟區的清單。
 - d. 記下要移動的磁碟區的名稱以及它們所在的目前聚合的名稱。
4. 將磁碟區移至您確定為在新節點上具有最大可用性能容量的聚合。

您可以使用ONTAP System Manager、OnCommand Workflow Automation、ONTAP指令或這些工具的組合來執行行動操作。

幾天後，您可以檢查是否從該節點或聚合接收到相同類型的事件。

將工作負載移動到不同節點上的聚合

您可以使用 Unified Manager 來協助識別比工作負載目前執行的節點繁忙程度較低的其他節點上的聚合，然後您可以將選定的磁碟區移至該聚合。將高效能工作負載移至較不繁忙的節點上的聚合體，可使兩個節點上的工作負載更有效率地執行。

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。
- 您必須記錄目前存在效能問題的節點的名稱。
- 您必須記錄節點接收效能事件的日期和時間。
- Unified Manager 必須收集並分析一個月或更長時間的效能資料。

這些步驟可協助您識別以下資源，以便您可以將高效能工作負載移至使用率較低的節點：

- 同一叢集中利用率較低的節點
- 新節點上利用率最低的聚合
- 當前節點上效能最高的捲

步驟

1. 確定叢集中利用率最低的節點：
 - a. 在「*事件*詳細資料」頁面中，按一下節點所在叢集的名稱。

集群詳細資訊顯示在效能/集群登陸頁面中。
 - b. 在「摘要」頁面上，按一下「管理物件」窗格中的「節點」。

顯示該叢集上的節點清單。

c. 點選「利用率」欄位依利用率最低的順序對節點進行排序。

您還可以識別具有最大*可用容量*的節點。這提供了您可能想要將工作負載移動到的潛在節點的清單。

d. 寫下您想要將工作負載移動到的節點的名稱。

2. 確定新節點上利用率最低的聚合：

a. 在左側導覽窗格中，按一下“儲存”>“聚合”，然後從“檢視”功能表中選擇“效能”>“所有聚合”。

將顯示“效能：所有聚合”視圖。

b. 點擊“過濾”，從左側下拉選單中選擇“節點”，在文字欄位中輸入節點的名稱，然後點擊“套用篩選器”。

效能：所有聚合視圖將重新顯示此節點上可用的聚合清單。

c. 按一下「使用率」列，依利用率最低的順序對聚合進行排序。

您還可以識別那些具有最大*可用容量*的聚合。這提供了您可能想要移動工作負載的潛在聚合清單。

d. 寫下要將工作負載移到的聚合的名稱。

3. 從接收事件的節點識別高效能工作負載：

a. 返回活動的「活動」詳細資訊頁面。

b. 在「受影響的磁碟區」欄位中，按一下卷數的連結。

效能：所有磁碟區視圖顯示該節點上磁碟區的篩選清單。

c. 按一下「總容量」列，依已指派的最高空間對磁碟區進行排序。

這提供了您可能想要移動的潛在磁碟區的清單。

d. 記下要移動的磁碟區的名稱以及它們所在的目前聚合的名稱。

4. 將磁碟區移至您確定為新節點上利用率較低的聚合。

您可以使用ONTAP System Manager、OnCommand Workflow Automation、ONTAP指令或這些工具的組合來執行行動操作。

幾天後，檢查您是否從該節點或聚合接收到相同類型的事件。

將工作負載移至不同 HA 對中的節點

您可以使用 Unified Manager 來協助識別不同高可用性 (HA) 對中節點上的聚合，該聚合比您的工作負載目前運行的 HA 對具有更多的可用性能容量。然後，您可以將選定的磁碟區移至新 HA 對上的聚合。

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。
- 您的集群必須至少包含兩個 HA 對

如果您的叢集中只有一個 HA 對，則無法使用此修復程序。

- 您必須記錄 HA 對中目前存在效能問題的兩個節點的名稱。
- 您必須記錄節點接收效能事件的日期和時間。
- Unified Manager 必須收集並分析一個月或更長時間的效能資料。

將高效能工作負載移至具有更多可用性能容量的節點上的聚合體，可使兩個節點上的工作負載更有效率地執行。此流程可協助您識別下列資源，以便您可以將高效能工作負載移至不同 HA 對上具有更多可用性能容量的節點：

- 在同一叢集上不同 HA 對中具有最大可用性能容量的節點
- 新節點上具有最大可用性能容量的聚合
- 當前節點上效能最高的捲

步驟

1. 辨識屬於同一叢集上不同 HA 對的節點：

- a. 在「事件詳情」頁面上，按一下節點所在叢集的名稱。

叢群詳細資訊顯示在效能/叢群登陸頁面中。

- b. 在「摘要」頁面上，按一下「管理物件」窗格中的「節點」。

此叢集上的節點清單顯示在「效能：所有節點」視圖中。

- c. 記下與目前存在效能問題的 HA 對不同的 HA 對中的節點的名稱。

2. 確定新 HA 對中具有最大可用性能容量的節點：

- a. 在「效能：所有節點」檢視中，按一下「已使用效能容量」列，依使用率最低的百分比對節點進行排序。

這提供了您可能想要將工作負載移動到的潛在節點的清單。

- b. 記下您想要將工作負載移到的不同 HA 對上的節點的名稱。

3. 確定新節點上具有最大可用性能容量的聚合：

- a. 在「效能：所有節點」視圖中，按一下該節點。

節點詳細資訊顯示在效能/節點資源管理器頁面中。

- b. 在*檢視和比較*選單中，選擇*此節點上的聚合*。

此節點上的聚合顯示在網格中。

- c. 按一下「已使用的效能容量」列，以最少使用對聚合進行排序。

這提供了您可能想要移動工作負載的潛在聚合清單。

- d. 寫下要將工作負載移到的聚合的名稱。

4. 從接收事件的節點中辨識高效能工作負載：

- a. 返回活動的「活動」詳細資訊頁面。

b. 在「受影響的磁碟區」欄位中，按一下第一個節點的捲數連結。

效能：所有磁碟區視圖顯示該節點上磁碟區的篩選清單。

c. 按一下「總容量」列，依已指派的最高空間對磁碟區進行排序。

這提供了您可能想要移動的潛在磁碟區的清單。

d. 記下要移動的磁碟區的名稱以及它們所在的目前聚合的名稱。

e. 針對此事件的第二個節點執行步驟 4c 和 4d，以確定您想要從該節點移動的可能的磁碟區。

5. 將磁碟區移至您確定為在新節點上具有最大可用性能容量的聚合。

您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 指令或這些工具的組合來執行行動操作。

幾天後，您可以檢查是否從該節點或聚合接收到相同類型的事件。

將工作負載移至不同 HA 對中的另一個節點

您可以使用 Unified Manager 來協助識別不同 HA 對中節點上的聚合，該聚合的繁忙程度低於您的工作負載目前正在執行的 HA 對。然後，您可以將選定的磁碟區移至新 HA 對上的聚合。將高效能工作負載移至較不繁忙的節點上的聚合體，可使兩個節點上的工作負載更有效率地執行。

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。
- 您的叢集必須至少包含兩個 HA 對；如果您的叢集中只有一個 HA 對，則無法使用此修復程序。
- 您必須記錄 HA 對中目前存在效能問題的兩個節點的名稱。
- 您必須記錄節點接收效能事件的日期和時間。
- Unified Manager 必須收集並分析一個月或更長時間的效能資料。

這些步驟可協助您識別以下資源，以便您可以將高效能工作負載移至不同 HA 對上使用率較低的節點：

- 在同一集群上不同 HA 對中利用率較低的節點
- 新節點上利用率最低的聚合
- 當前節點上效能最高的捲

步驟

1. 辨識屬於同一叢集上不同 HA 對的節點：

a. 在左側導覽窗格中，按一下“儲存”>“叢集”，然後從“檢視”功能表中選擇“效能”>“所有叢集”。

效能：顯示所有叢集視圖。

b. 按一下目前叢集的「節點數」欄位中的數字。

將顯示“效能：所有節點”視圖。

- c. 記下與目前存在效能問題的 HA 對不同的 HA 對中的節點的名稱。
2. 確定新 HA 對中使用率最低的節點：
 - a. 點選「利用率」欄位依利用率最低的順序對節點進行排序。

您還可以識別具有最大*可用容量*的節點。這提供了您可能想要將工作負載移動到的潛在節點的清單。
 - b. 寫下您想要將工作負載移動到的節點的名稱。
3. 確定新節點上利用率最低的聚合：
 - a. 在左側導覽窗格中，按一下“儲存”>“聚合”，然後從“檢視”功能表中選擇“效能”>“所有聚合”。

將顯示“效能：所有聚合”視圖。
 - b. 點擊“過濾”，從左側下拉選單中選擇“節點”，在文字欄位中輸入節點的名稱，然後點擊“套用篩選器”。

效能：所有聚合視圖將重新顯示此節點上可用的聚合清單。
 - c. 按一下「使用率」列，依利用率最低的順序對聚合進行排序。

您還可以識別那些具有最大*可用容量*的聚合。這提供了您可能想要移動工作負載的潛在聚合清單。
 - d. 寫下要將工作負載移到的聚合的名稱。
4. 從接收事件的節點中辨識高效能工作負載：
 - a. 返回活動的「活動」詳細資訊頁面。
 - b. 在「受影響的磁碟區」欄位中，按一下第一個節點的捲數連結。

效能：所有磁碟區視圖顯示該節點上磁碟區的篩選清單。
 - c. 按一下「總容量」列，依已指派的最高空間對磁碟區進行排序。

這提供了您可能想要移動的潛在磁碟區的清單。
 - d. 記下要移動的磁碟區的名稱以及它們所在的目前聚合的名稱。
 - e. 針對此事件的第二個節點執行步驟 4c 和 4d，以確定您想要從該節點移動的可能的磁碟區。
5. 將磁碟區移至您確定為新節點上利用率較低的聚合。

您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 指令或這些工具的組合來執行行動操作。

幾天後，檢查您是否從該節點或聚合接收到相同類型的事件。

使用 QoS 策略設定來優先處理此節點上的工作

您可以對 QoS 策略群組設定限制，以控制其包含的工作負載的每秒 I/O (IOPS) 或 MBps 吞吐量限制。如果工作負載位於沒有設定限制的策略群組（例如預設策略群組）中，或設定的限制無法滿足您的需求，您可以增加設定的限制或將工作負載移至具有所需限制的新策略群組或現有策略群組。

如果節點上的效能事件是由工作負載過度使用節點資源引起的，則事件詳細資訊頁面上的事件描述會顯示涉及的磁碟區清單的連結。在「效能/磁碟區」頁面中，您可以按 IOPS 和 MBps 對受影響的磁碟區進行排序，以查看哪些工作負載的使用率最高，可能導致該事件。

透過將過度使用節點資源的磁碟區分配給更嚴格的策略群組設置，策略群組可以限制工作負載以限制其活動，從而減少該節點上資源的使用。

您可以使用ONTAP系統管理員或ONTAP指令來管理策略群組，包括下列任務：

- 建立策略組
- 在策略群組中新增或刪除工作負載
- 在策略組之間移動工作負載
- 更改策略群組的吞吐量限制

刪除非活動捲和 LUN

當聚合可用空間被確定為問題時，您可以搜尋未使用的磁碟區和 LUN 並將其從聚合中刪除。這有助於緩解磁碟空間不足的問題。

如果聚合上的效能事件是由磁碟空間不足引起的，則您可以透過幾種方法確定哪些磁碟區和 LUN 不再使用。

要識別未使用的磁碟區：

- 在事件詳細資訊頁面上，*受影響的物件數*欄位提供了一個鏈接，顯示受影響卷的清單。

按一下該連結可在「效能：所有磁碟區」檢視中顯示磁碟區。從那裡您可以按 **IOPS** 對受影響的捲進行排序，以查看哪些磁碟區尚未啟動。

要識別未使用的 LUN：

1. 在事件詳細資料頁面中，記下發生事件的聚合的名稱。
2. 在左側導覽窗格中，按一下“儲存”>“LUN”，然後從“檢視”功能表中選擇“效能”>“所有 LUN”。
3. 按一下“過濾”，從左側下拉選單中選擇“聚合”，在文字欄位中輸入聚合的名稱，然後按一下“套用篩選器”。
4. 按 **IOPS** 對受影響的 LUN 的結果清單進行排序，以查看不活動的 LUN。

確定未使用的磁碟區和 LUN 後，您可以使用ONTAP系統管理員或ONTAP指令刪除這些物件。

新增磁碟並執行聚合佈局重建

您可以向聚合添加磁碟以增加該聚合的儲存容量和效能。新增磁碟後，只有在重建聚合後才能看到效能的提升。

當您在事件詳細資料頁面上收到系統定義的閾值事件時，事件描述文字會列出出現問題的聚合的名稱。您可以在此聚合上新增磁碟並重建資料。

新增到聚合的磁碟必須已存在於叢集中。如果叢集沒有可用的額外磁碟，您可能需要聯絡管理員或購買更多磁碟。您可以使用ONTAP系統管理員或ONTAP命令將磁碟新增至聚合。

在 Unified Manager 伺服器 and 外部資料提供者之間建立連接

Unified Manager 伺服器和外部資料提供者之間的連線可讓您將叢集效能資料傳送至外部伺服器，以便儲存管理員可以使用第三方軟體繪製效能指標圖表。

Unified Manager 伺服器和外部資料提供者之間的連線是透過維護控制台中標有「外部資料提供者」的選單選項建立的。

可以傳送到外部伺服器的效能數據

Unified Manager 從其監控的所有叢集收集各種效能資料。您可以將特定的資料組傳送到外部伺服器。

根據您想要繪製的效能數據，您可以選擇傳送以下一組統計資料：

統計資料組	包含的數據	細節
效能監視器	以下物件的高階效能統計資訊： <ul style="list-style-type: none">• LUN• 卷	此群組提供所有受監控叢集中所有 LUN 和磁碟區的總 IOPS 或延遲。 該組提供的統計數據最少。
資源利用率	以下物件的資源利用率統計： <ul style="list-style-type: none">• 節點• 聚合	此群組提供節點的利用率統計資訊並聚合所有受監控叢集中的實體資源。 它還提供效能監視器群組中收集的統計資料。
深入研究	所有追蹤物件的低階讀/寫和每個協定的統計資料： <ul style="list-style-type: none">• 節點• 聚合• LUN• 卷• 磁碟• LIF• 連接埠/NIC	此群組為所有受監控叢集中的所有七種追蹤物件類型提供讀取/寫入和每個協定的細分。 它還提供效能監視器組和資源利用率組中收集的統計資料。 該組提供了最多的統計數據。



如果儲存系統上的叢集或叢集物件的名稱發生更改，則新舊物件都會包含外部伺服器上的效能資料（稱為「metric_path」）。這兩個對象並不相關，而是同一個對象。例如，如果將磁碟區的名稱從“volume1_acct”變更為“acct_vol1”，您將看到舊磁碟區的舊效能資料和新磁碟區的新效能資料。

有關可傳送至外部資料提供者的所有效能計數器的列表，請參閱知識庫文章 30096。

"可匯出至外部資料提供者的 Unified Manager 效能計數器"

設定 Graphite 以從 Unified Manager 接收效能數據

Graphite 是一個用於收集和繪製電腦系統效能資料的開放軟體工具。您的 Graphite 伺服器 and 軟體必須正確配置才能從 Unified Manager 接收統計資料。

NetApp 不會測試或驗證 Graphite 或其他第三方工具的特定版本。



Graphite 伺服器未從 Unified Manager 接收磁碟區的效能資料。

按照安裝說明安裝 Graphite 後，您需要進行以下變更以支援從 Unified Manager 傳輸統計資料：

- 在 `/opt/graphite/conf/carbon.conf` 文件，每分鐘可以在 Graphite 伺服器上建立的最大文件數必須設定為 `200 (MAX_CREATES_PER_MINUTE = 200)`。

根據您配置中的群集數量和您選擇發送的統計對象，可能需要最初建立數千個新檔案。以每分鐘 200 個檔案的速度，可能需要 15 分鐘或更長時間才能初始建立所有指標檔案。建立所有唯一度量檔案後，此參數不再相關。

- 如果您在使用 IPv6 位址部署的伺服器上執行 Graphite，則 `/opt/graphite/conf/carbon.conf` 文件必須從“`0.0.0.0`”更改為“`::`”(`LINE_RECEIVER_INTERFACE = ::`)
- 在 `/opt/graphite/conf/storage-schemas.conf` 文件，``retentions`` 必須使用參數將頻率設定為 5 分鐘，並將保留期設定為與您的環境相關的天數。

保留期可以根據您的環境允許的時間長短而定，但對於至少一個保留設置，頻率值必須設定為 5 分鐘。在以下範例中，使用 `pattern`` 參數，其值將初始頻率設定為 5 分鐘，將保留期設定為 100 天： `[OPM]`

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



如果預設供應商標籤從「netapp-performance」變更為其他標籤，則該變更必須反映在 `pattern`` 參數也是如此。



如果 Unified Manager 伺服器嘗試傳送效能數據時 Graphite 伺服器不可用，則不會傳送數據，且收集的數據中會出現差距。

設定從 Unified Manager 伺服器到外部資料提供者的連接

Unified Manager 可以將叢集效能資料傳送到外部伺服器。您可以指定傳送的統計資料的類

型以及傳送資料的間隔。

開始之前

- 您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID。
- 您必須具有有關外部資料提供者的以下資訊：
 - 伺服器名稱或 IP 位址 (IPv4 或 IPv6)
 - 伺服器預設連接埠 (如果不使用預設連接埠 2003)
- 您必須設定遠端伺服器和第三方軟體，以便它可以從 Unified Manager 伺服器接收統計資料。
- 您必須知道要傳送哪一組統計資料：
 - PERFORMANCE_INDICATOR：效能監視器統計資訊
 - RESOURCE_UTILIZATION：資源利用率和效能監視器統計資料
 - DRILL_DOWN：所有統計數據
- 您必須知道傳輸統計資料的時間間隔：5、10 或 15 分鐘

預設情況下，Unified Manager 每隔 5 分鐘收集一次統計資料。如果將傳輸間隔設定為 10 (或 15) 分鐘，則每次傳輸期間發送的資料量是使用預設 5 分鐘間隔時的兩倍 (或三倍)。



如果將 Unified Manager 效能收集間隔變更為 10 或 15 分鐘，則必須變更傳輸間隔，使其等於或大於 Unified Manager 收集間隔。

您可以設定一台 Unified Manager 伺服器和一台外部資料提供者伺服器之間的連線。

步驟

1. 以維護使用者身分登入 Unified Manager 伺服器的維護控制台。

顯示 Unified Manager 維護控制台提示。

2. 在維護控制台中，輸入*外部資料提供者*選單選項的編號。

顯示外部伺服器連線選單。

3. 鍵入「新增/修改伺服器連線」選單選項的編號。

顯示目前伺服器連線資訊。

4. 出現提示時，輸入 `y` 繼續。

5. 出現提示時，輸入目標伺服器的 IP 位址或名稱以及伺服器連接埠資訊 (如果與預設連接埠 2003 不同)。

6. 出現提示時，輸入 `y` 驗證您輸入的資訊是否正確。

7. 按任意鍵返回外部伺服器連線選單。

8. 鍵入「修改伺服器設定」選單選項的編號。

顯示目前伺服器設定資訊。

9. 出現提示時，輸入 `y` 繼續。

10. 出現提示時，輸入要傳送的統計資料類型、傳送統計資料的時間間隔以及是否要立即啟用統計資料的傳輸：

為了..	進入...
統計組ID	<p>0- PERFORMANCE_INDICATOR (預設)</p> <p>1- 資源利用率</p> <p>2- DRILL_DOWN</p>
供應商標籤	<p>外部伺服器上儲存統計資訊的資料夾的描述性名稱。“netapp-performance”是預設名稱，但您可以輸入其他值。</p> <p>透過使用點分符號，您可以定義分層資料夾結構。例如，透過輸入 <code>stats.performance.netapp</code> 統計資料位於 <code>stats > performance > netapp</code>。</p>
傳輸間隔	5(預設), 10 , 或者 `15`分分鐘
啟用/停用	<p>0- 停用</p> <p>1- 啟用 (預設)</p>

11. 出現提示時，輸入 `y` 驗證您輸入的資訊是否正確。

12. 按任意鍵返回外部伺服器連線選單。

13. 類型 `x` 退出維護控制台。

設定連線後，選定的效能資料將依照您指定的時間間隔傳送到目標伺服器。指標需要幾分鐘才會開始出現在外部工具中。您可能需要刷新瀏覽器才能看到指標層次結構中的新指標。

監視和管理集群健康狀況

Active IQ Unified Manager健康監控簡介

Active IQ Unified Manager（以前稱為OnCommand Unified Manager）可協助您透過集中式使用者介面監控執行ONTAP軟體的大量系統。Unified Manager 伺服器基礎架構提供可擴充性、可支援性以及增強的監控和通知功能。

Unified Manager 的主要功能包括監控、警報、管理叢集的可用性和容量、管理保護功能以及捆綁診斷資料並將其傳送給技術支援。

您可以使用 Unified Manager 來監控您的叢集。當叢集中出現問題時，Unified Manager 會透過事件通知您此類問題的詳細資訊。有些事件還會為您提供可以採取的補救措施來糾正問題。您可以設定事件警報，以便在出現問題時透過電子郵件和 SNMP 陷阱通知您。

您可以使用 Unified Manager 透過將儲存物件與註解關聯來管理環境中的儲存物件。您可以建立自訂註釋，並透過規則將叢集、儲存虛擬機器 (SVM) 和磁碟區與註釋動態關聯。

您也可以使用容量和運行狀況圖表中提供的資訊來為各個叢集物件規劃叢集物件的儲存需求。

物理和邏輯容量

Unified Manager 利用用於ONTAP儲存物件的實體和邏輯空間的概念。

- 物理容量：物理空間是指磁碟區中使用的實體儲存區塊。由於儲存效率功能（例如重複資料刪除和壓縮）減少了數據，因此「物理已使用容量」通常小於邏輯已使用容量。
- 邏輯容量：邏輯空間是指磁碟區中的可用空間（邏輯區塊）。邏輯空間是指理論上如何使用空間，不考慮重複資料刪除或壓縮的結果。「使用的邏輯空間」是使用的實體空間加上已配置的儲存效率功能（例如重複資料刪除和壓縮）所節省的空间。這個測量值通常看起來大於物理使用容量，因為這沒有反映資料壓縮和物理空間的其他減少。因此，總邏輯容量可能高於配置的空间。

容量測量單位

Unified Manager 根據 1024 (2¹⁰) 位元組的二進位單位計算儲存容量。在ONTAP 9.10.0 及更早版本中，這些單位顯示為 KB、MB、GB、TB 和 PB。從ONTAP 9.10.1 開始，它們在 Unified Manager 中顯示為 KiB、MiB、GiB、TiB 和 PiB。



對於ONTAP的所有版本，吞吐量使用的單位仍然是每秒千位元組 (Kbps)、每秒兆位元組 (Mbps)、每秒千兆位元組 (Gbps) 或每秒太字節 (Tbps) 等等。

Unified Manager for ONTAP 9.10.0 及更早版本中顯示的容量單位	Unified Manager for ONTAP 9.10.1 中顯示的容量單位	計算	以位元組為單位的值
知識庫	基布	1024	1024 位元組
MB	資訊局	1024 * 1024	1,048,576 字節

Unified Manager for ONTAP 9.10.0 及更早版本中顯示的容量單位	Unified Manager for ONTAP 9.10.1 中顯示的容量單位	計算	以位元組為單位的值
英國	吉布	1024 * 1024 * 1024	1,073,741,824 字節
結核病	硼化鈦	1024 * 1024 * 1024 * 1024	1,099,511,627,776 字節

Unified Manager 健康監控功能

Unified Manager 建立在伺服器基礎架構上，可提供可擴充性、可支援性以及增強的監控和通知功能。 Unified Manager 支援監控執行ONTAP軟體的系統。

Unified Manager 包含以下功能：

- 發現、監控和通知安裝了ONTAP軟體的系統：
 - 實體物件：節點、磁碟、磁碟架、SFO 對、連接埠和快閃記憶體
 - 邏輯物件：叢集、儲存虛擬機器 (SVM)、聚合、磁碟區、LUN、命名空間、qtree、LIF、Snapshot 副本、連線路徑、NFS 共用、SMB 共用、使用者和群組配額、QoS 原則群組和啟動器群組
 - 協定：CIFS、NFS、FC、iSCSI、NVMe 和 FCoE
 - 儲存效率：SSD 聚合、Flash Pool 聚合、FabricPool聚合、重複資料刪除和壓縮
 - 保護： SnapMirror關係（同步和非同步）和SnapVault關係
- 查看叢集發現和監控狀態
- MetroCluster透過 FC 和 IP 配置：檢視和監控叢集組件的配置、問題和連線狀態。適用於 FC 設定上的MetroCluster的 MetroCluster交換器和網橋
- 增強的警報、事件和閾值基礎設施
- LDAP、LDAPS、SAML 身份驗證和本機使用者支持
- RBAC（針對一組預先定義的角色）
- AutoSupport和支援包
- 增強的儀表板可顯示環境的容量、可用性、保護和效能健康狀況
- 磁碟區移動互通性、磁碟區移動歷史記錄和連接路徑變更歷史記錄
- 影響範圍區域以圖形方式顯示受某些故障磁碟、 MetroCluster聚合鏡像降級和MetroCluster備用磁碟遺留事件等事件影響的資源
- 顯示MetroCluster事件影響的「可能影響」區域
- 建議的糾正措施區域，其中顯示了可以執行的操作，以解決某些故障磁碟、 MetroCluster聚合鏡像降級和MetroCluster備用磁碟遺留等事件
- 可能受影響的資源區域，顯示可能受事件（例如捲脫機事件、磁碟區限制事件和精簡配置磁碟區空間處於風險事件）影響的資源
- 支援具有FlexVol或FlexGroup磁碟區的 SVM

- 支援監控節點根卷
- 增強的 Snapshot 副本監控，包括計算可回收空間和刪除 Snapshot 副本
- 儲存對象的註解
- 報告建立和管理儲存物件訊息，例如實體和邏輯容量、利用率、空間節省、效能和相關事件
- 與OnCommand Workflow Automation整合以執行工作流程

儲存自動化商店包含經NetApp認證的自動化儲存工作流程包，這些工作流程包專為與OnCommand Workflow Automation(WFA) 配合使用而開發。您可以下載這些套件，然後將其匯入 WFA 來執行它們。自動化工作流程可在此處取得：

["儲存自動化商店"](#)

用於管理儲存系統健康狀況的 **Unified Manager** 介面

這些部分包含有關Active IQ Unified Manager提供的兩個使用者介面的信息，用於解決資料儲存容量、可用性和保護問題。這兩個 UI 是 Unified Manager Web UI 和維護控制台。

如果您想要使用 Unified Manager 中的保護功能，您也必須安裝和設定OnCommand Workflow Automation (WFA)。

Unified Manager Web UI

Unified Manager Web UI 可讓管理員監控和排除與資料儲存容量、可用性和保護相關的叢集問題。

這些部分介紹了管理員可以遵循的一些常見工作流程，以解決 Unified Manager Web UI 中顯示的儲存容量、資料可用性或保護問題。

維護控制台

Unified Manager 維護控制台可讓管理員監控、診斷和解決與 Unified Manager 伺服器本身相關的作業系統問題、版本升級問題、使用者存取問題和網路問題。如果 Unified Manager Web UI 不可用，則維護控制台是存取 Unified Manager 的唯一方法。

您可以使用此資訊存取維護控制台並使用它來解決與 Unified Manager 伺服器功能相關的問題。

管理和監控叢集和叢集物件健康狀況

Unified Manager 使用定期 API 查詢和資料收集引擎從叢集收集資料。透過將叢集新增至 Unified Manager 資料庫，您可以監控和管理這些叢集的任何可用性和容量風險。

了解集群監控

您可以將叢集新增至 Unified Manager 資料庫，以監控叢集的可用性、容量和其他詳細信息，例如 CPU 使用率、介面統計資料、可用磁碟空間、qtree 使用率和機箱環境。

如果狀態異常或超出預先定義的閾值，則會產生事件。如果已設定為這樣做，當事件觸發警報時，Unified Manager 會向指定收件者傳送通知。

了解節點根卷

您可以使用 Unified Manager 監控節點根磁碟區。最佳做法是節點根磁碟區應具有足夠的容量以防止節點關閉。

當節點根磁碟區的已使用容量超過節點根磁碟區總容量的 80% 時，將產生節點根磁碟區空間將會滿事件。您可以為事件配置警報以取得通知。您可以使用 ONTAP 系統管理員或 ONTAP CLI 採取適當的措施來防止節點關閉。



如果叢集執行 ONTAP 9.14.1 版本或更高版本，則監控節點根磁碟區的功能不可用。

了解節點根聚合的事件和閾值

您可以使用 Unified Manager 監控節點根聚合。最佳做法是在根聚合中密集配置根卷，以防止節點停止運作。

預設情況下，不會為根聚合產生容量和效能事件。此外，Unified Manager 使用的閾值不適用於節點根聚合。只有技術支援代表可以修改產生這些事件的設定。當技術支援代表修改設定時，容量閾值將應用於節點根聚合。

您可以使用 ONTAP 系統管理員或 ONTAP CLI 採取適當的措施來防止節點停止。



如果叢集執行 ONTAP 9.14.1 版本或更高版本，則監控節點根聚合的功能不可用。

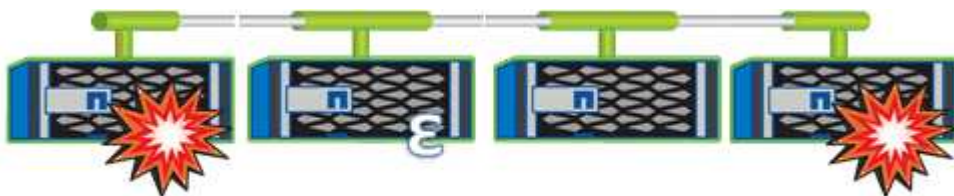
了解法定人數和 epsilon

Quorum 和 epsilon 是衡量集群健康和功能的重要指標，它們共同表明集群如何應對潛在的通訊和連接挑戰。

Quorum 是叢集完全正常運作的先決條件。當叢集處於法定人數時，大多數節點都是健康的並且可以相互通訊。當仲裁遺失時，集群將失去完成正常集群操作的能力。由於所有節點共同共享單一資料視圖，因此任何時候都只能有一個節點集合具有仲裁。因此，如果允許兩個不通訊的節點以不同的方式修改數據，就不再可能將數據協調到單一數據視圖中。

叢集中的每個節點都參與投票協議，選舉一個節點主節點；其餘每個節點都是輔助節點。主節點負責整個叢集的資訊同步。當法定人數形成後，透過持續投票來維持。如果主節點離線且叢集仍然處於仲裁狀態，則由保持在線的節點選出新的主節點。

由於在具有偶數節點的集群中存在平局的可能性，因此一個節點具有稱為 epsilon 的額外分數投票權重。如果大型群集的兩個相等部分之間的連接失敗，則包含 epsilon 的節點組將維持仲裁，假設所有節點都是健康的。例如，下圖顯示了一個四節點群集，其中兩個節點發生故障。然而，由於其中一個倖存節點擁有 epsilon，因此即使健康節點的數量未達到簡單多數，叢集仍保持法定人數。



建立叢集時，Epsilon 會自動指派到第一個節點。如果持有 epsilon 的節點變得不健康、接管其高可用性夥伴節點或被其高可用性夥伴節點接管，則 epsilon 會自動重新分配到不同 HA 對中的健康節點。

使節點脫機可能會影響叢集保持仲裁的能力。因此，如果您嘗試執行使叢集脫離法定人數或使其因失去法定人數而發生一次中斷的操作，ONTAP會發出警告訊息。您可以在進階權限層級使用 `cluster quorum-service options modify` 指令停用仲裁警告訊息。

一般來說，假設群集節點之間的連接可靠，則較大的群集比較小的群集較穩定。與 2 個節點的群集相比，在 24 個節點的群集中更容易維持半數節點加 epsilon 的簡單多數的法定人數要求。

雙節點叢集對於維持仲裁提出了一些獨特的挑戰。雙節點叢集使用叢集 HA，其中兩個節點都不持有 epsilon；相反，兩個節點都會被持續輪詢，以確保如果一個節點發生故障，另一個節點可以完全讀寫數據，並可以存取邏輯介面和管理功能。

查看叢集清單及詳情

您可以使用「健康狀況：所有群集」視圖來查看叢集清單。容量：所有叢集視圖可讓您查看有關所有叢集的儲存容量和利用率之總計資訊。

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。

您還可以使用叢集/運行狀況詳細資訊頁面查看各個叢集的詳細信息，例如叢集運行狀況、容量、配置、LIF、節點和該叢集中的磁碟。

健康狀況：所有叢集視圖、容量：所有叢集視圖和叢集/健康狀況詳細資訊頁面中的詳細資訊可協助您規劃儲存。例如，在配置新的聚合之前，您可以從「運行狀況：所有叢集」視圖中選擇一個特定的叢集，並獲取容量詳細資訊以確定該叢集是否具有所需的空間。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 在「檢視」功能表中，選擇「運行狀況：所有群集」視圖以查看運行狀況信息，或選擇「容量：所有群集」視圖以查看有關所有群集的存儲容量和利用率之詳細信息。
3. 按一下叢集名稱可在「叢集/健康」詳細資料頁面中查看該叢集的完整詳細資訊。

相關資訊

- ["叢集/健康詳情頁面"](#)
- ["效能：所有叢集視圖"](#)
- ["監控MetroCluster配置"](#)
- ["查看叢集和儲存虛擬機器的安全狀態"](#)
- ["正在評估哪些安全標準"](#)

檢查MetroCluster配置中叢集的運作狀況

您可以使用Active IQ Unified Manager (Unified Manager) 檢查MetroCluster over FC 和MetroCluster over IP 設定中的叢集及其元件的運作狀況。如果叢集涉及 Unified Manager 偵測到的效能事件，則健康狀況可以協助您確定硬體或軟體問題是否導致了該事件。

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。
- 您必須已經分析了MetroCluster配置的效能事件並取得了所涉及叢集的名稱。
- 透過 FC 和 IP 的MetroCluster配置中的兩個叢集必須由同一個 Unified Manager 實例監控。

確定MetroCluster透過 FC 配置中的叢集運作狀況

請依照下列步驟確定MetroCluster over FC 配置中的叢集運作狀況。

步驟

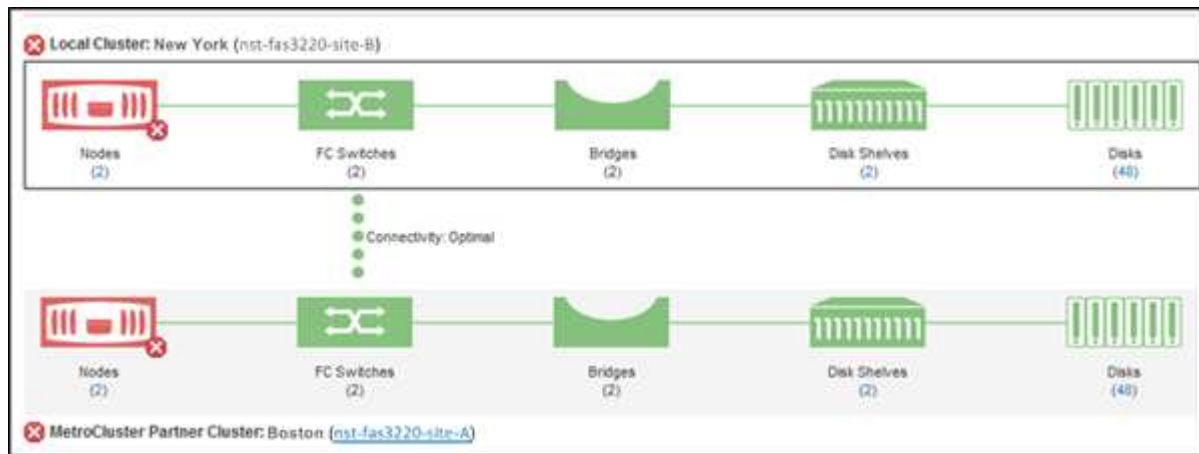
1. 在左側導覽列中，點選“事件管理”，顯示事件清單。
2. 在過濾器面板中，選擇「來源類型」類別下的所有MetroCluster過濾器。您將看到您的環境中針對所有MetroCluster配置引發的所有事件。
3. 在MetroCluster事件旁邊，按一下叢集的名稱。



如果沒有顯示MetroCluster事件，您可以使用搜尋列搜尋與您的MetroCluster over FC 設定相關的事件所涉及叢集的名稱。

健康狀況：所有群集視圖顯示有關該事件的詳細資訊。

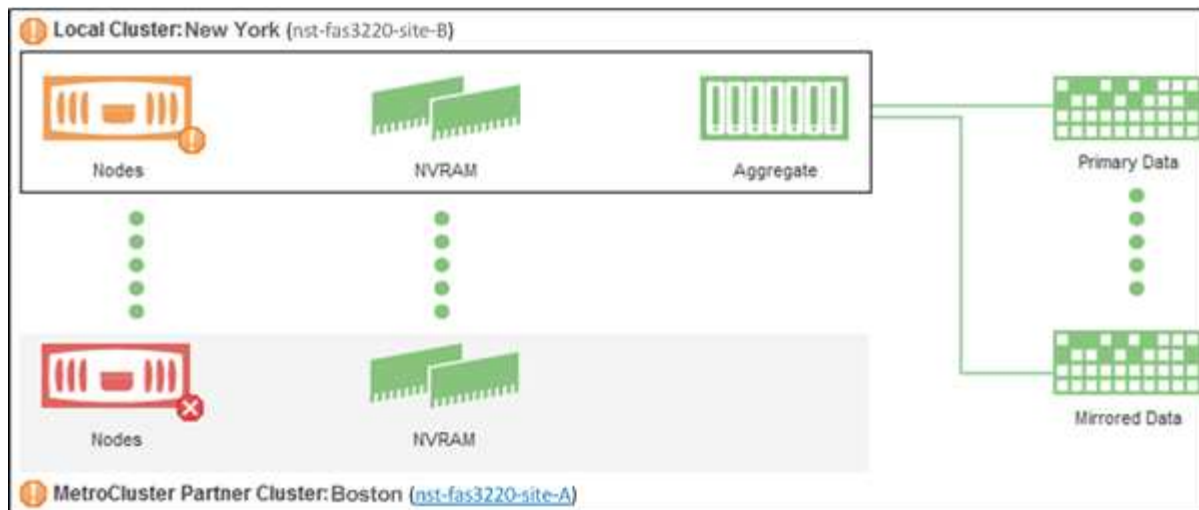
4. 選擇「MetroCluster Connectivity」標籤以顯示所選叢集與其夥伴叢集之間的連線運作狀況。



在此範例中，顯示了本機叢集及其夥伴叢集的名稱和元件。黃色或紅色圖示表示突出顯示的元件的健康事件。連接圖示表示叢集之間的連結。您可以將滑鼠遊標指向圖示以顯示事件訊息，或按一下圖示以顯示事件。任一集群的健康問題都可能導致性能事件。

Unified Manager 監控叢集之間連結的NVRAM元件。如果本地或合作夥伴叢集上的 FC 交換器圖示或連線圖示為紅色，則可能是連結健康問題導致了效能事件。

5. 選擇“MetroCluster複製”標籤。



在此範例中，如果本機或合作夥伴叢集上的NVRAM圖示為黃色或紅色，則NVRAM的健康問題可能導致了效能事件。如果頁面上沒有紅色或黃色圖標，則可能是合作夥伴叢集上的效能問題導致了效能事件。

確定MetroCluster over IP 配置中的叢集運作狀況

請依照下列步驟確定MetroCluster over IP 配置中的叢集運作狀況。

步驟

1. 在左側導覽列中，點選“事件管理”，顯示事件清單。
2. 在過濾器面板的“來源類型”類別下，選擇 `MetroCluster Relationship` 篩選。您將看到您的環境中針對所有MetroCluster配置引發的所有事件。



如果您看不到已報告的MetroCluster事件，您可以使用搜尋列依照與您的MetroCluster over IP 設定相關的事件所涉及叢集名稱進行搜尋。

3. 在相關的MetroCluster事件旁邊，按一下叢集的名稱。將顯示「集群」頁面，其中包含該集群的詳細資訊。有關確定健康問題的信息，請參閱["監控MetroCluster透過 IP 設定中的連線問題"](#)。

查看所有 SAN 陣列叢集的健康和容量狀態

您可以使用叢集清單頁面顯示所有 SAN 陣列叢集的健康和容量狀態。

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。

您可以在「運作狀況：所有叢集」視圖和「容量：所有叢集」視圖中查看所有 SAN 陣列叢集的概述資訊。此外，您還可以在集群/健康詳情頁面查看詳細資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 確保「個性」列顯示在*健康：所有群集*視圖中，或使用*顯示/隱藏*控制項新增它。

此列顯示您的所有 SAN 陣列叢集的「所有 SAN 陣列」。

3. 查看資訊。
4. 若要查看這些叢集中的儲存容量信息，請選擇容量：所有叢集視圖。
5. 若要查看這些叢集的運作狀況和儲存容量的詳細信息，請按一下全 SAN 陣列叢集的名稱。

在「叢集/健康詳情」頁面的「健康」、「容量」和「節點」標籤中查看詳細信息

查看節點列表及詳情

您可以使用「運行狀況：所有節點」視圖來查看叢集中的節點清單。您可以使用叢集/健康詳情頁面來查看有關受監控叢集的節點的詳細資訊。

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。

您可以查看節點狀態、包含該節點的叢集、聚合容量詳細資訊（已使用容量和總計容量）以及原始容量詳細資訊（可用容量、備用容量和總計容量）等詳細資訊。您還可以獲得有關 HA 對、磁碟架和連接埠的資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「節點」。
2. 在「**Health: All Nodes**」檢視中，按一下要查看其詳細資訊的節點。

所選節點的詳細資訊顯示在叢集/健康詳細資訊頁面中。左側窗格顯示 HA 對清單。預設情況下，HA 詳細資訊是開啟的，其中顯示與所選 HA 對相關的 HA 狀態詳細資訊和事件。

3. 要查看有關節點的其他詳細信息，請執行相應的操作：

要查看...	點擊...
有關磁碟架的詳細信息	磁碟架。
港口相關資訊	連接埠。

有關詳細信息，請參閱：For more information, see:

- ["效能：所有節點視圖"](#)
- ["查看節點和聚合可用 IOPS 值"](#)
- ["查看節點和聚合效能容量使用值"](#)

產生合約續約的硬體清單報告

您可以產生包含叢集和節點資訊完整清單的報告；例如硬體型號和序號、磁碟類型和數量、已安裝的授權等。此報告有助於在未連接到 NetAppActive IQ 平台的安全站點（「暗」站點）內續約。

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「儲存」>「節點」。
2. 轉到*健康：所有節點*視圖或*效能：所有節點*視圖。
3. 選擇*報告* > * > 硬體清單報告*。

硬體清單報告以 .csv 檔案的形式下載，其中包含截至當前日期的完整資訊。

4. 將此資訊提供給您的NetApp支援聯絡人以進行合約續約。

查看儲存虛擬機器列表和詳細信息

從「運作狀況：所有儲存虛擬機器」檢視中，您可以監控儲存虛擬機器 (SVM) 的庫存。您可以使用儲存虛擬機器/運作狀況詳細資訊頁面查看有關受監控的 SVM 的詳細資訊。

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。

您可以查看 SVM 詳細信息，例如 SVM 的容量、效率和配置。您也可以查看有關該 SVM 的相關設備和相關警報的資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 選擇以下方式之一以查看 SVM 詳細資料：
 - 若要查看所有叢集中所有 SVM 的運行狀況信息，請在「檢視」功能表中選擇「運行狀況：所有儲存虛擬機器視圖」。
 - 要查看完整詳細信息，請按一下儲存虛擬機器名稱。

您也可以透過點擊最小詳細資料對話方塊中的「查看詳細資料」來查看完整的詳細資訊。

3. 透過點選最小詳細資料對話方塊中的「檢視相關」來查看與 SVM 相關的物件。

相關資訊

- ["儲存虛擬機器：健康詳情頁面"](#)
- ["效能：所有儲存虛擬機器視圖"](#)
- ["安全：反勒索軟體視圖"](#)
- ["查看叢集和儲存虛擬機器的安全狀態"](#)
- ["關係：所有關係視圖"](#)

查看匯總列表和詳細信息

從「健康狀況：所有聚合體」視圖中，您可以監控聚合體的庫存。透過「容量：所有聚合」視圖，您可以查看有關所有叢集中聚合的容量和利用率的資訊。

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。

您可以從聚合/健康詳細資料頁面查看聚合容量和配置以及磁碟資訊等詳細資訊。如果需要，您可以在配置閾值設定之前使用這些詳細資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 選擇以下方式之一來查看聚合詳細資訊：
 - 若要查看有關所有叢集中所有聚合的健康狀況的信息，請在「檢視」功能表中選擇「健康狀況：所有聚合視圖」。
 - 若要查看有關所有叢集中所有聚合的容量和利用率的信息，請在「檢視」功能表中選擇「容量：所有聚合視圖」。
 - 要查看完整詳細信息，請按一下聚合名稱。

您也可以透過點擊最小詳細資料對話方塊中的「查看詳細資料」來查看完整的詳細資訊。

3. 透過點擊最小詳細資料對話方塊中的「檢視相關」來查看與聚合相關的物件。

相關資訊

- ["聚合/健康詳情頁面"](#)
- ["效能：所有聚合視圖"](#)
- ["自訂聚合容量報告"](#)

查看FabricPool容量資訊

您可以在這些物件的容量和效能清單和詳細資料頁面上查看叢集、聚合和磁碟區的FabricPool容量資訊。當配置了鏡像圖層時，這些頁面也會顯示FabricPool鏡像資訊。

這些頁面顯示的資訊包括本地性能層和雲層上的可用容量、兩個層中使用的容量、哪些聚合連接到雲層以及哪些卷通過將某些資訊移動到雲層來實現FabricPool功能。

當一個雲層鏡像到另一個雲端提供者（「鏡像層」）時，兩個雲層都會顯示在聚合/健康詳細資料頁面中。

步驟

1. 執行下列操作之一：

若要查看容量資訊...	這樣做...
叢集	<ol style="list-style-type: none">a. 在容量：所有叢集視圖中，按下一個叢集。b. 在叢集/健康詳情頁面，點選「設定」標籤。 顯示幕顯示該群集所連接的任何雲層的名稱。

若要查看容量資訊...	這樣做...
聚合	<p>a. 在「容量：所有聚合」檢視中，按一下「類型」欄位指示「SSD (FabricPool)」或「HDD (FabricPool)」的聚合。</p> <p>b. 在聚合/健康詳細資料頁面上，按一下「容量」標籤。</p> <p>顯示幕顯示雲層中使用的總容量。</p> <p>c. 按一下“磁碟資訊”標籤。</p> <p>顯示幕顯示雲層的名稱和使用的容量。</p> <p>d. 按一下“配置”標籤。</p> <p>顯示幕顯示雲層的名稱以及有關雲層的其他詳細資訊。</p>
卷	<p>a. 在「容量：所有磁碟區」檢視中，按一下「分層策略」欄位中出現策略名稱的磁碟區。</p> <p>b. 在磁碟區/健康詳情頁面上，按一下「設定」標籤。</p> <p>顯示幕顯示指派給該磁碟區的FabricPool分層策略的名稱。</p>

2. 在*工作負載分析*頁面中，您可以選擇*容量趨勢*區域中的「雲層視圖」來查看上個月本地效能層和雲層中使用的容量。

有關FabricPool聚合的更多信息，請參閱 ["磁碟和聚合概述"](#)。

查看儲存池詳細信息

您可以查看儲存池的詳細信息，以監控儲存池的健康狀況、總快取和可用快取以及已使用分配和可用分配。

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「儲存」>「聚合」。
2. 按一下聚合名稱。

顯示所選聚合的詳細資訊。

3. 按一下“磁碟資訊”標籤。

顯示詳細的磁碟資訊。



僅當選定的聚合正在使用儲存池時才會顯示快取表。

4. 在快取表中，將指標移到所需儲存池的名稱上。

顯示儲存池的詳細資訊。

查看卷冊列表和詳細信息

從「健康狀況：所有捲」視圖中，您可以監控磁碟區的庫存。容量：所有磁碟區視圖使您能夠查看有關叢集中磁碟區的容量和使用率的資訊。

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。

您還可以使用磁碟區/運行狀況詳細資訊頁面查看有關受監控磁碟區的詳細信息，包括磁碟區的容量、效率、配置和保護。您也可以查看有關特定磁碟區的相關設備和相關警報的資訊。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 選擇以下方式之一查看卷宗詳細資料：
 - 要查看有關集群中卷的健康狀況的詳細信息，請在“查看”菜單中選擇“健康狀況：所有捲視圖”。
 - 要查看有關叢集中磁碟區的容量和使用率的詳細信息，請在「檢視」功能表中選擇「容量：所有磁碟區」視圖。
 - 要查看完整詳細信息，請單擊卷名稱。

您也可以透過點擊最小詳細資料對話方塊中的「查看詳細資料」來查看完整的詳細資訊。

3. *可選：*透過點擊最小詳細資料對話方塊中的「檢視相關」來查看與磁碟區相關的物件。

相關資訊

- ["卷：健康詳情頁面"](#)
- ["效能：所有磁碟區視圖"](#)
- ["安全：反勒索軟體視圖"](#)
- ["查看卷宗保護關係"](#)
- ["建立報表以查看可用磁碟區容量圖表"](#)

查看有關 NFS 共享的詳細信息

您可以查看有關所有 NFS 共享的詳細信息，例如其狀態、與磁碟區（FlexGroup磁碟區或FlexVol磁碟區）關聯的路徑、客戶端對 NFS 共用的存取等級以及為匯出的磁碟區定義的匯出策略。使用「運作狀況：所有 NFS 共用」視圖查看所有受監控叢集上的所有 NFS 共用，並使用「儲存虛擬機器/運作狀況詳細資料」頁面查看特定儲存虛擬機器 (SVM) 上

的所有 NFS 共用。

開始之前

- 必須在叢集上啟用 NFS 許可證。
- 必須設定服務於 NFS 共享的網路介面。
- 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，根據您要查看所有 NFS 共用還是僅查看特定 SVM 的 NFS 共用，執行下列步驟。

到...	請依照以下步驟操作...
查看所有 NFS 共享	按一下“儲存”>“NFS 共用”
查看單一 SVM 的 NFS 共享	a. 按一下“儲存”>“儲存虛擬機器” b. 按一下要查看其 NFS 共用詳細資訊的 SVM。 c. 在儲存虛擬機器/運作狀況詳細資料頁面中，按一下 NFS 共用 標籤。

有關詳細信息，請參閱“[設定檔共享卷](#)”和“[使用 API 調配 CIFS 和 NFS 檔案共享](#)”。

查看有關 SMB/CIFS 共享的詳細信息

您可以查看有關所有 SMB/CIFS 共享的詳細信息，例如共享名稱、連接路徑、包含的物件、安全性設定以及為共享定義的匯出策略。使用「運作狀況：所有 SMB 共用」視圖查看所有受監控叢集上的所有 SMB 共用，並使用「儲存虛擬機器/運作狀況詳細資料」頁面查看特定儲存虛擬機器 (SVM) 上的所有 SMB 共用。

開始之前

- 必須在叢集上啟用 CIFS 許可證。
- 必須設定服務於 SMB/CIFS 共享的網路介面。
- 您必須具有操作員、應用程式管理員或儲存管理員角色。



資料夾中的共享不顯示。

步

1. 在左側導覽窗格中，根據您要查看所有 SMB/CIFS 共用還是僅查看特定 SVM 的共用，請執行下列步驟。

到...	請依照以下步驟操作...
查看所有 SMB/CIFS 共享	按一下“儲存”>“SMB 共用”

到...	請依照以下步驟操作...
查看單一 SVM 的 SMB/CIFS 共享	<ol style="list-style-type: none"> 按一下“儲存”>“儲存虛擬機器” 按一下要查看其 SMB/CIFS 共用詳細資訊的 SVM。 在儲存虛擬機器/運作狀況詳細資料頁面中，按一下 SMB 共用 標籤。

有關詳細信息，請參閱 ["使用 API 調配 CIFS 和 NFS 檔案共享"](#)。

查看 Snapshot 副本列表

您可以查看選定磁碟區的 Snapshot 副本清單。您可以使用 Snapshot 副本清單來計算刪除一個或多個 Snapshot 副本後可以回收的磁碟空間量，並且可以根據需要刪除 Snapshot 副本。

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。
- 包含 Snapshot 副本的磁碟區必須處於連線狀態。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「**Health: All Volumes**」檢視中，選擇包含要檢視的 Snapshot 副本的磁碟區。
3. 在*Volume / Health*詳細資訊頁面中，按一下*Capacity*標籤。
4. 在「容量」標籤的「詳細資料」窗格中，在其他詳細資料部分中，按一下「快照副本」旁的連結。

Snapshot 副本數量是一個顯示 Snapshot 副本清單的連結。

相關資訊

["健康/容量頁面"](#)

刪除 Snapshot 副本

您可以刪除 Snapshot 副本以節省空間或釋放磁碟空間，或者如果不再需要 Snapshot 副本，您也可以將其刪除。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

該卷必須處於線上狀態。

要刪除處於繁忙或鎖定狀態的 Snapshot 副本，您必須從正在使用它的應用程式中釋放該 Snapshot 副本。

- 如果FlexClone磁碟區正在使用基線 Snapshot 副本，則您無法刪除父磁碟區中的該 Snapshot 副本。

基本 Snapshot 副本是用於建立FlexClone磁碟區並顯示狀態的 Snapshot 副本 `Busy` 和應用程式依賴關係 `Busy, Vclone` 在父親卷中。

- 您無法刪除SnapMirror關係中使用的鎖定 Snapshot 副本。

Snapshot 副本已被鎖定，下次更新時需要它。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「**Health: All Volumes**」檢視中，選擇包含要檢視的 Snapshot 副本的磁碟區。

將顯示 Snapshot 副本清單。

3. 在*Volume / Health*詳細資訊頁面中，按一下*Capacity*標籤。
4. 在「容量」標籤的「詳細資料」窗格中，在其他詳細資料部分中，按一下「快照副本」旁的連結。

Snapshot 副本數量是一個顯示 Snapshot 副本清單的連結。

5. 在「Snapshot 副本」檢視中，選擇要刪除的 Snapshot 副本，然後按一下「刪除所選」。

計算 Snapshot 副本的可回收空間

您可以計算刪除一個或多個 Snapshot 副本後可以回收的磁碟空間量。

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。
- 該卷必須處於線上狀態。
- 該磁碟區必須是FlexVol volume；FlexGroup磁碟區不支援此功能。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「**Health: All Volumes**」檢視中，選擇包含要檢視的 Snapshot 副本的磁碟區。

將顯示 Snapshot 副本清單。

3. 在*Volume / Health*詳細資訊頁面中，按一下*Capacity*標籤。
4. 在「容量」標籤的「詳細資料」窗格中，在其他詳細資料部分中，按一下「快照副本」旁的連結。

Snapshot 副本數量是一個顯示 Snapshot 副本清單的連結。

5. 在「Snapshot 副本」檢視中，選擇要計算可回收空間的 Snapshot 副本。
6. 點選*計算*。

顯示磁碟區上的可回收空間（以百分比、KB、MB、GB 等為單位）。

7. 若要重新計算可回收空間，請選擇所需的 Snapshot 副本，然後按一下「重新計算」。

集群物件視窗和對話框的描述

您可以從對應的儲存物件頁面查看所有叢集和叢集物件。您也可以從對應的儲存對象詳情頁面查看詳情。現在您可以從 INVENTORY 的以下 STORAGE 和 PROTECTION 部分啟動系統管理器使用者介面。

- 叢集清單、叢集運作狀況和叢集效能頁面
- 匯總庫存、匯總健康狀況和匯總績效頁面
- 磁碟區清單、磁碟區運行狀況和磁碟區效能頁面
- 節點清單和節點效能頁面
- StorageVM 庫存、StorageVM 運作狀況和 StorageVM 效能頁面
- 保護關係頁面

常見的 Unified Manager 運作狀況工作流程與任務

與 Unified Manager 相關的一些常見管理工作流程和任務包括選擇要監控的儲存叢集；診斷對資料可用性、容量和保護產生不利影響的狀況；恢復遺失的資料；配置和管理磁碟區；以及捆綁並傳送診斷資料給技術支援（必要時）。

Unified Manager 讓儲存管理員能夠查看儀表板，評估託管儲存叢集的整體容量、可用性和保護健康狀況，然後快速識別、定位、診斷和分配可能出現的任何特定問題的解決方案。

與叢集、儲存虛擬機器 (SVM)、磁碟區或 FlexGroup 磁碟區相關的最重要的問題會影響託管儲存物件的儲存容量或資料可用性，這些問題顯示在「儀表板」頁面上的系統運作狀況圖表和事件中。當發現嚴重問題時，此頁面會提供連結來支援適當的故障排除工作流程。

Unified Manager 也可以包含在包含相關可管理性工具（例如 OnCommand Workflow Automation (WFA)）的工作流程中，以支援儲存資源的直接設定。

本文檔介紹了與以下管理任務相關的常見工作流程：

- 診斷和管理可用性問題

如果硬體故障或儲存資源配置問題導致儀表板頁面中顯示資料可用性事件，儲存管理員可以按照嵌入的連結查看受影響儲存資源的連線資訊、查看故障排除建議並將問題解決方案指派給其他管理員。

- 配置和監控效能事件

管理員可以監視和管理被監視的儲存系統資源的效能。查看"[Active IQ Unified Manager 效能監控簡介](#)"了解更多。

- 診斷與管理磁碟區容量問題

如果儀表板頁面中顯示卷宗儲存容量問題，儲存管理員可以按照嵌入的連結查看受影響卷的儲存容量相關的當前和歷史趨勢、查看故障排除建議並將問題解決方案指派給其他管理員。

- 配置、監控和診斷保護關係問題

建立和配置保護關係後，儲存管理員可以查看與保護關係相關的潛在問題、保護關係的當前狀態、受影響關係的當前和歷史保護作業成功資訊以及故障排除建議。查看["建立、監控和排除保護關係故障"](#)了解更多。

- 建立備份檔案並從備份檔案還原資料。
- 將儲存物件與註釋關聯

透過將儲存物件與註釋關聯，儲存管理員可以過濾和查看與儲存物件相關的事件，從而使儲存管理員能夠確定與事件相關的問題的優先順序並解決這些問題。

- 使用 REST API 查看 Unified Manager 擷取的運作狀況、容量和效能資訊，從而協助管理叢集。看["Active IQ Unified Manager REST API 入門"](#)了解更多。
- 向技術支援發送支援包

儲存管理員可以使用維護控制台檢索支援包並將其傳送給技術支援。當問題需要比AutoSupport訊息提供的更詳細的診斷和故障排除時，必須將支援包傳送給技術支援。

監控和排除數據可用性故障

Unified Manager 監控授權使用者存取您儲存的資料的可靠性，提醒您封鎖或妨礙存取的情況，並使您能夠診斷這些情況並指派和追蹤其解決方案。

本節中的可用性工作流程主題描述了儲存管理員如何使用 Unified Manager Web UI 來發現、診斷和分配對資料可用性產生不利影響的硬體和軟體條件的解決方案的範例。

掃描並解決儲存故障轉移互連鏈路故障情況


此工作流程提供了一個範例，說明如何掃描、評估和解決故障儲存故障轉移互連連結狀況。在這種情況下，您是管理員，使用 Unified Manager 在節點上啟動ONTAP版本升級之前掃描儲存故障轉移風險。

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。

如果在無中斷升級嘗試期間 HA 對節點之間的儲存故障轉移互連失敗，則升級失敗。因此，通常的做法是管理員在升級開始之前監視並確認要升級的叢集節點上的儲存故障轉移可靠性。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。
2. 在*活動管理*庫存頁面中，選擇*活動可用性事件*。
3. 在「活動管理」庫存頁面「名稱」欄位頂部，點選  並輸入 `*failover` 在文字方塊中限制要顯示的事件為與儲存故障轉移相關的事件。

顯示與儲存故障轉移條件相關的所有過去事件。

在這種情況下，Unified Manager 在其可用性事件部分顯示事件「儲存故障轉移互連一個或多個連結關閉」。

4. 如果「事件管理」清單頁面上顯示與儲存故障轉移相關的一個或多個事件，請執行下列步驟：

- a. 按一下事件標題連結以顯示該事件的事件詳細資訊。

在此範例中，您按一下事件標題「儲存故障轉移互連一個或多個連結關閉」。

將顯示該事件的事件詳細資訊頁面。

- a. 在活動詳細資訊頁面上，您可以執行以下一項或多項任務：
 - 查看原因欄位中的錯誤訊息並評估問題。
 - 將事件分配給管理員。
 - 確認該事件。

相關資訊

["活動詳情頁面"](#)

["Unified Manager 使用者角色和功能"](#)

對儲存故障轉移互連鏈路執行糾正措施

當您顯示與儲存故障轉移相關的事件的事件詳細資訊頁面時，您可以查看該頁面的摘要資訊以確定事件的緊急程度、問題的可能原因以及問題的可能解決方案。

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。

在此範例情境中，事件詳細資訊頁面上提供的事件摘要包含有關儲存故障轉移互連連結故障情況的下列資訊：

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

範例事件資訊表明，HA 對節點 aardvark 和 bonobo 之間的儲存故障轉移互連鏈路 Link1 已關閉，但 Apple 和 Boy 之間的 Link0 處於活動狀態。由於一個連結處於活動狀態，遠端動態記憶體存取 (RDMA) 仍在運行，且儲存故障轉移作業仍可成功。

但是，為了確保連結不會發生故障並且儲存故障轉移保護不會完全停用，您決定進一步診斷 Link1 發生故障的原因。

步驟

1. 在「*事件*詳細資料」頁面中，您可以點擊「來源」欄位中指定的事件的鏈接，以取得可能與儲存故障轉移互連鏈路故障情況相關的其他事件的更多詳細資訊。

在這個例子中，事件的來源是名為 `aardvark` 的節點。點擊該節點名稱會在叢集/健康詳情頁面的節點標籤上顯示受影響的 HA 對 `aardvark` 和 `bonobo` 的 HA 詳情，並顯示受影響的 HA 對上最近發生的其他事件。

2. 查看*HA 詳細資訊*以獲取有關該事件的更多資訊。

在此範例中，相關資訊位於事件表中。此表顯示了「儲存故障轉移連接一個或多個連結斷開」事件、事件產生的時間以及該事件的起源節點。

使用 HA 詳細資訊中的節點位置信息，請求或親自完成受影響的 HA 對節點上的存儲故障轉移問題的物理檢查和修復。

相關資訊

["活動詳情頁面"](#)

["Unified Manager 使用者角色和功能"](#)

解決卷線問題

此工作流程提供了一個範例，說明如何評估和解決 Unified Manager 可能在事件管理庫存頁面中顯示的捲線離線事件。在此場景中，您是使用 Unified Manager 排除一個或多個磁碟區離線事件故障的管理員。

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。

由於多種原因，卷可能會被報告為離線：

- SVM 管理員已故意使磁碟區脫機。
- 該磁碟區的託管叢集節點已關閉，並且到其 HA 對夥伴的儲存故障轉移也失敗了。
- 該磁碟區的託管儲存虛擬機器 (SVM) 已停止，因為託管該 SVM 根磁碟區的節點已關閉。
- 由於兩個 RAID 磁碟同時發生故障，該磁碟區的託管聚合已關閉。

您可以使用活動管理庫存頁面和叢集/運行狀況、儲存虛擬機器/運行狀況和磁碟區/運行狀況詳細資訊頁面來確認或消除其中一種或多種可能性。

步驟

1. 在左側導覽窗格中，按一下「事件管理」。
2. 在*活動管理*庫存頁面中，選擇*活動可用性事件*。
3. 按一下卷離線事件顯示的超文本連結。

將顯示可用性事件的事件詳細資訊頁面。

4. 在該頁面上，檢查註釋，查看是否有任何跡象表明 SVM 管理員已將相關卷離線。
5. 在「*活動*詳細資料」頁面上，您可以查看以下一項或多項任務的資訊：
 - 查看原因欄位中顯示的資訊以取得可能的診斷指導。

在此範例中，「原因」欄位中的資訊僅通知您磁碟區處於離線狀態。

- 檢查「註釋和更新」區域，查看是否有任何跡象表明 SVM 管理員故意將相關卷離線。
- 按一下事件來源（在本例中為報告離線的磁碟區）以取得有關該磁碟區的更多資訊。
- 將事件分配給管理員。
- 確認該事件，或如果適用，將其標記為已解決。

對磁碟區離線情況執行診斷操作

導航至報告離線的卷的卷/健康詳情頁面後，您可以搜尋有助於診斷卷離線狀況的其他資訊。

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。

如果報告脫機的卷不是故意脫機的，則該卷可能由於多種原因而脫機。

從離線磁碟區的磁碟區/執行狀況詳細資料頁面開始，您可以導覽至其他頁面和窗格來確認或消除可能的原因：

- 點擊“卷/運行狀況”詳細信息頁面鏈接，確定卷是否處於離線狀態，因為其主機節點已關閉，並且到其 HA 對夥伴的存儲故障轉移也失敗了。

看“[確定卷離線狀況是否由故障節點引起](#)”。

- 按一下「*磁碟區/運作狀況*詳細資料頁面鏈接，確定磁碟區是否處於離線狀態，以及其主機儲存虛擬機器 (SVM) 是否已停止，因為託管該 SVM 根磁碟區的節點已關閉。

看“[確定磁碟區是否處於離線狀態以及 SVM 是否因節點關閉而停止](#)”。

- 點擊“磁碟區/健康”詳細資料頁面鏈接，確定磁碟區是否由於其主機聚合中的磁碟損壞而處於離線狀態。

看“[確定磁碟區是否因聚合中的磁碟損壞而處於離線狀態](#)”。

相關資訊

["Unified Manager 使用者角色和功能"](#)

確定磁碟區是否由於其主機節點關閉而處於離線狀態



您可以使用 Unified Manager Web UI 來確認或排除磁碟區離線的可能性，因為其主機節點已關閉，並且儲存故障轉移到其 HA 對夥伴失敗。

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。

若要確定磁碟區離線情況是否由託管節點故障和隨後的儲存故障轉移失敗所引起，請執行下列操作：

步驟

1. 找到並點擊離線磁碟區的 **磁碟區/運作狀況** 詳細資料頁面的 **相關裝置** 窗格中 SVM 下顯示的超文本連結。
儲存虛擬機器/運作狀況詳細資訊頁面顯示離線磁碟區的託管儲存虛擬機器 (SVM) 的資訊。
2. 在「儲存虛擬機器/運作狀況」詳細資料頁面的「相關裝置」窗格中，找到並按一下「磁碟區」下顯示的超文本連結。
運行狀況：所有磁碟區視圖顯示有關 SVM 託管的所有磁碟區的資訊表。
3. 在「**Health: All Volumes**」檢視「State」欄位標題上，按一下篩選器符號 ，然後選擇選項*離線*。
僅列出處於離線狀態的 SVM 磁碟區。
4. 在「Health: All Volumes」檢視中，按一下網格符號 ，然後選擇選項*叢集節點*。
您可能需要在網格選擇框中捲動以找到*叢集節點*選項。
叢集節點列被加入到磁碟區清單中，並顯示託管每個離線磁碟區的節點的名稱。
5. 在「**Health: All Volumes**」檢視中，找到離線磁碟區的列表，然後在其「Cluster Node」欄位中按一下其託管節點的名稱。
叢集/健康詳情頁面上的節點標籤顯示託管節點所屬的 HA 節點對的狀態。顯示器上指示了託管節點的狀態和任何叢集故障轉移操作的成功情況。

確認卷線情況存在是因為其主機節點關閉並且儲存故障轉移到 HA 對夥伴節點失敗後，請聯絡對應的管理員或操作員手動重新啟動關閉的節點並修復儲存故障轉移問題。

確定磁碟區是否處於離線狀態且其 **SVM** 是否因節點關閉而停止

您可以使用 Unified Manager Web UI 來確認或排除磁碟區處於離線狀態的可能性，因為託管該 SVM 根磁碟區的節點已關閉，導致其主機儲存虛擬機器 (SVM) 停止。


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。

若要確定捲脫機情況是否因託管該 SVM 根磁碟區的節點關閉而導致其主機 SVM 停止，請執行下列操作：

步驟

1. 找到並點擊離線磁碟區的 **磁碟區/運作狀況** 詳細資料頁面的 **相關裝置** 窗格中 SVM 下方顯示的超文本連結。
儲存虛擬機器/運作狀況詳細資料頁面顯示託管 SVM 的「正在運作」或「已停止」狀態。如果 SVM 狀態為正在執行，則磁碟區離線情況不是由託管該 SVM 根磁碟區的節點關閉所引起的。
2. 如果 SVM 狀態為停止，請按一下「檢視 SVM」以進一步確定託管 SVM 停止的原因。

3. 在「運作狀況：所有儲存虛擬機器」檢視的 SVM 欄位標題上，按一下篩選符號  然後輸入已停止的 SVM 的名稱。

該 SVM 的資訊顯示在表中。

4. 在「運行狀況：所有儲存虛擬機器」視圖中，按一下  然後選擇選項*Root Volume*。

根卷列新增到 SVM 清單中，並顯示已停止的 SVM 的根磁碟區的名稱。

5. 在根卷列中，按一下根磁碟區的名稱以顯示該磁碟區的*儲存虛擬機器/運作狀況*詳細資料頁面。

如果 SVM 根磁碟區的狀態為（連線），則原始磁碟區脫機情況不是由於託管該 SVM 根磁碟區的節點已關閉而導致的。

6. 如果 SVM 根磁碟區的狀態為（離線），則找到並按一下 SVM 根磁碟區的「磁碟區/運作狀況詳細資料」頁面的「相關裝置」窗格中「聚合」下顯示的超文本連結。
7. 找到並點擊聚合的*聚合/健康*詳細資訊頁面的*相關裝置*窗格中節點下顯示的超文本連結。

叢集/運作狀況詳細資料頁面上的節點標籤顯示 SVM 根磁碟區的託管節點所屬的 HA 節點對的狀態。節點的狀態顯示在顯示幕上。

確認磁碟區離線狀態是由該磁碟區的主機 SVM 離線狀態引起的（而主機 SVM 離線狀態本身是由託管該 SVM 根磁碟區的節點關閉所引起的）後，請聯絡對應的管理員或操作員手動重新啟動關閉的節點。

確定磁碟區是否因聚合中的磁碟損壞而處於離線狀態

您可以使用 Unified Manager Web UI 來確認或消除磁碟區離線的可能性，因為 RAID 磁碟問題已導致其主機聚合離線。

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。

若要確定捲脫機情況是否由導致託管聚合離線的 RAID 磁碟問題所引起，請執行下列操作：

步驟

1. 找到並點擊「**Volume / Health**」詳細資訊頁面的「**Related Devices**」窗格中「Aggregate」下顯示的超文本連結。

聚合/健康詳情頁面顯示託管聚合的線上或離線狀態。如果聚合狀態為在線，則 RAID 磁碟問題不是導致磁碟區離線的原因。

2. 如果聚合狀態為離線，則按一下“磁碟資訊”，然後在“磁碟資訊”標籤上的“事件”清單中尋找損壞的磁碟事件。
3. 若要進一步識別損壞的磁碟，請按一下「相關裝置」窗格中「節點」下顯示的超文本連結。

顯示集群/健康詳情頁面。

4. 按一下“磁碟”，然後在“過濾器”窗格中選擇“損壞”以列出所有處於損壞狀態的磁碟。

如果處於損壞狀態的磁碟導致主機聚合處於離線狀態，則該聚合的名稱將顯示在「受影響的聚合」欄位中。

確認卷脫機狀態是由損壞的 RAID 磁碟和隨之而來的主機聚合脫機引起的後，請聯絡相應的管理員或操作員手動更換損壞的磁碟並使聚合重新連線。

解決容量問題

此工作流程提供如何解決容量問題的範例。在這種情況下，您是管理員或操作員，您可以造訪 Unified ManagerDashboard 頁面以查看任何受監控的儲存物件是否有容量問題。您想確定問題的可能原因和解決方案。

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。

在儀表板頁面上，您在事件下拉清單下的容量面板中尋找「磁碟區已滿」錯誤事件。

步驟

1. 在「儀表板」頁面的「容量*」面板中，按一下「磁碟區已滿」錯誤事件的名稱。

將顯示錯誤的事件詳細資訊頁面。

2. 在「活動」詳細資訊頁面中，您可以執行以下一項或多項任務：

- 查看原因欄位中的錯誤訊息，然後按一下建議的補救措施下的建議以查看可能的補救措施的描述。
- 按一下來源欄位中的物件名稱（在本例中為磁碟區）以取得有關該物件的詳細資訊。
- 尋找可能已新增的有關此事件的註釋。
- 為事件新增註釋。
- 將事件分配給另一個使用者。
- 確認該事件。
- 將事件標記為已解決。

相關資訊

["活動詳情頁面"](#)

對整個卷執行建議的補救措施

收到「磁碟區空間已滿」錯誤事件後，您可以查看事件詳細資料頁面上建議的補救措施，並決定執行其中一項建議的操作。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

具有任何角色的使用者都可以執行此工作流程中使用 Unified Manager 的所有任務。

在此範例中，您在 Unified Manager 事件管理庫存頁面上看到了磁碟區空間已滿錯誤事件，並按一下了該事件的名稱。

對於已滿捲，您可以執行的補救措施包括：

- 在磁碟區啟用自動增長、重複資料刪除或壓縮
- 調整捲大小或移動卷
- 從卷中刪除或移動數據

儘管所有這些操作都必須從ONTAP系統管理員或ONTAP CLI 執行，但您可以使用 Unified Manager 來查找可能需要的信息，以確定要採取哪些操作。

步驟

1. 在「事件」詳細資料頁面中，按一下「來源」欄位中的磁碟區名稱即可查看受影響磁碟區的詳細資訊。
2. 在「磁碟區/健康」詳細資料頁面上，按一下「配置」並查看磁碟區上已啟用重複資料刪除和壓縮。

您決定調整磁碟區的大小。

3. 在「相關裝置」窗格中，按一下託管聚合的名稱以查看該聚合是否可以容納更大的磁碟區。
4. 在「*聚合/運作狀況*詳細資料」頁面上，您會看到託管完整磁碟區的聚合確實具有足夠的未提交容量，因此您可以使用ONTAP系統管理員來調整磁碟區的大小，從而為其提供更多容量。

相關資訊

["活動詳情頁面"](#)

管理健康閾值

您可以為所有聚合、磁碟區和 qtree 配置全域健康閾值，以追蹤任何健康閾值違規。

儲存容量健康閾值是什麼

儲存容量健康閾值是 Unified Manager 伺服器產生事件以報告儲存物件的任何容量問題的點。您可以配置警報以便在發生此類事件時發送通知。

所有聚合、磁碟區和 qtree 的儲存容量健康閾值均設定為預設值。您可以根據需要變更一個物件或一組物件的設定。

配置全域健康閾值設置

您可以配置容量、成長、快照預留、配額和 inode 的全域健康閾值條件，以有效監控聚合、磁碟區和 qtree 大小。您也可以編輯產生超過滯後閾值的事件的設定。

全域健康閾值設定適用於與其關聯的所有對象，例如聚合、磁碟區等。當超過閾值時，就會產生一個事件，並且如果配置了警報，則會發送警報通知。閾值預設值設定為建議值，但您可以修改它們以按一定間隔產生事件，以滿足您的特定需求。當閾值發生變化時，事件會在下一個監控週期中產生或淘汰。

可以從左側導覽選單的事件閾值部分存取全域健康閾值設定。您也可以從該物件的庫存頁面或詳細資訊頁面修改單一物件的閾值設定。

- 有關信息，請參閱["配置全域聚合健康閾值"](#)。

您可以為所有聚合配置容量、增長和 Snapshot 副本的運行狀況閾值設置，以追蹤任何閾值違規。

- 有關信息，請參閱["配置全域磁碟區健康閾值"](#)。

您可以編輯所有磁碟區的容量、Snapshot 副本、qtree 配額、磁碟區增長、覆蓋保留空間和 inode 的運行狀況閾值設置，以追蹤任何閾值違規。

- 有關信息，請參閱["配置全域 qtree 運行狀況閾值"](#)。

您可以編輯所有 qtree 的容量健康閾值設置，以追蹤任何閾值違規。

- 有關信息，請參閱["編輯非託管保護關係的滯後健康閾值設置"](#)。

您可以增加或減少警告或錯誤延遲時間百分比，以便以更適合您需求的間隔產生事件。

配置全域聚合健康閾值

您可以為所有聚合配置全域健康閾值，以追蹤任何閾值違規。對於閾值突破，會產生適當的事件，您可以根據這些事件採取預防措施。您可以根據適用於所有受監控聚合的閾值的最佳實踐設定來配置全域值。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您全域配置選項時，物件的預設值將會被修改。但是，如果在物件層級更改了預設值，則不會修改全域值。

閾值選項具有預設值以便更好地監控，但是，您可以更改這些值以滿足您的環境要求。

當在聚合上的磁碟區上啟用自動增長時，聚合容量閾值將被視為已突破，具體取決於自動增長設定的最大磁碟區大小，而不是原始磁碟區大小。



健康閾值不適用於節點的根聚合。

步驟

1. 在左側導覽窗格中，按一下「事件閾值」>「聚合」。
2. 為容量、成長和 Snapshot 副本配置適當的閾值。
3. 點選“儲存”。

相關資訊

["新增用戶"](#)

配置全域磁碟區健康閾值

您可以配置所有磁碟區的全域健康閾值來追蹤任何閾值違規。對於健康閾值違規，會產生適當的事件，您可以根據這些事件採取預防措施。您可以根據適用於所有受監控磁碟區的閾值的最佳實務設定來設定全域值。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

大多數閾值選項都有預設值，以便更好地監控。但是，您可以變更這些值以滿足您的環境要求。

請注意，當在磁碟區上啟用自動增長時，容量閾值將根據自動增長設定的最大磁碟區大小（而不是原始磁碟區大小）被視為已突破。



1000 個 Snapshot 副本的預設值僅適用於 ONTAP 版本為 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本為 9.8 及更高版本的 FlexGroup 卷。對於安裝了舊版 ONTAP 軟體的集群，每個卷的最大 Snapshot 副本數量為 250 個。對於這些舊版本，Unified Manager 將此數字 1000（以及 1000 到 250 之間的任何數字）解釋為 250；這表示當 Snapshot 副本數量達到 250 時，您將繼續接收事件。如果您希望將這些舊版本的閾值設為小於 250，則必須在此處、在「運行狀況：所有磁碟區」視圖中或在「磁碟區/運行狀況詳細資料」頁面中將閾值設為 250 或更低。

步驟

1. 在左側導覽窗格中，按一下「事件閾值」>「音量」。
2. 為容量、Snapshot 副本、qtree 配額、磁碟區增長和 inode 配置適當的閾值。
3. 點選“儲存”。

相關資訊

"新增用戶"

配置全域 qtree 運行狀況閾值

您可以為所有 qtree 配置全域健康閾值，以追蹤任何閾值違規。對於健康閾值違規，會產生適當的事件，您可以根據這些事件採取預防措施。您可以根據適用於所有受監控 qtree 的閾值的最佳實務設定來設定全域值。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

閾值選項具有預設值以便更好地監控，但是，您可以更改這些值以滿足您的環境要求。

只有在 qtree 上設定了 qtree 配額或預設配額時，才會為 qtree 產生事件。如果使用者配額或群組配額中定義的空間超出閾值，則不會產生事件。

步驟

1. 在左側導覽窗格中，按一下「事件閾值」>「Qtree」。
2. 配置適當的容量閾值。
3. 點選“儲存”。

為非託管保護關係配置滯後閾值設定

您可以編輯非託管保護關係的全域預設滯後警告和錯誤健康閾值設置，以便按照適合您需求的間隔產生事件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

滯後時間不得超過定義的傳輸計劃間隔。例如，如果傳輸時間表是每小時一次，那麼滯後時間不得超過一小時。滯後閾值指定滯後時間不得超過的百分比。以一小時為例，如果滯後閾值定義為 150%，那麼當滯後時間超過 1.5 小時時，您將收到事件。

此任務中所述的設定將全域套用至所有非託管保護關係。無法指定這些設定並將其專門應用於一個非託管保護關係。

步驟

1. 在左側導覽窗格中，按一下「事件閾值」>「關係」。
2. 根據需要增加或減少全域預設警告或錯誤滯後時間百分比。
3. 若要停用因任何滯後閾值量而觸發的警告或錯誤事件，請取消選取「已啟用」旁的方塊。
4. 點選“儲存”。

相關資訊

["新增用戶"](#)

編輯單一聚合健康閾值設置

您可以編輯一個或多個聚合的聚合容量、成長和 Snapshot 副本的運作狀況閾值設定。當超過閾值時，就會產生警報並且您會收到通知。這些通知可協助您根據產生的事件採取預防措施。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

根據閾值的變化，事件會在下一個監控週期中產生或淘汰。

當在聚合上的磁碟區上啟用自動增長時，聚合容量閾值將被視為已突破，具體取決於自動增長設定的最大磁碟區大小，而不是原始磁碟區大小。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 在「**Health: All Aggregates**」檢視中，選擇一個或多個聚合，然後按一下「**Edit Thresholds**」。
3. 在「編輯聚合閾值」對話框中，透過選取相應的複選框，然後修改設定來編輯以下之一的閾值設定：容量、成長或 Snapshot 副本。
4. 點選“儲存”。

相關資訊

["新增用戶"](#)

編輯單一卷健康閾值設置

您可以編輯一個或多個磁碟區的磁碟區容量、成長、配額和空間預留的運作狀況閾值設定。當超過閾值時，就會產生警報並且您會收到通知。這些通知可協助您根據產生的事件採取預防措施。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

根據閾值的變化，事件會在下一個監控週期中產生或淘汰。

請注意，當在磁碟區上啟用自動增長時，容量閾值將根據自動增長設定的最大磁碟區大小（而不是原始磁碟區大小）被視為已突破。



1000 個 Snapshot 副本的預設值僅適用於 ONTAP 版本為 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本為 9.8 及更高版本的 FlexGroup 卷。對於安裝了舊版 ONTAP 軟體的集群，每個卷的最大 Snapshot 副本數量為 250 個。對於這些舊版本，Unified Manager 將此數字 1000（以及 1000 到 250 之間的任何數字）解釋為 250；這表示當 Snapshot 副本數量達到 250 時，您將繼續接收事件。如果您希望將這些舊版本的閾值設為小於 250，則必須在此處、在「運行狀況：所有磁碟區」視圖中或在「磁碟區/運行狀況詳細資料」頁面中將閾值設為 250 或更低。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「**Health: All Volumes**」檢視中，選擇一個或多個磁碟區，然後按一下「**Edit Thresholds**」。
3. 在「編輯卷閾值」對話框中，透過選取相應的複選框，然後修改設置，編輯以下之一的閾值設定：容量、Snapshot 副本、qtree 配額、增長或 inode。
4. 點選“儲存”。

相關資訊

"新增用戶"

編輯單一 qtree 運行狀況閾值設定

您可以編輯一個或多個 qtree 的 qtree 容量的運作狀況閾值設定。當超過閾值時，就會產生警報並且您會收到通知。這些通知可協助您根據產生的事件採取預防措施。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

根據閾值的變化，事件會在下一個監控週期中產生或淘汰。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「Qtree」。
2. 在「容量：所有 Qtree」視圖中，選擇一個或多個 qtree，然後按一下「編輯閾值」。
3. 在「編輯 Qtree 閾值」對話方塊中，變更所選 qtree 或 qtree 的容量閾值，然後按一下「儲存」。



您也可以從儲存虛擬機器/運行狀況詳細資料頁面上的 Qtrees 標籤設定單獨的 qtree 閾值。

管理叢集安全目標

Unified Manager 提供了一個儀表板，可根據《NetApp ONTAP 9 安全強化指南》中定義

的建議來確定ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全性。

安全儀表板的目標是顯示ONTAP叢集與NetApp建議指南不一致的任何區域，以便您可以修復這些潛在問題。大多數情況下，您可以使用ONTAP System Manager 或ONTAP CLI 來解決問題。您的組織可能不會遵循所有建議，因此在某些情況下您不需要進行任何更改。

查看 ["NetApp ONTAP 9 安全強化指南"](#) (TR-4569) 以獲取詳細的建議和解決方案。

除了報告安全狀態之外，Unified Manager 還會為任何有安全性違規的叢集或 SVM 產生安全性事件。您可以在事件管理庫存頁面中追蹤這些問題，並且可以為這些事件配置警報，以便在發生新的安全事件時通知您的儲存管理員。

有關詳細信息，請參閱 ["正在評估哪些安全標準"](#)。

正在評估哪些安全標準

一般來說，您的ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全標準將根據《NetApp ONTAP 9 安全強化指南》中定義的建議進行評估。

一些安全檢查包括：

- 叢集是否使用安全性身份驗證方法，例如 SAML
- 對等集群的通訊是否加密
- 儲存虛擬機器是否啟用了稽核日誌
- 您的磁碟區是否啟用了軟體或硬體加密

請參閱合規類別和 ["NetApp ONTAP 9 安全強化指南"](#)了解詳細資訊。



Active IQ平台報告的升級事件也被視為安全事件。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。這些事件不會顯示在安全面板中，但可從事件管理庫存頁面取得。

有關詳細信息，請參閱 ["管理叢集安全目標"](#)。

集群合規性類別

此表描述了 Unified Manager 評估的叢集安全性合規性參數、NetApp建議以及該參數是否影響叢集合規性的整體判定。

叢集上存在不合規的 SVM 將影響叢集的合規性值。因此在某些情況下，您可能需要先修復 SVM 的安全性問題，然後叢集安全性才被視為合規。

請注意，以下列出的每個參數並非都會出現在所有安裝中。例如，如果您沒有對等集群，或者您在集群上停用了AutoSupport，那麼您將不會在 UI 頁面中看到 Cluster Peering 或AutoSupport HTTPS Transport 項目。

範圍	描述	推薦	影響集群合規性
全球 FIPS	指示是否啟用或停用全球 FIPS (聯邦資訊處理標準) 140-2 合規模式。啟用 FIPS 時, TLSv1 和 SSLv3 被停用, 並且只允許使用 TLSv1.1 和 TLSv1.2。	已啟用	是的
遠端登入	指示是否啟用或停用 Telnet 系統存取。NetApp 建議使用安全外殼 (SSH) 進行安全遠端存取。	已停用	是的
不安全的 SSH 設定	指示 SSH 是否使用不安全的密碼, 例如以 *cbc 開頭的密碼。	不	是的
登入橫幅	指示是否對存取系統的使用者啟用或停用登入橫幅。	已啟用	是的
集群對等連接	指示對等集群之間的通訊是否加密或未加密。必須在來源叢集和目標叢集上配置加密, 此參數才被視為合規。	加密	是的
網路時間協定	指示叢集是否已配置一個或多個 NTP 伺服器。為了實現冗餘和最佳服務, NetApp 建議您將至少三個 NTP 伺服器與叢集關聯。	已配置	是的
OCSP	從 9.14.1 開始, Active IQ Unified Manager 在儲存虛擬機器 (SVM, 以前稱為 Vserver) 層級提供線上憑證狀態協定 (OCSP) 狀態資訊。這意味著 OCSP 驗證適用於與 SVM 建立的所有 SSL/TLS 連接, 並確保這些連接中使用的憑證的完整性和有效性。	已啟用	不
遠端審計日誌	指示日誌轉送 (Syslog) 是否加密。	加密	是的

範圍	描述	推薦	影響集群合規性
AutoSupport HTTPS 傳輸	指示是否使用 HTTPS 作為向NetApp支援發送AutoSupport訊息的預設傳輸協定。	已啟用	是的
預設管理員用戶	指示預設管理員使用者（內建）是否啟用或停用。NetApp建議鎖定（停用）任何不必要的內建帳戶。	已停用	是的
SAML 用戶	指示是否配置了 SAML。SAML 可讓您將多重驗證 (MFA) 設定為單一登入的登入方法。	不	不
Active Directory 用戶	指示是否配置了 Active Directory。Active Directory 和 LDAP 是使用者存取叢集的首選驗證機制。	不	不
LDAP 用戶	指示是否配置了 LDAP。對於管理叢集的使用者而非本機使用者來說，Active Directory 和 LDAP 是首選的驗證機制。	不	不
憑證用戶	指示是否配置了憑證使用者來登入叢集。	不	不
本地用戶	指示是否配置本機使用者登入叢集。	不	不
遠端 Shell	指示 RSH 是否啟用。出於安全原因，應停用 RSH。首選使用安全外殼 (SSH) 進行安全遠端存取。	已停用	是的
MD5 使用中	指示ONTAP使用者帳戶是否使用安全性較低的 MD5 雜湊函數。建議將 MD5 Hashed 使用者帳戶遷移到更安全的加密雜湊函數（如 SHA-512）。	不	是的

範圍	描述	推薦	影響集群合規性
證書頒發者類型	指示使用的數位憑證的類型。	CA簽名	不

儲存虛擬機器合規性類別

此表描述了 Unified Manager 評估的儲存虛擬機器 (SVM) 安全性合規性標準、NetApp 建議以及該參數是否會影響 SVM 是否符合規定的整體判斷。

範圍	描述	推薦	影響 SVM 合規性
審計日誌	指示審計日誌記錄是否啟用或停用。	已啟用	是的
不安全的 SSH 設定	指示 SSH 是否使用不安全的密碼，例如以 cbc*。	不	是的
登入橫幅	指示是否為存取系統上的 SVM 的使用者啟用或停用登入橫幅。	已啟用	是的
LDAP 加密	指示 LDAP 加密是否啟用或停用。	已啟用	不
NTLM 身份驗證	指示 NTLM 驗證是否啟用或停用。	已啟用	不
LDAP 有效負載簽名	指示 LDAP 有效負載簽章是否啟用或停用。	已啟用	不
CHAP 設定	指示 CHAP 是啟用還是停用。	已啟用	不
Kerberos V5	指示是否啟用或停用 Kerberos V5 驗證。	已啟用	不
NIS 身份驗證	指示是否配置了使用 NIS 身份驗證。	已停用	不
FPolicy 狀態有效	指示是否創建了 FPolicy。	是的	不
已啟用 SMB 加密	指示是否未啟用 SMB-Signing & Sealing。	是的	不

範圍	描述	推薦	影響 SVM 合規性
已啟用 SMB 簽名	指示是否未啟用 SMB 簽章。	是的	不

容量合規性類別

下表描述了 Unified Manager 評估的捲加密參數，以確定磁碟區上的資料是否受到充分保護，以免被未經授權的使用者存取。



請注意，卷加密參數不會影響叢集或儲存虛擬機器是否被視為合規。

範圍	描述
軟體加密	顯示使用 NetApp 磁碟區加密 (NVE) 或 NetApp 聚合加密 (NAE) 軟體加密解決方案保護的磁碟區的數量。
硬體加密	顯示使用 NetApp 儲存加密 (NSE) 硬體加密保護的捲數。
軟體和硬體加密	顯示受軟體和硬體加密保護的捲的數量。
未加密	顯示未加密的捲數。

不合規意味著什麼

如果根據《NetApp ONTAP 9 安全強化指南》中定義的建議評估的任何安全標準未滿足，則叢集和儲存虛擬機器 (SVM) 被視為不合規。此外，當任何 SVM 被標記為不合規時，該叢集被視為不合規。

安全卡中的狀態圖示與其合規性有以下含義：

-  - 參數配置符合建議要求。
-  - 參數未依建議配置。
-  - 叢集上未啟用此功能，或未依照建議配置該參數，但此參數對物件的合規性沒有貢獻。

請注意，磁碟區加密狀態不會影響叢集或 SVM 是否合規。

查看叢集和儲存虛擬機器的安全狀態

Active IQ Unified Manager 可讓您從介面中的不同點檢視環境中儲存物件的安全狀態。您可以根據定義的參數收集和分析資訊和報告，並偵測受監控叢集和儲存虛擬機器上的可疑行為或未經授權的系統變更。

有關安全建議，請參閱 "[NetApp ONTAP 9 安全強化指南](#)"

在「安全性」頁面上查看物件層級的安全狀態

身為系統管理員，您可以使用「安全性」頁面來了解資料中心和網站層級的ONTAP叢集和儲存虛擬機器的安全強度。支援的物件是叢集、儲存虛擬機器和磁碟區。請依照以下步驟操作：

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 根據您是否要查看所有受監控叢集或單一叢集的安全狀態，選擇「所有叢集」或從下拉式選單中選擇單一叢集。
3. 按一下“安全性”面板中的右箭頭。將顯示“安全”頁面。

點擊條形圖、計數和 `View Reports` 連結將帶您進入磁碟區、叢集或儲存虛擬機器頁面，以便您根據需要查看相應的詳細資訊或產生報告。

安全頁面顯示以下面板：

- 集群合規性：資料中心內所有集群的安全狀態（合規或不合規的集群數量）
- 儲存虛擬機器合規性：資料中心內所有儲存虛擬機器的安全狀態（合規或不合規的儲存虛擬機器數量）
- 磁碟區加密：您環境中所有磁碟區的磁碟區加密狀態（已加密或未加密的磁碟區數）
- 捲反勒索軟體狀態：您環境中所有磁碟區的安全狀態（啟用或停用反勒索軟體的捲數）
- 叢集身分驗證和憑證：使用每種驗證方法的叢集數量，例如 SAML、Active Directory 或透過憑證和本機驗證。此面板還顯示證書已過期或即將在 60 天內過期的群集數量。


在叢集頁面查看所有叢集的安全詳情

透過「叢集/安全」詳細資訊頁面，您可以查看叢集層級的安全合規性狀態。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 選擇“檢視”>“安全性”>“所有叢集”。

顯示預設安全參數，例如全域 FIPS、Telnet、不安全的 SSH 設定、登入橫幅、網路時間協定、AutoSupport HTTPS 傳輸和叢集憑證過期狀態。

您可以點選  更多選項按鈕並選擇在 Unified Manager 的安全 頁面或系統管理員上查看安全性詳細資訊。您應該擁有有效的憑證才能查看系統管理員上的詳細資訊。



如果叢集的憑證已過期，您可以按一下 `expired` 在*叢集憑證有效性*下，並從系統管理員 (9.10.1 及更高版本) 更新它。您無法點擊 `expired` 如果系統管理員實例的版本早於 9.10.1。


從儲存虛擬機器頁面查看所有叢集的安全詳細信息

透過「儲存虛擬機器/安全」詳細資訊頁面，您可以查看儲存虛擬機器層級的安全合規性狀態。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 選擇「檢視」>「安全性」>「所有儲存虛擬機器」。顯示具有安全參數的群集清單。

您可以透過檢查安全性參數（例如儲存虛擬機器、叢集、登入橫幅、稽核日誌和不安全的 SSH 設定）來預設了解儲存虛擬機器的安全性合規性。

您可以點選  更多選項按鈕並選擇在 Unified Manager 的 安全 頁面或系統管理員上查看安全性詳細資訊。您應該擁有有效的憑證才能查看系統管理員上的詳細資訊。

有關捲和存儲虛擬機的反勒索軟體安全詳細信息，請參閱[查看所有磁碟區和儲存虛擬機器的反勒索軟體狀態](#)。

查看可能需要軟體或韌體更新的安全性事件

某些安全事件的影響範圍為「升級」。這些事件由Active IQ平台報告，它們識別需要升級ONTAP軟體、節點韌體或作業系統軟體（用於安全公告）才能解決的問題。

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。您可以查看所有這些事件並將其指派給可以解決問題的使用者。此外，如果您不想收到某些安全升級事件的通知，此清單可以幫助您識別這些事件，以便您可以停用它們。

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（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」功能表中，選擇「升級事件」。

此頁面顯示所有活動的升級安全事件。

查看所有叢集上使用者身份驗證的管理方式

安全性頁面顯示用於對每個叢集上的使用者進行身份驗證的身份驗證類型，以及使用每種類型存取叢集的使用者數量。這使您能夠驗證使用者身份驗證是否按照組織的定義安全地執行。

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 在儀表板頂部，從下拉式選單中選擇“所有集群”。
3. 按一下「安全」面板中的右箭頭，將顯示「安全」頁面。
4. 查看*群集身份驗證*卡片，以了解使用每種驗證類型存取系統的使用者數量。
5. 查看「叢集安全」卡以查看用於對每個叢集上的使用者進行身份驗證的身份驗證機制。

如果某些使用者使用不安全的方法存取系統，或使用NetApp不建議的方法，您可以停用該方法。

查看所有磁碟區的加密狀態

您可以查看所有磁碟區及其目前加密狀態的列表，以便確定磁碟區上的資料是否受到充分

保護，以免被未經授權的使用者存取。

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。

可以應用於卷的加密類型有：

- 軟體 - 使用NetApp磁碟區加密 (NVE) 或NetApp聚合加密 (NAE) 軟體加密解決方案保護的磁碟區。
- 硬體 - 使用NetApp儲存加密 (NSE) 硬體加密保護的磁碟區。
- 軟體和硬體 - 受軟體和硬體加密保護的捲。
- 無 - 未加密的捲。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在“檢視”選單中，選擇“健康”>“卷加密”
3. 在*健康：卷加密*視圖中，按*加密類型*欄位進行排序，或使用篩選器顯示具有特定加密類型或未加密的磁碟區（加密類型為「無」）。

查看所有磁碟區和儲存虛擬機器的反勒索軟體狀態

您可以查看所有磁碟區和儲存虛擬機器 (SVM) 及其目前反勒索軟體狀態的列表，以便確定磁碟區和 SVM 上的資料是否受到充分保護，免受勒索軟體攻擊。

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。

有關不同反勒索軟體狀態的更多信息，請參閱["ONTAP：啟用反勒索軟體"](#)。

查看所有具有反勒索軟體檢測功能的捲的安全詳細信息

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在“檢視”功能表中，選擇“健康”>“安全性”>“反勒索軟體”
3. 在*安全：反勒索軟體*視圖中，您可以按各個欄位進行排序或使用篩選器。



離線磁碟區、受限磁碟區、SnapLock磁碟區、FlexGroup磁碟區、FlexCache磁碟區、僅 SAN 磁碟區、已停止的儲存虛擬機器的磁碟區、儲存虛擬機器的根磁碟區或資料保護磁碟區則不支援反勒索軟體。

查看所有具有反勒索軟體檢測功能的儲存虛擬機器的安全性詳細信息

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 選擇「檢視」>「安全性」>「反勒索軟體」。顯示具有反勒索軟體狀態的 SVM 清單。



未啟用 NAS 協定的儲存虛擬機器不支援反勒索軟體監控。

查看所有活動的安全事件

您可以查看所有活動的安全事件，然後將每個事件指派給可以解決問題的使用者。此外，如果您不想接收某些安全事件，此清單可以幫助您識別要停用的事件。

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「檢視」功能表中，選擇「活動安全事件」。

此頁面顯示過去 7 天內產生的所有新的和已確認的安全事件。

新增安全事件警報

您可以為單一安全事件設定警報，就像 Unified Manager 收到的任何其他事件一樣。此外，如果您想平等對待所有安全事件並將電子郵件發送給同一個人，您可以建立單一警報，在觸發任何安全事件時通知您。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

下面的範例顯示如何為「Telnet 協定已啟用」安全事件建立警報。如果配置了 Telnet 存取以對叢集進行遠端管理訪問，則將發送警報。您可以使用相同的方法為所有安全事件建立警報。

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，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*並選擇要啟用此警報的叢集或叢集。
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*警告*。
 - b. 在符合事件清單中，選擇*Telnet 協定已啟用*。
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，包括通知頻率、發出 SNMP trap 和執行腳本。
8. 點選“儲存”。

禁用特定安全事件

預設情況下，所有事件均啟用。您可以停用特定事件以防止產生那些在您的環境中不重要的事件的通知。如果您想要恢復接收已停用的事件的通知，您可以啟用它們。

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。

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	<ol style="list-style-type: none">a. 按一下“禁用”。b. 在「停用事件」對話方塊中，選擇「警告」嚴重性。這是所有安全事件的類別。c. 在「符合事件」列中，選擇要停用的安全性事件，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	<ol style="list-style-type: none">a. 從已停用事件清單中，選取要重新啟用的一個或多個事件的複選框。b. 按一下“啟用”。

安全事件

安全事件根據《NetApp ONTAP 9 安全性強化指南》中定義的參數，為您提供有關ONTAP叢集、儲存虛擬機器 (SVM) 和磁碟區的安全狀態的資訊。這些事件會通知您潛在的問題，以便您評估其嚴重性並在必要時解決問題。

安全事件按來源類型分組，包括事件和陷阱名稱、影響等級和嚴重性。這些事件出現在叢集和儲存虛擬機器事件類別中。

管理備份和復原作業

您可以建立Active IQ Unified Manager的備份，並在系統發生故障或資料遺失時使用復原功能將備份還原至相同（本機）系統或新的（遠端）系統。

根據安裝 Unified Manager 的作業系統以及所管理的叢集和節點的數量，有三種備份和還原方法：

作業系統	部署規模	推薦的備份方法
VMware vSphere	任何	Unified Manager 虛擬設備的 VMware 快照
紅帽企業 Linux	小的	Unified Manager MySQL 資料庫轉儲
	大的	NetApp Unified Manager 資料庫快照
微軟 Windows	小的	Unified Manager MySQL 資料庫轉儲
	大的	採用 iSCSI 協定的 Unified Manager 資料庫的 NetApp 快照

這些不同的方法將在以下章節中描述。

虛擬設備上 Unified Manager 的備份與還原

當 Unified Manager 安裝在虛擬裝置上時，其備份和復原模型是擷取和還原完整虛擬應用程式的映像。

以下任務可讓您完成虛擬設備的備份：

1. 關閉虛擬機器並拍攝 Unified Manager 虛擬設備的 VMware 快照。
2. 在資料儲存上製作 NetApp Snapshot 副本以擷取 VMware 快照。

如果資料儲存庫未託管在執行 ONTAP 軟體的系統上，請依照儲存供應商指南建立 VMware 快照的備份。

3. 將 NetApp Snapshot 副本或等效快照複製到備用儲存。
4. 移除 VMware 快照。

您應該使用這些任務來實施備份計劃，以確保在出現問題時 Unified Manager 虛擬裝置受到保護。

若要還原虛擬機，您可以使用已建立的 VMware 快照將虛擬機還原至備份時間點狀態。

使用 MySQL 資料庫轉儲進行備份和還原

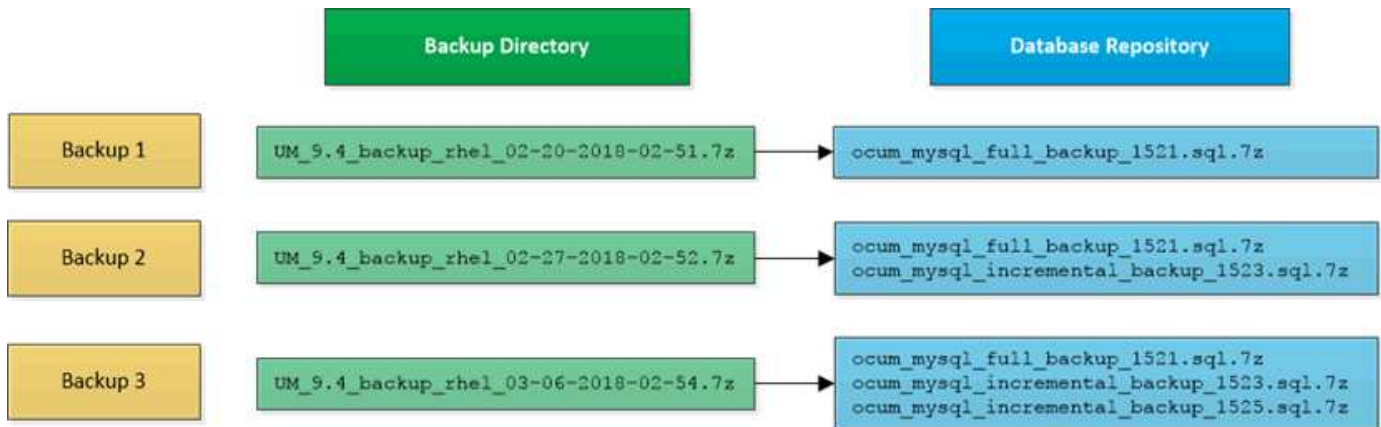
MySQL 資料庫轉儲備份是 Active IQ Unified Manager 資料庫和設定檔的副本，您可以在系統故障或資料遺失時使用它。您可以安排將備份寫入本機目標或遠端目標。強烈建議您定義 Active IQ Unified Manager 主機系統外部的遠端位置。



當 Unified Manager 安裝在 Linux 和 Windows 伺服器上時，MySQL 資料庫轉儲是預設備份機制。但是，如果 Unified Manager 管理大量叢集和節點，或者您的 MySQL 備份需要花費數小時才能完成，則您可以使用 Snapshot 副本進行備份。此功能可在 Red Hat Enterprise Linux 和 Windows 上使用。

資料庫轉儲備份由備份目錄中的單一檔案和資料庫儲存庫目錄中的一個或多個檔案組成。備份目錄中的檔案非常小，因為它僅包含指向重新建立備份所需的資料庫儲存庫目錄中的檔案的指標。

第一次產生資料庫備份時，會在備份目錄中建立一個文件，並在資料庫儲存庫目錄中建立一個完整的備份文件。下次產生備份時，將在備份目錄中建立一個文件，並在資料庫儲存庫目錄中建立一個增量備份文件，其中包含與完整備份文件的差異。當您建立其他備份時，此過程將繼續，直到達到最大保留設置，如下圖所示。



請勿重新命名或刪除這兩個目錄中的任何備份文件，否則任何後續的復原作業都會失敗。

如果您將備份檔案寫入本機系統，則應該啟動一個程序將備份檔案複製到遠端位置，以便在出現需要完全還原的系統問題時可以使用它們。

在開始備份作業之前，Active IQ Unified Manager 會執行完整性檢查，以驗證所有必要的備份檔案和備份目錄是否存在且可寫入。它還檢查系統上是否有足夠的空間來建立備份檔案。

配置資料庫轉儲備份的目標和計劃

您可以設定 Unified Manager 資料庫轉儲備份設定來設定資料庫備份路徑、保留計數和備份計畫。您可以啟用每日或每週的計畫備份。預設情況下，計劃備份是禁用的，但您應該設定備份計劃。

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。
- 您定義為備份路徑的位置必須至少有 150 GB 的可用空間。

建議您使用 Unified Manager 主機系統外部的遠端位置。

- 當 Unified Manager 安裝在 Linux 系統上並使用 MySQL 備份時，請確保在備份目錄上設定下列權限和所有權。

權限：0750，所有權：jboss：maintenance

- 當 Unified Manager 安裝在 Windows 系統上並使用 MySQL 備份時，請確保只有管理員才能存取備份目錄。

由於第一次備份是完整備份，因此第一次備份所需的時間比後續備份要多。完整備份可能超過 1 GB，並且可能需要三到四個小時。後續備份是增量的，需要的時間更少。



- 如果您發現增量備份檔案的數量對於您為備份分配的空間來說太大，您可以定期進行完整備份以替換舊備份及其增量檔案。另一種選擇是，您可以使用 Snapshot 副本進行備份。
- 在新叢集新增後的最初 15 天內進行的備份可能不夠準確，無法取得歷史效能資料。

步驟

1. 在左側導覽窗格中，按一下「常規」>「資料庫備份」。
2. 在*資料庫備份*頁面中，按一下*備份設定*。
3. 為備份路徑、保留計數和計畫配置適當的值。

保留計數的預設值為 10；您可以使用 0 來建立無限備份。

4. 選擇*每日計畫*或*每週計畫*按鈕，然後指定計畫詳細資訊。
5. 按一下“應用”。

資料庫轉儲備份文件是根據計畫建立的。您可以在資料庫備份頁面中看到可用的備份檔案。

什麼是資料庫還原

MySQL 資料庫還原是將現有的 Unified Manager 備份檔案還原到相同或不同的 Unified Manager 伺服器的過程。您可以從 Unified Manager 維護控制台執行復原操作。

如果您在相同（本機）系統上執行還原操作，且備份檔案都儲存在本機，則可以使用預設位置執行還原選項。如果您在不同的 Unified Manager 系統（遠端系統）上執行還原操作，則必須在執行還原選項之前將備份檔案從輔助儲存複製到本機磁碟。

在復原過程中，您將退出 Unified Manager。恢復過程完成後，您可以登入系統。

如果要將備份映像還原到新伺服器，則還原作業完成後，您需要產生新的 HTTPS 安全性憑證並重新啟動 Unified Manager 伺服器。將備份映像還原到新伺服器時，您還需要重新設定 SAML 驗證設定（如果需要）。



Unified Manager 升級到較新版本的軟體後，舊備份檔案無法用於復原映像。為了節省空間，升級 Unified Manager 時會自動刪除除最新檔案之外的所有舊備份檔案。

相關資訊

["產生 HTTPS 安全性憑證"](#)

["啟用 SAML 身份驗證"](#)

["使用 Active Directory 或 OpenLDAP 進行驗證"](#)

如果發生資料遺失或資料損壞，您可以使用復原功能將 Unified Manager 還原到先前的穩定狀態，同時將損失降至最低。您可以使用 Unified Manager 維護控制台將 Unified Manager MySQL 資料庫還原到本機 Windows 系統或遠端 Windows 系統。

開始之前

- 您必須具有 Windows 管理員權限。
- 您必須已將 Unified Manager 備份檔案和資料庫儲存庫目錄的內容複製到將執行復原作業的系統。

建議您將備份檔案複製到預設目錄 `\ProgramData\NetApp\OnCommandAppData\ocum\backup`。資料庫儲存庫檔案必須複製到 `\database_dumps_repo` 下的子目錄 `\backup` 目錄。

- 備份檔案必須是 `.7z` 類型。

恢復功能是特定於平台和特定於版本的。您只能在相同版本的 Unified Manager 上還原 Unified Manager MySQL 備份，並且只能在 Windows 平台上還原 Windows 備份。



如果資料夾名稱包含空格，則必須將備份檔案的絕對路徑或相對路徑括在雙引號中。

步驟

1. 如果您要在新伺服器上執行還原，則安裝 Unified Manager 後，請勿在安裝完成後啟動 UI 或設定任何叢集、使用者或驗證設定。備份檔案在復原過程中填入此資訊。
2. 使用管理員憑證登入 Unified Manager 系統。
3. 以 Windows 管理員身分啟動 PowerShell 或命令提示字元。
4. 輸入命令 ``maintenance_console`` 然後按 Enter 鍵。
5. 在維護控制台*主選單*中，輸入*備份還原*選項的編號。
6. 輸入*還原 MySQL 備份*的號碼。
7. 出現提示時，輸入備份檔案的絕對路徑。

```
Bundle to restore from:  
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac  
kup_windows_02-20-2020-02-51.7z
```

還原操作完成後，您可以登入 Unified Manager。

還原備份後，如果 OnCommand Workflow Automation 伺服器無法運作，請執行下列步驟：

1. 在工作流程自動化伺服器上，將 Unified Manager 伺服器的 IP 位址變更為指向最新的機器。
2. 在 Unified Manager 伺服器上，如果在步驟 1 中取得失敗，請重設資料庫密碼。

使用 NetApp 快照進行備份與還原

NetApp Snapshot 副本會建立 Unified Manager 資料庫和設定檔的時間點映像，您可以在

系統發生故障或資料遺失時使用這些映像進行復原。您可以安排定期將 Snapshot 副本寫入其中一個ONTAP叢集上的捲，以便始終擁有最新副本。



此功能不適用於安裝在虛擬裝置上的Active IQ Unified Manager 。

在 Linux 上設定備份

如果您的Active IQ Unified Manager安裝在 Linux 機器上，那麼您可以決定使用NetApp Snapshots 配置備份和復原。

快照複製所需的時間非常短，通常只需幾分鐘，且 Unified Manager 資料庫的鎖定時間非常短，因此對您的安裝造成的干擾非常小。此影像所佔用的儲存空間極小，且產生的效能開銷可以忽略不計，因為它僅記錄自上次 Snapshot 副本製作以來對檔案的變更。由於快照是在ONTAP叢集上建立的，因此您可以利用其他NetApp功能（例如SnapMirror）來建立二級保護（如果需要）。

在開始備份作業之前，Unified Manager 會執行完整性檢查以驗證目標系統是否可用。

- 您只能在相同版本的Active IQ Unified Manager上還原 Snapshot 副本。



例如，如果您在 Unified Manager 9.16 上建立了備份，則只能在 Unified Manager 9.16 系統上還原該備份。

- 如果快照配置有任何變化，可能會導致快照無效。

配置 Snapshot 副本位置

您可以使用ONTAP系統管理員或ONTAP CLI 來配置在其中一個ONTAP叢集上儲存 Snapshot 副本的磁碟區。

開始之前

叢集、儲存虛擬機器和磁碟區必須符合以下要求：

- 集群要求：
 - 必須安裝ONTAP 9.3 或更高版本
 - 它應該在地理位置上靠近 Unified Manager 伺服器
 - 它可以透過 Unified Manager 進行監控，但這不是必要的
- 儲存虛擬機器需求：
 - 必須設定名稱開關和名稱映射才能使用“檔案”
 - 建立與客戶端用戶對應的本機用戶
 - 確保選擇了“所有讀取/寫入訪問”
 - 確保在匯出策略中將超級使用者存取權限設定為“any”
 - 適用於 Linux 的NetApp快照的 NFS
 - 必須在 NFS 伺服器上啟用 NFSv4，並在用戶端和儲存虛擬機器上指定 NFSv4 ID 網域
 - 該磁碟區的大小至少應為 Unified Manager/opt/netapp/data 目錄的兩倍

使用指令 `du -sh /opt/netapp/data/` 檢查目前大小。

- 音量要求：
 - 該磁碟區的大小至少應為 Unified Manager /opt/netapp/data 目錄的兩倍
 - 安全模式必須設定為 UNIX
 - 必須停用本機快照策略
 - 應啟用磁碟區自動調整功能
 - 效能服務等級應設定為高IOPS、低延遲的策略，例如“Extreme”

有關建立 NFS 磁碟區的詳細步驟，請參閱 ["如何在ONTAP 9 中設定 NFSv4"](#)以及 ["ONTAP 9 NFS 設定快速指南"](#)。

指定 **Snapshot** 副本的目標位置

您應該在已在某個ONTAP叢集中設定的磁碟區上設定Active IQ Unified Manager Snapshot 副本的目標位置。您應該使用維護控制台來定義位置。

- 您必須擁有安裝了Active IQ Unified Manager 的Linux 主機 root 使用者憑證。
- 您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。
- 您必須擁有叢集管理 IP 位址、儲存 VM 的名稱、磁碟區的名稱以及儲存系統使用者名稱和密碼。
- 您必須已將磁碟區掛載至Active IQ Unified Manager主機，且必須具有掛載路徑。

步驟

1. 使用安全外殼連接到Active IQ Unified Manager系統的 IP 位址或 FQDN。
2. 使用維護使用者（umadmin）名稱和密碼登入系統。
3. 輸入命令 ``maintenance_console`` 然後按 Enter 鍵。
4. 在維護控制台*主選單*中，輸入*備份還原*選項的編號。
5. 輸入「配置**NetApp**快照備份」的號碼。
6. 輸入數字來設定 NFS。
7. 查看您需要提供的信息，然後輸入“輸入備份配置詳細信息”的編號。
8. 若要識別將寫入快照的捲，請輸入叢集管理介面的 IP 位址、儲存 VM 的名稱、磁碟區的名稱、LUN 名稱、儲存系統使用者名稱和密碼以及掛載路徑。
9. 驗證此資訊並輸入 `y`。

系統執行以下任務：

- 建立與集群的連接
- 停止所有服務
- 在磁碟區中建立新目錄並複製Active IQ Unified Manager資料庫設定檔
- 從Active IQ Unified Manager中刪除檔案並建立指向新資料庫目錄的符號鏈接
- 重新啟動所有服務

10. 如果您尚未執行此操作，請登出維護控制台並啟動Active IQ Unified Manager介面來為 Snapshot 副本建立計畫。

在 **Windows** 上設定備份

Active IQ Unified Manager支援在 Windows 作業系統上使用使用 iSCSI 協定的 LUN 使用NetApp Snapshots 進行備份和還原。

當所有 Unified Manager 服務都在執行時，可以進行基於快照的備份。由於備份對整個資料庫設定了全域讀取鎖，以防止任何並發寫入，因此資料庫的一致狀態被捕獲為快照的一部分。為了讓安裝在 Windows 作業系統上的 Unified Manager 系統使用NetApp Snapshots 執行備份和恢復，您應該先使用維護控制台將 Unified Manager 備份配置為基於 Snapshot。

在設定 Unified Manager 以建立 Snapshot 副本之前，您應該執行下列設定任務。

- 配置ONTAP集群
- 配置 Windows 主機

配置 **Windows** 的備份位置

在 Windows 上備份 Unified Manager 後，您應該設定用於儲存 Snapshot 副本的磁碟區。

開始之前

叢集、儲存虛擬機器和磁碟區必須符合以下要求：

- 集群要求：
 - 必須安裝ONTAP 9.3 或更高版本
 - 它應該在地理位置上靠近 Unified Manager 伺服器
 - 由 Unified Manager 監控
- 儲存虛擬機器需求：
 - ONTAP叢集上的 iSCSI 連接
 - 必須為配置的機器啟用 iSCSI 協議
 - 您應該有一個專用捲和 LUN 用於備份配置。所選卷應該只包含一個 LUN，而不包含任何其他內容。
 - LUN 的大小應至少為 9.9 Active IQ Unified Manager中預期處理的資料大小的兩倍。

這也對體積提出了相同的尺寸要求。

- 確保選擇了“所有讀取/寫入訪問”
- 確保在匯出策略中將超級使用者存取權限設定為“any”
- 捲和 LUN 要求：
 - 該磁碟區的大小至少應為 Unified Manager MySQL 資料目錄的兩倍。
 - 安全模式必須設定為 Windows
 - 必須停用本機快照策略

- 應啟用磁碟區自動調整功能
- 效能服務等級應設定為高IOPS、低延遲的策略，例如“Extreme”

配置ONTAP集群

在 Windows 系統上使用 Snapshot 副本備份和還原Active IQ Unified Manager之前，您需要在ONTAP叢集上執行一些預先設定步驟。

您可以使用命令提示字元或系統管理員使用者介面設定ONTAP叢集。ONTAP叢集的配置涉及設定資料 LIF，以便可作為 iSCSI LIF 指派給儲存虛擬機器。下一步是使用系統管理器使用者介面配置啟用 iSCSI 的儲存虛擬機器。您需要為此儲存虛擬機器設定靜態網路路由，以控制 LIF 如何使用網路進行出站流量。



您應該有一個專用捲和一個 LUN 用於備份配置。選定的磁碟區應該只包括一個 LUN。LUN 的大小應至少為Active IQ Unified Manager預計處理的資料大小的兩倍。

您需要執行以下配置：

步驟

1. 配置啟用 iSCSI 的儲存虛擬機器或使用具有相同配置的現有儲存虛擬機器。
2. 為已設定的儲存虛擬機器設定網路路由。
3. 配置適當容量的磁碟區和其中的單一 LUN，確保該磁碟區僅專用於此 LUN。



在系統管理員上建立 LUN 的情況下，取消對映 LUN 可能會刪除 igroup，且還原可能會失敗。為避免這種情況，請確保在建立 LUN 時明確建立 LUN，並且在取消對映 LUN 時不會刪除該 LUN。

4. 在儲存虛擬機器中設定啟動器群組。
5. 配置連接埠集。
6. 將 igroup 與連接埠集整合。
7. 將 LUN 對應到 igroup。

配置 Windows 主機

您需要先設定 Windows 主機，然後才能使用NetApp Snapshot 備份和還原Active IQ Unified Manager。若要在 Windows 主機上啟動 Microsoft iSCSI 啟動器，請在搜尋列中輸入“iscsi”，然後按一下 **iSCSI Initiator**。

開始之前

您應該清理主機上的所有先前配置。

如果您嘗試在全新安裝的 Windows 上啟動 iSCSI 啟動器，系統會提示您確認，確認後將顯示「iSCSI 屬性」對話方塊。如果是現有的 Windows 安裝，則會顯示「iSCSI 屬性」對話框，其中的目標處於非活動狀態或正在嘗試連線。因此，您需要確保刪除 Windows 主機上的所有先前配置。

步驟

1. 清理主機上的所有先前配置。

2. 發現目標門戶。
3. 連接到目標門戶。
4. 使用多路徑連接到目標入口網站。
5. 發現這兩個 LIF。
6. 發現在 Windows 機器中配置為裝置的 LUN。
7. 在 Windows 中將發現的 LUN 設定為新的磁碟區磁碟機。

指定 Windows 上 Snapshot 副本的目標位置

您應該在已在某個ONTAP叢集中設定的磁碟區上設定Active IQ Unified Manager Snapshot 副本的目標位置。您應該使用維護控制台來定義位置。

- 您必須擁有安裝了Active IQ Unified Manager 的Windows 主機的管理員權限。
- 您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。
- 您必須擁有叢集管理 IP 位址、儲存 VM 的名稱、磁碟區的名稱、LUN 名稱以及儲存系統使用者名稱和密碼。
- 您必須已將磁碟區作為網路磁碟機掛載至Active IQ Unified Manager主機，並且必須具有掛載磁碟機。

步驟

1. 使用 Power Shell 連接到Active IQ Unified Manager系統的 IP 位址或完全限定網域名稱。
2. 使用維護使用者 (umadmin) 名稱和密碼登入系統。
3. 輸入命令 `maintenance_console` 然後按 Enter 鍵。
4. 在維護控制台*主選單*中，輸入*備份還原*選項的編號。
5. 輸入「配置NetApp快照備份」的號碼。
6. 輸入號碼來配置 iSCSI。
7. 查看您需要提供的信息，然後輸入“輸入備份配置詳細信息”的編號。
8. 若要識別將寫入快照的捲，請輸入叢集管理介面的 IP 位址、儲存 VM 的名稱、磁碟區的名稱、LUN 名稱、儲存系統使用者名稱和密碼以及掛載磁碟機。
9. 驗證此資訊並輸入 y。

系統執行以下任務：

- 儲存虛擬機器已驗證
- 音量已驗證
- 安裝驅動器並驗證狀態
- LUN 存在與狀態
- 網路驅動器存在
- 已驗證安裝磁碟區上是否存在推薦空間（大於 mysql 資料目錄的兩倍）
- 卷中專用 LUN 對應的 LUN 路徑

- igroup 名稱
- 網路磁碟機安裝磁碟區的 GUID
- 用於與ONTAP通訊的 iSCSI 啟動器

10. 退出維護控制台並啟動Active IQ Unified Manager介面來建立 Snapshot 副本的計畫。

從維護控制台設定 **Snapshot** 副本備份

若要使用 Snapshot 副本進行Active IQ Unified Manager備份，您應該從維護控制台執行一些設定步驟。

開始之前

您應該了解系統的以下詳細資訊：

- 叢集 IP 位址
- 儲存 VM 名稱
- 卷名
- LUN 名稱
- 掛載路徑
- 儲存系統憑證

步驟

1. 存取 Unified Manager 的維護控制台。
2. 輸入 4 選擇 備份還原。
3. 輸入 2 選擇 使用**NetApp Snapshot** 備份和還原。



如果要變更備份配置，請輸入 3 選擇 **更新NetApp Snapshot Backup Configuration**。您只能更新密碼。

4. 從選單輸入 1 選擇 配置**NetApp**快照備份。
5. 輸入 1 以提供所需資訊。
6. 提供維護控制台的使用者名稱和密碼，然後確認 LUN 已安裝在主機上。

然後，該程序會驗證您提供的資料目錄、LUN 路徑、儲存 VM、磁碟區、空間可用性、磁碟機等是否正確。在背景進行的操作包括：

- 服務已停止
- 資料庫目錄已移至已安裝的存儲
- 資料庫目錄被刪除，符號連結被建立
- 服務重新啟動在Active IQ Unified Manager介面中完成配置後，備份類型會修改為NetApp Snapshot，並在使用者介面中反映為資料庫備份（基於快照）。

在開始備份作業之前，您必須檢查快照配置是否有任何變化，因為這可能會導致快照無效。假設您在 G 碟中配置了備份並拍攝了快照。您稍後將備份重新配置到 E 盤，並且資料將按照新配置儲存在 E 盤。如果您嘗試還原

在 G 磁碟機中拍攝的快照，則會失敗並出現錯誤「G 磁碟機不存在」。

為 **Linux** 和 **Windows** 定義備份計劃

您可以使用 Unified Manager UI 設定建立 Unified Manager Snapshot 副本的計畫。

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。
- 您必須已從維護控制台配置建立 Snapshot 副本的設置，以確定將建立快照的目標位置。

只需幾分鐘即可建立快照副本，並且 Unified Manager 資料庫僅鎖定幾秒鐘。



在新叢集新增後的最初 15 天內進行的備份可能不夠準確，無法取得歷史效能資料。

步驟

1. 在左側導覽窗格中，按一下「常規」>「資料庫備份」。
2. 在*資料庫備份*頁面中，按一下*備份設定*。
3. 在「保留計數」欄位中輸入要保留的 Snapshot 副本的最大數量。

保留計數的預設值為 10。Snapshot 副本的最大數量由叢集上的 ONTAP 軟體版本決定。無論 ONTAP 版本為何，您都可以將此欄位留空以實現最大值。

4. 選擇*每日計劃*或*每週計劃*按鈕，然後指定計劃詳細資訊。
5. 按一下“應用”。

快照副本是根據計劃建立的。您可以在資料庫備份頁面中看到可用的備份檔案。

由於此磁碟區和快照的重要性，您可能需要為此磁碟區建立一個或兩個警報，以便在以下情況下收到通知：

- 捲空間已滿 90%。使用事件 **Volume Space Full** 來設定警報。

您可以使用 ONTAP System Manager 或 ONTAP CLI 為磁碟區新增容量，以便 Unified Manager 資料庫不會耗盡空間。

- 快照數量已接近最大數量。使用事件 **Too Many Snapshot Copies** 來設定警報。

您可以使用 ONTAP System Manager 或 ONTAP CLI 刪除舊快照，以便始終有空間儲存新的 Snapshot 副本。

您可以在警報設定頁面中配置警報。

使用 **Snapshot** 副本還原 **Unified Manager**

如果發生資料遺失或資料損壞，您可以將 Unified Manager 還原到先前的穩定狀態，同時將資料損失降至最低。您可以使用 Unified Manager 維護控制台將 Unified Manager Snapshot 資料庫還原到本機或遠端作業系統。

開始之前

- 您必須擁有 Linux 主機的 root 使用者憑證以及安裝了 Unified Manager 的 Windows 主機的管理權限。
- 您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。

恢復功能是特定於平台和特定於版本的。您只能在相同版本的 Unified Manager 上還原 Unified Manager 備份。

步驟

1. 連接到 Unified Manager 系統的 IP 位址或完全限定網域名稱。
 - Linux：安全殼
 - Windows：Power Shell
2. 使用 root 使用者憑證登入系統。
3. 輸入命令 `maintenance_console` 然後按 Enter 鍵。
4. 在維護控制台*主選單*中，輸入 4 作為*備份還原*選項。
5. 輸入 2 選擇 使用**NetApp Snapshot** 備份和還原。

如果您要在新伺服器上執行還原，則安裝 Unified Manager 後，請勿在安裝完成後啟動 UI 或設定任何叢集、使用者或驗證設定。輸入 1 選擇 配置**NetApp Snapshot Backup** 並配置 Snapshot 副本的設置，就像它們在原始系統上一樣。

6. 輸入 3 選擇 使用**NetApp Snapshot** 恢復。
7. 選擇要從中還原 Unified Manager 的 Snapshot 副本。按 **Enter**。
8. 復原過程完成後，登入 Unified Manager 使用者介面。

恢復備份後，如果工作流程自動化伺服器無法運作，請執行下列步驟：

1. 在工作流程自動化伺服器上，將 Unified Manager 伺服器的 IP 位址變更為指向最新的機器。
2. 在 Unified Manager 伺服器上，如果在步驟 1 中取得失敗，請重設資料庫密碼。

修改備份類型

如果您想要變更Active IQ Unified Manager系統的備份類型，則可以使用維護控制台選項。取消配置**NetApp**快照備份 選項可讓您還原至基於 MySQL 的備份。

開始之前

您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。

步驟

1. 存取維護控制台。
2. 從*主選單*中選擇 4 進行備份和還原。
3. 從*備份和還原選單*中選擇 2。
4. 選擇 4 表示「取消配置**NetApp**快照備份」。

顯示執行的操作：停止服務、斷開符號連結、將資料從儲存移動到目錄，然後重新啟動服務。

修改備份方式後，備份機制由Snapshot copy改為預設MySQL備份。此變更出現在常規設定的資料庫備份部

分。

Unified Manager 的按需備份

您可以使用Active IQ Unified Manager使用者介面在需要時產生按需備份。按需備份可讓您使用現有的備份方法立即建立備份。按需備份不區分基於 MySQL 或NetApp Snapshot 的備份。

您可以使用資料庫備份頁面上的*立即備份*按鈕執行按需備份。按需備份不依賴您為Active IQ Unified Manager 配置的計畫。

將 Unified Manager 虛擬設備遷移到 Linux 系統

如果您想要變更執行 Unified Manager 的主機作業系統，您可以將 Unified Manager MySQL 資料庫轉儲備份從虛擬裝置還原到 Red Hat Enterprise Linux 系統。

開始之前

- 在虛擬設備上：
 - 您必須具有操作員、應用程式管理員或儲存管理員角色。
 - 您必須知道執行復原作業的 Unified Manager 會維護使用者的名稱。
- 在Linux系統上：
 - 您必須按照[在 Linux 系統上安裝 Unified Manager](#)。
 - 此伺服器上的 Unified Manager 版本必須與您使用備份檔案的虛擬裝置上的版本相同。
 - 安裝後，請勿啟動 UI 或在 Linux 系統上設定任何叢集、使用者或驗證設定。備份檔案在復原過程中填入此資訊。
 - 您必須擁有 Linux 主機的 root 使用者憑證。

這些步驟描述如何在虛擬設備上建立備份文件，將備份文件複製到 Red Hat Enterprise Linux，然後將資料庫備份還原到新系統。

步驟

1. 在虛擬設備上，按一下*管理*>*資料庫備份*。
2. 在*資料庫備份*頁面中，按一下*備份設定*。
3. 將備份路徑變更為/jail/support。
4. 在“計畫”部分中，選擇“每日計畫”，然後輸入比當前時間晚幾分鐘的時間，以便盡快建立備份。
5. 按一下“應用”。
6. 等待幾個小時即可產生備份。

完整備份可能超過 1 GB，並且可能需要三到四個小時才能完成。

7. 以 root 使用者身分登入安裝了 Unified Manager 的 Linux 主機，然後使用 SCP 從虛擬裝置上的 /support 複製備份文件。

```
root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/*
```

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

確保您已複製 .7z 備份檔案和 /database-dumps-repo 子目錄中的所有 .7z 儲存庫檔案。

8. 在命令提示字元下，恢復備份：`um backup restore -f /<backup_file_path>/<backup_file_name>`

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. 復原作業完成後，登入 Unified Manager Web UI。

您應該執行以下任務：

- 產生新的 HTTPS 安全性憑證並重新啟動 Unified Manager 伺服器。
- 將備份路徑變更為 Linux 系統的預設設定（/data/ocum-backup），或變更為您選擇的新路徑，因為 Linux 系統上沒有 /jail/support 路徑。
- 如果正在使用 WFA，請重新配置工作流程自動化連接的兩側。
- 如果您使用 SAML，請重新設定 SAML 驗證設定。

驗證 Linux 系統上的所有內容均如預期運作後，您可以關閉並刪除 Unified Manager 虛擬裝置。

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。

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”。

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。

- 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. 在腳本頁面中，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	<ol style="list-style-type: none">a. 按一下“新增”。b. 在「操作」部分，將警報與您的測試腳本關聯。

到...	這樣做...
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。

管理和監控群組

您可以在 Unified Manager 中建立群組來管理儲存物件。

了解群組

您可以在 Unified Manager 中建立群組來管理儲存物件。了解有關群組的概念以及群組規則如何使您能夠將儲存物件新增至群組將有助於您管理環境中的儲存物件。

什麼是群組

群組是異質儲存物件（叢集、SVM 或磁碟區）的動態集合。您可以在 Unified Manager 中建立群組來輕鬆管理一組儲存物件。群組中的成員可能會發生變化，具體取決於 Unified Manager 在某個時間點監控的儲存物件。

- 每個群組都有一個唯一的名稱。
- 您必須為每個群組配置至少一個群組規則。
- 您可以將一個群組與多個群組規則關聯。
- 每個群組可以包含多種類型的儲存對象，例如叢集、SVM 或磁碟區。
- 根據群組規則的建立時間或 Unified Manager 完成監控週期的時間，儲存物件會動態新增至群組。
- 您可以同時對群組中的所有儲存物件套用操作，例如設定磁碟區的閾值。

群組規則如何適用於群組

群組規則是您定義的標準，用於將儲存物件（磁碟區、叢集或 SVM）納入特定群組。您可以使用條件群組或條件來定義群組的群組規則。

- 您必須將群組規則與群組關聯。
- 您必須為群組規則關聯一個物件類型；一個群組規則只能關聯一種物件類型。
- 在每個監控週期之後或建立、編輯或刪除規則時，都會在群組中新增或刪除儲存物件。
- 一個組規則可以有一個或多個條件組，每個條件組可以有一個或多個條件。
- 根據您建立的群組規則，儲存物件可以屬於多個群組。

狀況

您可以建立多個條件組，每個條件組可以有一個或多個條件。您可以在群組的群組規則中套用所有定義的條件群組，以指定哪些儲存物件包含在群組中。

條件組內的條件使用邏輯「與」來執行。條件組中的所有條件必須滿足。建立或修改群組規則時，將建立一個條件，該條件僅套用、選取和分組符合條件群組中所有條件的儲存物件。當您想要縮小群組中包含的儲存物件的範圍時，您可以在條件群組中使用多個條件。

您可以使用下列運算元和運算子並指定所需的值來建立具有儲存物件的條件。

儲存物件類型	適用操作數
體積	<ul style="list-style-type: none">物件名稱所屬群集名稱所屬 SVM 名稱註解
支援向量機	<ul style="list-style-type: none">物件名稱所屬群集名稱註解
簇	<ul style="list-style-type: none">物件名稱註解

當您選擇註解作為任何儲存物件的運算元時，「Is」運算子可用。對於所有其他運算元，您可以選擇“Is”或“Contains”作為運算符。

- 操作數

Unified Manager 中的操作數清單會根據所選的物件類型而變更。此清單包括物件名稱、所屬叢集名稱、所屬 SVM 名稱以及您在 Unified Manager 中定義的註解。

- 操作員

運算子清單會根據條件所選的操作數而變化。Unified Manager 中支援的運算元是「Is」和「Contains」。

當您選擇「Is」運算子時，將評估條件是否為操作數值與所選運算元提供的值完全相符。

當您選擇「包含」運算子時，將評估條件是否符合下列條件之一：

- 操作數值與所選操作數提供的值完全匹配
- 操作數值包含為所選操作數提供的值

- 價值

值欄位會根據所選的操作數而變化。

帶有條件的群組規則範例

考慮具有以下兩個條件的捲的條件組：

- 名稱包含“vol”
- SVM 名稱稱為“data_svm”

此條件群組選擇名稱中包含「vol」且託管在名為「data_svm」的 SVM 上的所有磁碟區。

條件組

條件組使用邏輯或執行，然後套用於儲存物件。儲存物件必須滿足其中一個條件群組才能被納入某個群組。所有條件組的儲存物件合併在一起。您可以使用條件群組來增加群組中儲存物件的範圍。

具有條件組的組規則範例

考慮一個卷的兩個條件組，每個組包含以下兩個條件：

- 條件組 1
 - 名稱包含“vol”
 - SVM 名稱稱為「data_svm」條件群組 1 選擇名稱中包含「vol」且託管在名為「data_svm」的 SVM 上的所有磁碟區。
- 條件組 2
 - 名稱包含“vol”
 - 資料優先權的註解值為「critical」條件群組 2 選擇名稱中包含「vol」且資料優先權註解值為「critical」的所有磁碟區。

當包含這兩個條件群組的群組規則套用至儲存物件時，下列儲存物件將會新增至選取的群組：

- 名稱中包含「vol」且託管在名為「data_svm」的 SVM 上的所有磁碟區。
- 所有名稱中包含「vol」且資料優先註解值為「critical」的磁碟區。

群組操作如何作用於儲存對象

群組操作是對群組內所有儲存物件執行的操作。例如，您可以設定磁碟區閾值組操作來同時變更群組中所有磁碟區的磁碟區閾值。

群組支援獨特的群組行動類型。一個組只能具有一種卷健康閾值組操作類型。但是，您可以為同一組配置不同類型的群組操作（如果可用）。組操作的等級決定了該操作應用於儲存物件的順序。儲存物件的詳細資訊頁面提供有關對儲存物件套用哪些群組操作的資訊。

獨特的群體行動範例

考慮屬於組 G1 和 G2 的捲 A，並且為這些組配置了以下卷健康閾值組操作：

- `Change_capacity_threshold` 等級為 1 的群組操作，用於配置磁碟區的容量
- `Change_snapshot_copies` 等級為 2 的群組操作，用於設定磁碟區的 Snapshot 副本

這 `Change_capacity_threshold` 集體行動總是優先於 `Change_snapshot_copies` 群組操作並應用於磁碟區 A。
當 Unified Manager 完成一個監控週期後，將根據 `Change_capacity_threshold` 集體行動。您不能為 G1 或 G2 組配置其他容量閾值類型的群組操作。

新增群組

您可以建立群組來組合叢集、磁碟區和儲存虛擬機器 (SVM)，以便於管理。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您可以定義群組規則來新增或刪除群組成員以及修改群組的群組操作。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組」標籤中，按一下「新增」。
3. 在「新增群組」對話方塊中，輸入群組的名稱和描述。
4. 按一下“新增”。

編輯群組

您可以編輯在 Unified Manager 中建立的群組的名稱和描述。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您編輯群組以更新名稱時，必須指定唯一的名稱；不能使用現有的群組名稱。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組」標籤中，選擇要編輯的群組，然後按一下「編輯」。
3. 在「編輯群組」對話方塊中，變更群組的名稱、描述或兩者。
4. 點選“儲存”。

刪除群組

當不再需要某個群組時，您可以從 Unified Manager 中刪除該群組。

開始之前

- 任何儲存物件（叢集、SVM 或磁碟區）都不能與要刪除的群組關聯的任何群組規則關聯。
- 您必須具有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「儲存管理」>「群組」。
2. 在「群組」標籤中，選擇要刪除的群組，然後按一下「刪除」。

3. 在「警告」對話方塊中，按一下「是」確認刪除。

刪除群組並不會刪除與該群組關聯的群組操作。但是，刪除群組後，這些群組操作將取消映射。

新增群組規則

您可以為群組建立群組規則，以便將儲存物件（例如磁碟區、叢集或儲存虛擬機器 (SVM)）動態新增至該群組。您必須配置至少一個包含至少一個條件的條件群組才能建立群組規則。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

一旦建立群組規則，就會新增目前監控的儲存物件。僅在監控週期完成後才會新增物件。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組規則」標籤中，按一下「新增」。
3. 在「新增群組規則」對話方塊中，指定群組規則的名稱。
4. 在*目標物件類型*欄位中，選擇要分組的儲存物件的類型。
5. 在*組*欄位中，選擇要為其建立組規則的組。
6. 在「條件」部分中，執行下列步驟來建立條件、條件群組或兩者：

創造....	這樣做...
一個條件	<ol style="list-style-type: none">a. 從操作數清單中選擇一個操作數。b. 選擇 Contains 或 Is 作為運算子。c. 輸入一個值，或從可用清單中選擇一個值。
條件組	<ol style="list-style-type: none">a. 按一下“新增條件組”b. 從操作數清單中選擇一個操作數。c. 選擇 Contains 或 Is 作為運算子。d. 輸入一個值，或從可用清單中選擇一個值。e. 如果需要，請按一下「新增條件」以建立更多條件，並對每個條件重複步驟 a 到 d。

7. 按一下“新增”。

建立組規則的範例

在「新增群組規則」對話方塊中，執行下列步驟建立群組規則，包括設定條件和新增條件群組：

步驟

1. 指定組規則的名稱。
2. 選擇物件類型作為儲存虛擬機器 (SVM)。
3. 從群組清單中選擇一個群組。
4. 在條件部分中，選擇*物件名稱*作為操作數。
5. 選擇 **Contains** 作為運算子。
6. 輸入值 `svm_data`。
7. 按一下*新增條件*。
8. 選擇*物件名稱*作為操作數。
9. 選擇 **Contains** 作為運算子。
10. 輸入值 `vol`。
11. 點選*新增條件*。
12. 重複步驟 8 到 10，步驟 8 選擇 **data-priority** 作為運算元，步驟 9 選擇 **Is** 作為運算符，步驟 10 中選擇 **critical** 作為值。
13. 按一下「新增」為群組規則建立條件。

編輯群組規則

您可以編輯群組規則來修改條件群組和條件群組內的條件，以便向特定群組新增或從特定群組中刪除儲存物件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組規則」標籤中，選擇要編輯的群組規則，然後按一下「編輯」。
3. 在*編輯群組規則*對話方塊中，根據需要變更群組規則名稱、關聯群組名稱、條件群組和條件。



您不能變更群組規則的目標物件類型。

4. 點選“儲存”。

刪除群組規則

當不再需要群組規則時，您可以從Active IQ Unified Manager中刪除該群組規則。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當刪除群組規則時，關聯的儲存物件將從群組中刪除。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組規則」標籤中，選擇要刪除的群組規則，然後按一下「刪除」。
3. 在「警告」對話方塊中，按一下「是」確認刪除。

新增群組操作

您可以設定要套用於群組中儲存物件的群組操作。為群組配置操作可以節省您的時間，因為您不必將這些操作單獨新增至每個物件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組動作」標籤中，按一下「新增」。
3. 在「新增群組操作」對話方塊中，輸入操作的名稱和描述。
4. 從*Group*選單中，選擇您想要設定操作的群組。
5. 從*操作類型*選單中，選擇一種操作類型。

對話方塊展開，使您能夠使用所需參數配置所選的操作類型。

6. 輸入所需參數的適當值來配置群組操作。
7. 按一下“新增”。

編輯組操作

您可以編輯在 Unified Manager 中設定的群組操作參數，例如群組操作名稱、描述、關聯群組名稱和操作類型的參數。

開始之前

您必須具有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「儲存管理」>「群組」。
2. 在「群組操作」標籤中，選擇要編輯的群組操作，然後按一下「編輯」。
3. 在「編輯群組操作」對話方塊中，根據需要變更群組操作名稱、描述、關聯群組名稱和操作類型的參數。
4. 點選“儲存”。

為組配置卷健康閾值

您可以為容量、Snapshot 副本、qtree 配額、增長和 inode 配置組級卷健康閾值。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

磁碟區健康閾值類型的群組操作僅適用於群組的磁碟區。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組動作」標籤中，按一下「新增」。
3. 輸入組操作的名稱和描述。
4. 從*群組*下拉方塊中，選擇要配置群組操作的群組。
5. 選擇*操作類型*作為磁碟區健康閾值。
6. 選擇要設定閾值的類別。
7. 輸入健康閾值所需的值。
8. 按一下“新增”。

刪除群組操作

當不再需要群組操作時，您可以從 Unified Manager 中刪除該群組操作。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您刪除磁碟區運行狀況閾值的群組操作時，全域閾值將套用至該群組中的儲存物件。在儲存物件上設定的任何物件級健康閾值都不會受到影響。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組操作」標籤中，選擇要刪除的群組操作，然後按一下「刪除」。
3. 在「警告」對話方塊中，按一下「是」確認刪除。

重新排序組操作

您可以變更套用於群組中儲存物件的群組操作的順序。群組操作根據儲存物件的等級依序套用於儲存物件。最低等級分配給您最後配置的群組操作。您可以根據需要更改團體行動的等級。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您可以選擇單行或多行，然後執行多次拖曳操作以變更群組操作的排名。但是，您必須儲存更改，以便重新排序能夠反映在群組操作網格中。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「群組」。
2. 在「群組操作」標籤中，按一下「重新排序」。
3. 在「重新排序組操作」對話方塊中，拖放行以根據需要重新排列群組操作的順序。

4. 點選“儲存”。

使用註釋確定儲存物件事件的優先權

您可以建立註釋規則並將其應用於儲存對象，以便您可以根據所應用的註釋類型及其優先順序來識別和篩選這些對象。

了解有關註釋的更多信息

了解有關註釋的概念有助於您管理與環境中的儲存物件相關的事件。

什麼是註釋

註釋是分配給另一個文字字串（值）的文字字串（名稱）。每個註解名稱-值對可以使用註解規則動態地與儲存物件關聯。當您將儲存物件與預先定義註解關聯時，您可以篩選和查看與它們相關的事件。您可以將註解套用至叢集、磁碟區和儲存虛擬機器 (SVM)。

每個註釋名稱可以有幾個值；每個名稱-值對都可以透過規則與一個儲存物件相關聯。

例如，您可以建立一個名為“data-center”的註釋，其值為“Boston”和“Canada”。然後，您可以將註解「data-center」和值「Boston」套用到磁碟區 v1。當針對標有“data-center”的磁碟區 v1 上的任何事件產生警報時，產生的電子郵件會指示卷的位置“Boston”，這使您能夠確定問題的優先順序並解決問題。

Unified Manager 中的註解規則如何運作

註釋規則是您定義的用於註釋儲存物件（磁碟區、叢集或儲存虛擬機器 (SVM)）的標準。您可以使用條件群組或條件來定義註解規則。

- 您必須將註釋規則與註釋關聯起來。
- 您必須為註解規則關聯一個物件類型；一個註解規則只能關聯一種物件類型。
- Unified Manager 在每個監控週期之後或在建立、編輯、刪除或重新排序規則時從儲存物件中新增或刪除註解。
- 一個註解規則可以有一個或多個條件組，每個條件組可以有一個或多個條件。
- 儲存物件可以有幾個註釋。針對特定註釋的註解規則也可以使用規則條件中的不同註釋來為已註釋的物件新增另一個註釋。

狀況

您可以建立多個條件組，每個條件組可以有一個或多個條件。您可以在註釋的註解規則中套用所有定義的條件群組，以便註釋儲存物件。

條件組內的條件使用邏輯「與」來執行。條件組中的所有條件必須滿足。當您建立或修改註解規則時，會建立一個條件，該條件僅套用、選取和註解那些符合條件群組中所有條件的儲存物件。當您想要縮小要註解的儲存物件的範圍時，您可以在條件群組中使用多個條件。

您可以使用下列運算元和運算子並指定所需的值來建立具有儲存物件的條件。

儲存物件類型	適用操作數
體積	<ul style="list-style-type: none"> 物件名稱 所屬群集名稱 所屬 SVM 名稱 註解
支援向量機	<ul style="list-style-type: none"> 物件名稱 所屬群集名稱 註解
簇	<ul style="list-style-type: none"> 物件名稱 註解

當您選擇註解作為任何儲存物件的運算元時，「Is」運算子可用。對於所有其他運算元，您可以選擇“Is”或“Contains”作為運算符。當您選擇「Is」運算子時，將評估條件是否為操作數值與所選運算元提供的值完全相符。當您選擇「包含」運算子時，將評估條件是否符合下列條件之一：

- 操作數值與所選操作數的值完全相符。
- 操作數值包含為所選操作數提供的值。

帶有條件的註解規則範例

考慮具有一個條件組的註釋規則，該規則針對具有以下兩個條件的捲：

- 名稱包含“vol”
- SVM 名稱稱為“data_svm”

此註解規則使用選定的註解和註解類型對名稱中包含「vol」且託管在名為「data_svm」的 SVM 上的所有磁碟區進行註解。

條件組

條件組使用邏輯或執行，然後套用於儲存物件。儲存物件必須滿足要註釋的其中一個條件群組的要求。對滿足所有條件組條件的儲存物件進行註釋。您可以使用條件群組來增加要註解的儲存物件的範圍。

帶有條件組的註釋規則範例

考慮一個具有兩個卷條件組的註釋規則；每個組包含以下兩個條件：

- 條件組 1
 - 名稱包含“vol”
 - SVM 名稱稱為「data_svm」此條件群組註解名稱中包含「vol」且託管在名為「data_svm」的 SVM 上的所有磁碟區。

- 條件組 2
 - 名稱包含“vol”
 - 資料優先權的註解值為「critical」 此條件群組將名稱中包含「vol」且資料優先權註解值為「critical」的所有磁碟區進行註解。

當包含這兩個條件組的註解規則套用至儲存物件時，則會註解以下儲存物件：

- 名稱中包含「vol」且託管在 SVM 上且名為「data_svm」的所有磁碟區。
- 所有名稱中包含「vol」且資料優先註解值為「critical」的磁碟區。

預定義註釋值的描述

資料優先權 是一個預定義註釋，其值為任務關鍵、高和低。這些值使您能夠根據儲存物件所包含的資料的優先順序對其進行註釋。您不能編輯或刪除預先定義的註釋值。

- 資料優先：任務關鍵

此註釋適用於包含關鍵任務資料的儲存物件。例如，包含生產應用程式的物件可以被視為任務關鍵型。

- 資料優先：高

此註釋適用於包含高優先權資料的儲存物件。例如，承載業務應用程式的物件可以被視為高優先級。

- 資料優先：低

此註釋適用於包含低優先級資料的儲存物件。例如，位於二級儲存上的物件（如備份和鏡像目標）可能優先順序較低。

動態新增註釋

建立自訂註解時，Unified Manager 會使用規則將叢集、儲存虛擬機器 (SVM) 和磁碟區與註解動態關聯。這些規則會自動將註解指派給儲存物件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在*註釋*頁面中，按一下*新增註解*。
3. 在「新增註解」對話方塊中，鍵入註解的名稱和描述。
4. 可選：在*註釋值*部分中，按一下*新增*以向註釋新增值。
5. 點選“儲存”。

為註釋添加值

您可以為註解新增值，然後將儲存物件與特定的註解名稱-值對關聯。在註釋中新增值可以

幫助您更有效地管理儲存物件。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您不能為預定義註解新增值。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註釋」頁面中，選擇要新增值的註釋，然後按一下「值」部分中的「新增」。
3. 在「新增註釋值」對話方塊中，指定註釋的值。

您指定的值對於選定的註釋必須是唯一的。

4. 按一下“新增”。

刪除註釋

當不再需要自訂註釋及其值時，您可以刪除它們。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 註釋值不得在其他註釋或群組規則中使用。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註釋」標籤中，選擇要刪除的註釋。

顯示所選註釋的詳細資訊。

3. 按一下「動作」>「刪除」以刪除選取的註解及其值。
4. 在警告對話方塊中，按一下「是」確認刪除。

查看註釋列表和詳細信息

您可以查看與叢集、磁碟區和儲存虛擬機器 (SVM) 動態關聯的註釋清單。您還可以查看註釋的詳細信息，例如描述、創建者、建立日期、值、規則以及與註釋相關的物件。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註釋」標籤中，按一下註釋名稱以查看相關詳細資訊。

從註釋中刪除值

當與自訂註解關聯的值不再適用於該註解時，您可以刪除該值。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 註釋值不得與任何註釋規則或群組規則相關聯。

您無法從預定義註解中刪除值。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註釋」標籤的註解清單中，選擇要從中刪除值的註解。
3. 在「註釋」標籤的「值」區域中，選擇要刪除的值，然後按一下「刪除」。
4. 在「警告」對話方塊中，按一下「是」。

該值已被刪除，並且不再顯示在所選註釋的值清單中。

建立註解規則

您可以建立註解規則，Unified Manager 可以使用該規則動態註解儲存對象，例如磁碟區、叢集或儲存虛擬機器 (SVM)。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

一旦建立註釋規則，就會對目前監控的儲存物件進行註釋。僅在監控週期完成後才會對新物件進行註解。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註解規則」標籤中，按一下「新增」。
3. 在「新增註解規則」對話方塊中，指定註解規則的名稱。
4. 在*目標物件類型*欄位中，選擇要註解的儲存物件的類型。
5. 在*應用註解*欄位中，選擇要使用的註解和註解值。
6. 在「條件」部分中，執行適當的操作來建立條件、條件群組或兩者：

創建...	這樣做...
一個條件	<ol style="list-style-type: none">a. 從操作數清單中選擇一個操作數。b. 選擇 Contains 或 Is 作為運算子。c. 輸入一個值，或從可用清單中選擇一個值。

創建...	這樣做...
條件組	<ol style="list-style-type: none"> 按一下“新增條件組”。 從操作數清單中選擇一個操作數。 選擇 Contains 或 Is 作為運算子。 輸入一個值，或從可用清單中選擇一個值。 如果需要，請按一下「新增條件」以建立更多條件，並對每個條件重複步驟 a 到 d。

7. 按一下“新增”。

建立註解規則的範例

在「新增註解規則」對話方塊中執行下列步驟來建立註解規則，包括設定條件和新增條件群組：

步驟

- 指定註解規則的名稱。
- 選擇目標物件類型為儲存虛擬機器 (SVM)。
- 從註釋清單中選擇一個註釋，並指定一個值。
- 在條件部分中，選擇*物件名稱*作為操作數。
- 選擇 **Contains** 作為運算子。
- 輸入值 `svm_data`。
- 按一下*新增條件組*。
- 選擇*物件名稱*作為操作數。
- 選擇 **Contains** 作為運算子。
- 輸入值 `vol`。
- 點選*新增條件*。
- 重複步驟 8 到 10，在步驟 8 中選擇 **data-priority** 作為操作數，在步驟 9 中選擇 **Is** 作為運算符，在步驟 10 中選擇 **mission-critical** 作為值。
- 按一下“新增”。

手動為個別儲存物件新增註釋

您可以手動註解選定的磁碟區、叢集和 SVM，而無需使用註解規則。您可以註釋單一儲存對象或多個儲存對象，並為註釋指定所需的名稱-值對組合。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

- 導航至要註釋的儲存物件：

若要新增註釋...	這樣做...
叢集	a. 按一下「儲存」>「叢集」。 b. 選擇一個或多個集群。
卷	a. 按一下「儲存」>「卷」。 b. 選擇一個或多個磁碟區。
支援向量機	a. 按一下“儲存”>“SVM”。 b. 選擇一個或多個 SVM。

2. 點擊“註釋”並選擇一個名稱-值對。
3. 按一下“應用”。

編輯註釋規則

您可以編輯註解規則來修改條件群組和條件群組內的條件，從而向儲存物件新增註解或從儲存物件中刪除註解。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您編輯相關的註釋規則時，註釋將與儲存物件解除關聯。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註解規則」標籤中，選擇要編輯的註解規則，然後按一下「動作」>「編輯」。
3. 在*編輯註解規則*對話方塊中，根據需要變更規則名稱、註解名稱和值、條件群組和條件。

您不能變更註解規則的目標物件類型。

4. 點選“儲存”。

配置註解規則的條件

您可以設定一個或多個條件來建立 Unified Manager 套用於儲存物件的註解規則。滿足註釋規則的儲存物件將被註釋為規則中指定的值。

開始之前

您必須具有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「儲存管理」>「註解」。
2. 在「註解規則」標籤中，按一下「新增」。

3. 在「新增註解規則」對話方塊中，輸入規則的名稱。
4. 從目標物件類型清單中選擇一種物件類型，然後從清單中選擇註解名稱和值。
5. 在對話方塊的「條件」部分中，從清單中選擇一個操作數和一個運算符，然後輸入條件值，或按一下「新增條件」來建立新條件。
6. 點擊“儲存並新增”。

配置註解規則條件的範例

考慮物件類型 SVM 的條件，其中物件名稱包含“svm_data”。

在「新增註解規則」對話方塊中執行下列步驟來設定條件：

步驟

1. 輸入註解規則的名稱。
2. 選擇目標物件類型為SVM。
3. 從註釋清單中選擇一個註釋和一個值。
4. 在*條件*欄位中，選擇*物件名稱*作為操作數。
5. 選擇 **Contains** 作為運算子。
6. 輸入值 svm_data。
7. 按一下“新增”。

刪除註解規則

當不再需要註解規則時，您可以從Active IQ Unified Manager中刪除這些規則。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

當您刪除註釋規則時，註釋將取消關聯並從儲存物件中刪除。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註解規則」標籤中，選擇要刪除的註解規則，然後按一下「刪除」。
3. 在「警告」對話方塊中，按一下「是」確認刪除。

重新排序註釋規則

您可以變更 Unified Manager 將註解規則套用到儲存物件的順序。註釋規則根據儲存物件的等級依序應用於儲存物件。配置註解規則時，排序最小。但是您可以根據需要更改註釋規則的等級。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您可以選擇單行或多行並執行多次拖放操作來變更註解規則的等級。但是，您必須儲存更改，以便重新排序顯示在「註釋規則」標籤中。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「註解」。
2. 在「註解規則」標籤中，按一下「重新排序」。
3. 在*重新排序註解規則*對話方塊中，拖放單行或多行以重新排列註解規則的順序。
4. 點選“儲存”。

您必須儲存變更才能顯示重新排序。

透過 Web UI 和維護控制台發送支援包

當您遇到的問題需要比AutoSupport訊息提供的更詳細的診斷和故障排除時，您應該發送支援包。您可以使用 Unified Manager Web Ui 和維護控制台將支援包傳送給技術支援。

Unified Manager 一次最多可儲存兩個完整支援包和三個輕量支援包。

相關資訊

["Unified Manager 使用者角色和功能"](#)

將**AutoSupport**訊息和支援包發送給技術支持

AutoSupport頁面可讓您向技術支援團隊發送預先定義和按需的AutoSupport訊息，以確保您的環境正常運行，並協助您維護環境的完整性。AutoSupport預設處於啟用狀態，您不應停用它，以便您獲得 NetAppActive IQ 的優勢。

您可以根據需要在訊息中傳送有關 Unified Manager 伺服器的診斷系統資訊和詳細數據，安排定期傳送訊息，甚至產生並傳送支援包給技術支援團隊。



具有儲存管理員角色的使用者可以產生並發送按需AutoSupport訊息和支援包給技術支援。但是，只有管理員或維護使用者可以啟用或停用定期AutoSupport並配置 HTTP 設置，如設定 HTTP 代理伺服器部分中所述。在需要使用 HTTP 代理伺服器的環境中，應先完成配置，然後儲存管理員才能向技術支援發送按需AutoSupport訊息和支援包。

發送按需AutoSupport訊息

您可以產生並發送按需訊息給技術支援人員，或發送給指定的電子郵件收件人，或同時發送給兩者。

步驟

1. 導覽至 常規 > **AutoSupport**，然後執行以下操作之一或全部兩個：
2. 如果您想將AutoSupport訊息傳送給技術支持，請選取 傳送至技術支援 複選框。
3. 如果要將AutoSupport訊息傳送給特定的電子郵件收件人，請選取「傳送給電子郵件收件人」複選框，然後輸入收件人的電子郵件地址。
4. 點選“儲存”。

5. 點擊“生成並發送AutoSupport”。

啟用定期AutoSupport

您可以定期向技術支援發送特定的預定義訊息，以進行問題診斷和解決。此功能預設為啟用。如果停用，管理員或維護使用者可以啟用該設定。

步驟

1. 導覽至 常規 > **AutoSupport**。
2. 在定期AutoSupport部分中，選取*啟用定期向Active IQ發送AutoSupport資料*複選框。
3. 如果需要，請依照設定 HTTP 代理伺服器部分中的說明定義 HTTP 代理伺服器的名稱、連接埠和驗證資訊。
4. 點選“儲存”。

上傳按需支援包

您可以根據故障排除要求產生支援包並將其發送給技術支援。Unified Manager 僅儲存最近產生的兩個支援包。較舊的支援包已從系統中刪除。

由於某些類型的支援資料可能會使用大量叢集資源或需要很長時間才能完成，因此當您選擇完整支援包時，您可以包含或排除特定資料類型以減少支援包的大小。您也可以選擇建立一個輕量級支援包，其中僅包含 30 天的日誌和設定資料庫記錄 - 它不包括效能資料、擷取記錄檔和伺服器堆轉儲。

步驟

1. 導覽至 常規 > **AutoSupport**。
2. 在按需支援包部分，按一下*產生並傳送支援包*。
3. 若要向技術支援發送輕量支援包，請在產生並傳送支援包彈出視窗中選取產生輕量支援包複選框。
4. 或者，要傳送完整的支援包，請選取「產生完整的支援包」複選框。選擇要在支援包中包含或排除的特定資料類型。



即使您未選擇任何資料類型，支援包仍會與其他 Unified Manager 資料一起產生。

5. 選取*將捆綁包傳送給技術支援*複選框以產生捆綁包並將其傳送給技術支援。如果您未選取此複選框，則會在 Unified Manager 伺服器本機產生並儲存捆綁包。產生的支援包可供日後在 VMware 系統的 /support 目錄中使用，`/opt/netapp/data/support/` 在 Linux 系統上，`ProgramData\NetApp\OnCommandAppData\ocum\support` 在 Windows 系統上。
6. 按一下“發送”。

設定 HTTP 代理伺服器

如果您的環境不提供從 Unified Manager 伺服器的直接訪問，您可以指定代理來提供互聯網訪問，以便將AutoSupport內容傳送给支援人員。此部分僅供管理員和維護使用者使用。

• 使用 HTTP 代理

勾選此方塊可識別用作 HTTP 代理的伺服器。

輸入代理伺服器的主機名稱或 IP 位址，以及用於連接伺服器的連接埠號碼。

- 使用身份驗證

如果需要提供身份驗證資訊來存取用作 HTTP 代理的伺服器，請選取此方塊。

輸入透過 HTTP 代理進行身份驗證所需的使用者名稱和密碼。



不支援僅提供基本驗證的 HTTP 代理。

存取維護控制台

如果 Unified Manager 使用者介面未執行，或者您需要執行使用者介面中不可用的功能，則可以存取維護控制台來管理 Unified Manager 系統。

開始之前

您必須已安裝並設定 Unified Manager。

15 分鐘不活動後，維護控制台將註銷您。



在 VMware 上安裝時，如果您已經透過 VMware 控制台以維護使用者身分登錄，則無法同時使用安全外殼登入。

步

1. 請依照下列步驟存取維護控制台：

在此作業系統上...	請依照以下步驟操作...
VMware	<ol style="list-style-type: none"> a. 使用安全性外殼連接到 Unified Manager 虛擬設備的 IP 位址或完全限定網域名稱。 b. 使用您的維護使用者名稱和密碼登入維護控制台。
Linux	<ol style="list-style-type: none"> a. 使用安全性外殼連接到 Unified Manager 系統的 IP 位址或完全限定網域名稱。 b. 使用維護使用者 (umadmin) 名稱和密碼登入系統。 c. 輸入命令 `maintenance_console` 然後按 Enter 鍵。
視窗	<ol style="list-style-type: none"> a. 使用管理員憑證登入 Unified Manager 系統。 b. 以 Windows 管理員身分啟動 PowerShell。 c. 輸入命令 `maintenance_console` 然後按 Enter 鍵。

顯示 Unified Manager 維護控制台選單。

產生並上傳支援包

您可以產生包含診斷資訊的支援包，以便將其傳送給技術支援以獲得故障排除協助。

從 Unified Manager 9.8 開始，如果您的 Unified Manager 伺服器已連接到互聯網，您也可以從維護控制台將支援套件上傳到 NetApp。

開始之前

您必須以維護使用者身分存取維護控制台。

由於某些類型的支援資料可能會使用大量叢集資源或需要很長時間才能完成，因此當您選擇完整支援包時，您可以指定要包含或排除的資料類型以減少支援包的大小。您也可以選擇建立一個輕量級支援包，其中僅包含 30 天的日誌和設定資料庫記錄 - 它不包括效能資料、擷取記錄檔和伺服器堆轉儲。

Unified Manager 僅儲存最近產生的兩個支援包。較舊的支援包已從系統中刪除。

步驟

1. 在維護控制台*主選單*中，選擇*支援/診斷*。
2. 根據您希望在支援包中擁有的詳細程度，選擇*產生輕量支援包*或*生成支援包*。
3. 如果選擇完整支援包，請選擇或取消選擇以下資料類型以在支援包中包含或排除：

- 資料庫轉儲

MySQL 伺服器資料庫的轉儲。

- 堆轉儲

主 Unified Manager 伺服器進程狀態的快照。此選項預設為停用狀態，僅應在客戶支援要求時選擇。

- 採集記錄

Unified Manager 與受監控叢集之間的所有通訊的記錄。



如果取消選擇所有資料類型，則支援包仍會與其他 Unified Manager 資料一起產生。

4. 類型 `g`，然後按 Enter 鍵產生支援包。

由於產生支援包是一項佔用大量記憶體的操作，因此系統會提示您確認是否確定要在此時產生支援包。

5. 類型 `y`，然後按 Enter 鍵產生支援包。

如果您現在不想產生支援包，請鍵入 `n`，然後按 Enter。

6. 如果您在完整支援包中包含了資料庫轉儲文件，系統將提示您指定要包含效能統計資料的時間段。包含效能統計資訊可能會佔用大量時間和空間，因此您也可以轉儲資料庫而不包含效能統計資料：

- a. 以 YYYYMMDD 格式輸入開始日期。

例如，輸入 `20210101` 截至 2021 年 1 月 1 日。進入 `n` 如果您不想包含效能統計資料。

b. 輸入要包含的統計資料的天數，從指定開始日期的凌晨 12 點開始。

您可以輸入 1 到 10 之間的數字。

如果包括效能統計數據，系統將顯示將收集效能統計資料的時間段。

7. 建立支援包後，系統會提示您是否要將其上傳到 NetApp。類型 *y*，然後按 Enter。

系統會提示您輸入支援案例編號。

8. 如果您已經有案件編號，請輸入該編號並按 Enter。否則只需按 Enter 鍵。

支援包已上傳至 NetApp。

如果您的 Unified Manager 伺服器未連接到互聯網，或者您因任何其他原因無法上傳支援包，那麼您可以檢索它並手動傳送。您可以使用 SFTP 用戶端或使用 UNIX 或 Linux CLI 命令檢索它。在 Windows 安裝中，您可以使用遠端桌面 (RDP) 來擷取支援包。

產生的支援包位於 VMware 系統上的 /support 目錄中、Linux 系統上的 /opt/netapp/data/support/ 中以及 Windows 系統上的 ProgramData\ NetApp\OnCommandAppData\ocum\support 中。

相關資訊

["Unified Manager 使用者角色和功能"](#)

使用 **Windows** 用戶端檢索支援包

如果您是 Windows 用戶，您可以下載並安裝一個工具來從 Unified Manager 伺服器檢索支援包。您可以將支援包發送給技術支持，以便對問題進行更詳細的診斷。Filezilla 或 WinSCP 是您可以使用的工具的範例。

開始之前

您必須是維護使用者才能執行此任務。

您必須使用支援 SCP 或 SFTP 的工具。

步驟

1. 下載並安裝工具來檢索支援包。
2. 打開工具。
3. 透過 SFTP 連線到您的 Unified Manager 管理伺服器。

該工具顯示 /support 目錄的內容，您可以查看所有現有的支援包。

4. 選擇要複製的支援包的目標目錄。
5. 選擇要複製的支援包，然後使用該工具將檔案從 Unified Manager 伺服器複製到本機系統。

使用 **UNIX** 或 **Linux** 用戶端檢索支援包

如果您是 UNIX 或 Linux 用戶，則可以使用 Linux 用戶端伺服器上的命令列介面 (CLI) 從

vApp 中擷取支援包。您可以使用 SCP 或 SFTP 來檢索支援包。

開始之前

您必須是維護使用者才能執行此任務。

您必須已使用維護控制台產生支援包並具有可用的支援包名稱。

步驟

1. 使用 Linux 用戶端伺服器透過 Telnet 或控制台存取 CLI。
2. 訪問`/support`目錄。
3. 使用以下命令檢索支援包並將其複製到本機目錄：

如果您正在使用...	然後使用以下命令...
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
安全FTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

當您使用維護控制台產生支援包時，會向您提供其名稱。

4. 輸入維護用戶密碼。

範例

以下範例使用 SCP 檢索支援包：

```
`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z 100% 119MB 11.9MB/s 00:10
```

以下範例使用 SFTP 檢索支援包：

```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

向技術支援發送支援包

當問題需要比AutoSupport訊息提供的更詳細的診斷和故障排除資訊時，您可以向技術支援發送支援包。

開始之前

您必須具有支援包的存取權限才能將其傳送給技術支援。

您必須擁有透過技術支援網站產生的案例編號。

步驟

1. 登入NetApp支援站點。
2. 上傳文件。

["如何將檔案上傳到NetApp"](#)

與多個工作流程相關的任務和訊息

一些可以幫助您理解和完成工作流程的任務和參考文字對於 Unified Manager 中的許多工作流程都是通用的，包括添加和查看有關事件的註釋、分配事件、確認和解決事件以及有關磁碟區、儲存虛擬機器 (SVM)、聚合等的詳細資訊。

集群組件及其爭用的原因

當叢集元件發生爭用時，您可以識別叢集效能問題。使用該元件的工作負載的效能會變慢，且其對用戶端請求的回應時間（延遲）會增加，從而觸發 Unified Manager 中的事件。

存在爭用的組件無法達到最佳效能。它的性能已經下降，並且其他群集組件和工作負載（稱為“受害者”）的性能可能會增加延遲。要使組件擺脫爭用，必須減少其工作負載或提高其處理更多工作的能力，以便效能恢復到正常水準。由於 Unified Manager 以五分鐘為間隔收集和分析工作負載效能，因此它僅偵測叢集元件何時持續過度使用。未偵測到在五分鐘間隔內僅持續很短時間的過度使用瞬態峰值。

例如，儲存聚合可能處於爭用狀態，因為其上的一個或多個工作負載正在競爭滿足其 I/O 請求。聚合上的其他工作負載可能會受到影響，導致其效能下降。為了減少聚合上的活動量，您可以採取不同的步驟，例如將一個或多個工作負載移至較不繁忙的聚合或節點，以減少目前聚合上的整體工作負載需求。對於 QoS 策略群組，您可以調整吞吐量限制，或將工作負載移至其他策略群組，這樣工作負載就不會再受到限制。

Unified Manager 監控以下叢集元件，並在它們發生爭用時提醒您：

- 網路

表示叢集上外部網路協定的 I/O 請求的等待時間。等待時間是指叢集回應 I/O 請求之前等待「傳輸就緒」事務完成所花費的時間。如果網路元件處於爭用狀態，則表示協定層的高等待時間會影響一個或多個工作負載的延遲。

- 網路處理

表示集群中涉及協定層和集群之間的 I/O 處理的軟體元件。自從偵測到該事件以來，處理網路處理的節點可能已經發生變化。如果網路處理元件存在爭用，則表示網路處理節點的高利用率正在影響一個或多個工作負

載的延遲。

在主動-主動配置中使用全 SAN 陣列群集時，將顯示兩個節點的網路處理延遲值，以便您可以驗證節點是否平等地共享負載。

- **QoS 限制最大值**

表示指派給工作負載的儲存服務品質 (QoS) 策略群組的最大吞吐量 (峰值) 設定。如果策略群組元件存在爭用，則表示策略群組中的所有工作負載都受到設定的吞吐量限制的限制，這會影響其中一個或多個工作負載的延遲。

- **QoS 限制最小值**

表示由分配給其他工作負載的 QoS 吞吐量最小 (預期) 設定導致的工作負載延遲。如果某些工作負載上設定的 QoS 最小值使用大部分頻寬來保證承諾的吞吐量，則其他工作負載將受到限制並出現更多延遲。

- **集群互連**

表示叢集節點實體連接的電纜和適配器。如果叢集互連元件處於爭用狀態，則表示叢集互連處 I/O 請求的等待時間過長會影響一個或多個工作負載的延遲。

- **Data Processing**

表示叢集中涉及叢集與包含工作負載的儲存聚合之間的 I/O 處理的軟體元件。自從偵測到事件以來，處理資料處理的節點可能已經發生變化。如果資料處理元件存在爭用，則表示資料處理節點的高利用率正在影響一個或多個工作負載的延遲。

- **音量啟動**

表示追蹤所有活動卷使用情況的進程。在有超過 1000 個磁碟區處於活動狀態的大型環境中，此流程會追蹤有多少個關鍵磁碟區需要同時透過節點存取資源。當並發活動卷的數量超過建議的最大閾值時，一些非關鍵卷將會出現此處標識的延遲。

- *** MetroCluster資源***

表示MetroCluster資源，包括NVRAM和交換器間連結 (ISL)，用於在MetroCluster配置中的叢集之間鏡像資料。如果MetroCluster元件存在爭用，則表示本地叢集上的工作負載的高寫入吞吐量或連結健康問題正在影響本地叢集上一個或多個工作負載的延遲。如果叢集不在MetroCluster配置中，則不會顯示此圖示。

- **聚合或 SSD 聚合操作**

表示運行工作負載的儲存聚合。如果聚合元件存在爭用，則表示聚合的高利用率正在影響一個或多個工作負載的延遲。聚合由所有 HDD 組成，或由 HDD 和 SSD 的混合 (Flash Pool 聚合) 組成，或由 HDD 和雲層的混合 (FabricPool聚合) 組成。「SSD 聚合」由所有 SSD (全快閃聚合) 或 SSD 和雲層 (FabricPool 聚合) 的混合組成。

- **雲延遲**

表示叢集中涉及叢集和儲存使用者資料的雲層之間的 I/O 處理的軟體元件。如果雲端延遲元件存在爭用，則表示託管在雲層上的磁碟區的大量讀取會影響一個或多個工作負載的延遲。

- **同步SnapMirror**

表示叢集中涉及在SnapMirror同步關係中將使用者資料從主磁碟區複製到輔助磁碟區的軟體元件。如果同

步SnapMirror元件存在爭用，則表示SnapMirror同步操作的活動正在影響一個或多個工作負載的延遲。

音量/健康詳情頁面

您可以使用卷/健康詳情頁面查看有關所選卷的詳細信息，例如容量、存儲效率、配置、保護、註釋和生成的事件。您也可以查看有關該磁碟區的相關對象和相關警報的資訊。

您必須具有應用程式管理員或儲存管理員角色。

命令按鈕

命令按鈕可讓您對選定的磁碟區執行下列任務：

- 切換到效能視圖

使您能夠導航到磁碟區/效能詳細資訊頁面。

- 行動

- 添加警報

使您能夠在選定卷上新增警報。

- 編輯閾值

使您能夠修改選定卷的閾值設定。

- 註解

使您能夠註釋選定的捲。

- 保護

使您能夠為選定的磁碟區建立SnapMirror或SnapVault關係。

- 關係

使您能夠執行以下保護關係操作：

- 編輯

啟動「編輯關係」對話框，該對話框使您能夠更改現有保護關係的現有SnapMirror策略、計劃和最大傳輸速率。

- 中止

中止選定關係正在進行的傳輸。或者，它使您能夠刪除除基線傳輸之外的傳輸的重新啟動檢查點。您無法刪除基線傳輸的檢查點。

- 靜止

暫時停用選定關係的計畫更新。正在進行的傳輸必須在關係停止之前完成。

- 休息

中斷開源磁碟區和目標磁碟區之間的關係，並將目標變更為讀寫磁碟區。

- 消除

永久刪除所選來源和目標之間的關係。磁碟區不會被破壞，磁碟區上的 Snapshot 副本也不會被刪除。此操作無法撤銷。

- 恢復

為靜止關係啟用預定的傳輸。在下一個計劃的傳輸間隔，將使用重新啟動檢查點（如果存在）。

- 重新同步

使您能夠重新同步先前中斷的關係。

- 初始化/更新

使您能夠對新的保護關係執行首次基準傳輸，或者如果關係已經初始化，則執行手動更新。

- 反向重新同步

使您能夠重新建立先前中斷的保護關係，透過將來源變為原始目標的副本來逆轉來源和目標的功能。來源上的內容將被目標上的內容覆蓋，並且任何比通用 Snapshot 副本上的資料更新的資料都將被刪除。

- 恢復

使您能夠將資料從一個磁碟區還原到另一個磁碟區。有關信息，請參閱["使用卷/健康詳情頁面恢復數據"](#)。



對於處於同步保護關係中的捲，「恢復」按鈕和「關係」操作按鈕不可用。

- 查看卷

使您能夠導航至“運行狀況：所有磁碟區”視圖。

容量選項卡

容量標籤顯示有關所選卷的詳細信息，例如其物理容量、邏輯容量、閾值設定、配額容量以及有關任何磁碟區移動操作的資訊：

- 物理容量

詳細說明卷的物理容量：

- 快照溢出

顯示 Snapshot 副本佔用的資料空間。

- 用過的

顯示磁碟區中資料所使用的空間。

- 警告

表示磁碟區中的空間已快滿。如果超過此閾值，則會產生空間幾乎已滿事件。

- 錯誤

表示磁碟區中的空間已滿。如果超出此閾值，則會產生空間已滿事件。

- 無法使用

表示已產生精簡配置磁碟區空間面臨風險事件，且精簡配置磁碟區中的空間因聚合容量問題而面臨風險。僅對精簡配置磁碟區顯示不可用容量。

- 數據圖

顯示磁碟區的總資料容量和已使用資料容量。

如果啟用了自動成長，資料圖也會顯示聚合中可用的空間。資料圖顯示磁碟區中資料可使用的有效儲存空間，可以是以下之一：

- 卷的實際資料容量適用於以下條件：

- 自動增長已停用。

- 啟用自動增長的磁碟區已達到最大大小。

- 啟用自動增長的厚配置磁碟區無法進一步增長。

- 考慮最大磁碟區大小後的磁碟區資料容量（對於精簡配置磁碟區和密集配置卷，當聚合具有使磁碟區達到最大大小所需的空間時）

- 考慮下一個可能的自動增長大小後的卷的資料容量（對於具有自動增長百分比閾值的厚配置磁碟區）

- 快照副本圖

僅當已用快照容量或快照預留不為零時才會顯示此圖。

如果已使用的快照容量超過快照預留，則兩個圖表都會顯示快照容量超過快照預留的容量。

- 容量邏輯

顯示磁碟區的邏輯空間特徵。邏輯空間表示儲存在磁碟上的資料的實際大小，而不考慮使用ONTAP儲存效率技術所節省的資料。

- 邏輯空間報告

顯示磁碟區是否已配置邏輯空間報告。該值可以是「啟用」、「停用」或「不適用」。對於舊版ONTAP上的卷或不支援邏輯空間報告的卷，將顯示「不適用」。

- 用過的

顯示磁碟區中資料正在使用的邏輯空間量，以及基於總資料容量的已使用邏輯空間百分比。

- 邏輯空間執行

顯示是否為精簡配置磁碟區配置了邏輯空間強制執行。當設定為 Enabled 時，磁碟區的邏輯使用大小不能大於目前設定的實體磁碟區大小。

- 自動生長

顯示捲空間不足時是否自動增大。

- 艙位保證

當磁碟區從聚合中刪除可用區塊時顯示FlexVol volume設定控制。然後保證這些區塊可用於寫入磁碟區中的檔案。空間保證可以設定為以下之一：

- 沒有任何

沒有為該磁碟區配置空間保證。

- 文件

保證稀疏寫入檔案（例如 LUN）的完整大小。

- 體積

保證卷的完整大小。

- 部分的

FlexCache卷根據其大小預留空間。如果FlexCache磁碟區的大小為 100 MB 或更多，則最小空間保證預設為 100 MB。如果FlexCache磁碟區的大小小於 100 MB，則最小空間保證設定為FlexCache磁碟區的大小。如果FlexCache磁碟區的大小稍後增加，則最小空間保證不會增加。



當磁碟區的類型為資料快取時，空間保證是部分的。

- 詳細資料（物理）

顯示卷的物理特性。

- 總容量

顯示磁碟區中的總物理容量。

- 數據容量

顯示磁碟區已使用的實體空間量（已使用容量）和磁碟區中仍可用的實體空間量（可用容量）。這些值也顯示為總物理容量的百分比。

當為精簡配置磁碟區產生「精簡配置磁碟區空間處於風險」事件時，將顯示磁碟區已使用的空間量（已使用容量）以及磁碟區中可用但因聚合容量問題而無法使用的空間量（不可用容量）。

- 快照保留

顯示磁碟區中 Snapshot 副本使用的空間量（已使用容量）和可用於 Snapshot 副本的空間量（可用容量）。這些值也顯示為總快照儲備的百分比。

當為精簡配置磁碟區產生「精簡配置磁碟區空間處於風險」事件時，將顯示 Snapshot 副本使用的空間量（已使用容量）以及磁碟區中可用但因聚合容量問題而無法用於製作 Snapshot 副本的空間量（不可用容量）。

- 音量閾值

顯示以下磁碟區容量閾值：

- 接近滿閾值

指定卷接近滿的百分比。

- 完整閾值

指定磁碟區已滿的百分比。

- 其他詳情

- 自動增長最大尺寸

顯示卷可以自動增長到的最大大小。預設值為建立時磁碟區大小的 120%。僅當磁碟區啟用自動增長時才會顯示此欄位。

- Qtree 配額承諾容量

顯示配額中保留的空間。

- Qtree 配額過載容量

顯示系統產生磁碟區 Qtree 配額過載事件之前可以使用的空間量。

- 部分準備金

控制覆蓋保留的大小。預設情況下，預留百分比設定為 100，表示保留 100% 的所需預留空間，以便完全保護物件免於覆蓋。如果預留百分比小於 100%，則該磁碟區中所有空間預留檔案的預留空間將減少至預留百分比。

- 每日增長率快照

顯示選定磁碟區中 Snapshot 副本每 24 小時發生的變更（以百分比或 KB、MB、GB 等為單位）。

- 快照天數至滿

顯示為磁碟區中的 Snapshot 副本保留的空間達到指定閾值之前估計剩餘的天數。

當磁碟區中 Snapshot 副本的成長率為零或負數，或沒有足夠的資料來計算成長率時，「Snapshot Days to Full」欄位將顯示「不適用」值。

- 快照自動刪除

指定當因聚合空間不足而導致寫入磁碟區失敗時是否自動刪除 Snapshot 副本以釋放空間。

- 快照副本

顯示有關磁碟區中的 Snapshot 副本的資訊。

卷中的 Snapshot 副本數量顯示為連結。點擊該連結將開啟「磁碟區上的 Snapshot 副本」對話框，其中顯示 Snapshot 副本的詳細資料。

Snapshot 副本計數大約每小時更新一次；但是，Snapshot 副本清單會在您點擊圖示時更新。這可能會導致拓撲中顯示的 Snapshot 副本數與單擊圖示時列出的 Snapshot 副本數有所不同。

- 音量移動

顯示對磁碟區執行的當前或最後一個磁碟區移動操作的狀態以及其他詳細信息，例如正在進行的磁碟區移動操作的當前階段、來源聚合、目標聚合、開始時間、結束時間和預計結束時間。

也顯示在選定磁碟區上執行的磁碟區移動操作的數量。您可以透過點擊「磁碟區移動記錄」連結查看更多關於磁碟區移動操作的資訊。

“配置”選項卡

配置選項卡顯示有關所選卷的詳細信息，例如卷的導出策略、RAID 類型、容量和存儲效率相關功能：

- 概述

- 姓名

顯示卷的完整名稱。

- 聚合

顯示磁碟區所在聚合的名稱，或FlexGroup磁碟區所在聚合的數量。

- 分層策略

顯示為磁碟區設定的分層策略；如果磁碟區部署在啟用FabricPool的聚合上。此策略可以是無、僅快照、備份、自動或全部。

- 儲存虛擬機

顯示包含該磁碟區的 SVM 的名稱。

- 連接路徑

顯示路徑的狀態，可以是活動的或非活動的。也會顯示 SVM 中磁碟區的掛載路徑。您可以點擊「歷史記錄」連結查看連接路徑的最近五次變更。

- 出口政策

顯示為磁碟區建立的匯出策略的名稱。您可以按一下連結以查看有關屬於 SVM 的磁碟區上啟用的匯出策略、驗證協定和存取的詳細資訊。

- 風格

顯示音量樣式。磁碟區樣式可以是FlexVol或FlexGroup。

- 類型

顯示選定卷的類型。卷類型可以是讀寫、負載共享、資料保護、資料快取或臨時。

- RAID類型

顯示選定磁碟區的 RAID 類型。 RAID 類型可以是 RAID0、RAID4、RAID-DP 或RAID-TEC。



FlexGroup磁碟區可能會顯示多種 RAID 類型，因為 FlexGroups 的組成磁碟區可以位於不同類型的聚合上。

- SnapLock類型

顯示包含該磁碟區的聚合的SnapLock類型。

- SnapLock到期

顯示SnapLock磁碟區的到期日。

- 容量

- 精簡配置

顯示是否為磁碟區配置了精簡配置。

- 自動成長

顯示靈活卷是否在聚合內自動增長。

- 快照自動刪除

指定當因聚合空間不足而導致寫入磁碟區失敗時是否自動刪除 Snapshot 副本以釋放空間。

- 配額

指定是否為磁碟區啟用配額。

- 效率

- 壓縮

指定是否啟用或停用壓縮。

- 重複資料刪除

指定是否啟用或停用重複資料刪除。

- 重複資料刪除模式

指定在磁碟區上啟用的重複資料刪除操作是手動、規劃或基於策略的操作。如果模式設定為Scheduled，則顯示操作計劃，如果模式設定為策略，則顯示策略名稱。

- 重複資料刪除類型

指定在磁碟區上執行的重複資料刪除操作的類型。如果磁碟區處於SnapVault關係中，則顯示的類型為SnapVault。對於任何其他卷，類型顯示為常規。

- 儲存效率策略

指定已透過 Unified Manager 指派給此磁碟區的儲存效率策略的名稱。此策略可以控制壓縮和重複資料刪除設定。

- 保護

- 快照副本

指定是否啟用或停用自動 Snapshot 副本。

保護選項卡

「保護」標籤顯示有關所選卷的保護詳細信息，例如滯後資訊、關係類型和關係拓撲。

- 概括

顯示選定磁碟區的保護關係（SnapMirror、SnapVault或儲存 VM DR）屬性。對於任何其他關係類型，僅顯示關係類型屬性。如果選擇了主磁碟區，則僅顯示託管和本機快照副本原則。SnapMirror和SnapVault關係顯示的屬性包括：

- 源體積

如果選定磁碟區是目標，則顯示選定磁碟區的來源的名稱。

- 滯後狀態

顯示保護關係的更新或傳輸滯後狀態。狀態可以是錯誤、警告或嚴重。

滯後狀態不適用於同步關係。

- 滯後持續時間

顯示鏡像上的資料落後於來源的時間。

- 上次成功更新

顯示最近一次成功保護更新的日期和時間。

上次成功更新不適用於同步關係。

- 儲存服務會員

顯示「是」或「否」以指示該磁碟區是否屬於儲存服務並由儲存服務管理。

- 版本靈活複製

顯示「是」、「有備份選項」或「無」。是表示即使來源磁碟區和目標磁碟區運行不同版本的ONTAP軟體，也可以進行SnapMirror複製。「是」且帶有備份選項表示實施SnapMirror保護，並能夠在目標上保留多個版本的備份副本。None 表示未啟用版本靈活複製。

- 關係能力

指示保護關係可用的ONTAP功能。

- 保護服務

如果關係由保護合作夥伴應用程式管理，則顯示保護服務的名稱。

- 關係類型

顯示任何關係類型，包括非同步鏡像、非同步保險庫、非同步鏡像保險庫、StrictSync 和同步。

- 關係狀態

顯示SnapMirror或SnapVault關係的狀態。狀態可以是未初始化、SnapMirrored 或 Broken-Off。如果選擇了來源卷，則關係狀態不適用且不會顯示。

- 轉移狀態

顯示保護關係的傳輸狀態。傳輸狀態可以是以下之一：

- 正在中止

SnapMirror傳輸已啟用；但是，傳輸中止操作（可能包括刪除檢查點）正在進行中。

- 檢查

目標磁碟區正在進行診斷檢查，並且沒有正在進行的傳輸。

- 最終確定

SnapMirror傳輸已啟用。該磁碟區目前處於增量SnapVault傳輸的後傳輸階段。

- 閒置的

傳輸已啟用並且沒有正在進行的傳輸。

- 同步

處於同步關係的兩個磁碟區中的資料是同步的。

- 不同步

目標磁碟區中的資料與來源磁碟區不同步。

- 準備

SnapMirror傳輸已啟用。該磁碟區目前處於增量SnapVault傳輸的預傳輸階段。

- 排隊

SnapMirror傳輸已啟用。目前沒有正在進行的轉移。

- 靜默

SnapMirror傳輸已停用。目前沒有正在進行的轉移。

- 靜默

SnapMirror傳輸正在進行中。附加傳輸已停用。

- 轉移

SnapMirror傳輸已啟用且傳輸正在進行中。

- 過渡

從來源到目標磁碟區的非同步資料傳輸已完成，並且已開始轉換到同步操作。

- 等待

SnapMirror傳輸已啟動，但一些相關任務正在等待排隊。

- 最大傳輸速率

顯示關係的最大傳輸速率。最大傳輸速率可以是每秒千位元組 (Kbps)、每秒兆位元組 (Mbps)、每秒千兆位元組 (Gbps) 或每秒太字節 (Tbps) 的數值。如果顯示“無限制”，則關係之間的基線轉移不受限制。

- SnapMirror策略

顯示卷的保護策略。DPDefault 表示預設的非同步鏡像保護策略，XDPEndpointDefault 表示預設的非同步保險庫策略，DPSyncDefault 表示預設的非同步鏡像保險庫策略。StrictSync表示預設的同步嚴格保護策略，Sync表示預設的同步策略。您可以單擊策略名稱以查看與該策略相關的詳細信息，包括以下信息：

- 轉讓優先權

- 忽略訪問時間設定

- 嘗試次數限制

- 評論

- SnapMirror標籤

- 保留設定

- 實際的 Snapshot 副本

- 保留 Snapshot 副本

- 保留警告閾值

- 沒有保留設定的 Snapshot 副本在來源是資料保護 (DP) 磁碟區的級聯SnapVault關係中，僅適用規則「sm_created」。

- 更新時間表

顯示指派給該關係的SnapMirror方案。將遊標放在資訊圖示上即可顯示時間表詳細資訊。

- 本機快照策略

顯示磁碟區的 Snapshot 副本策略。此策略是預設策略、無策略或任何自訂策略的名稱。

- 受保護

顯示所選磁碟區所使用的保護類型。例如，如果磁碟區受一致性群組和SnapMirror磁碟區關係保護，則此欄位同時顯示SnapMirror和一致性群組。該欄位還提供一個鏈接，將您重新導向到“關係”頁面以查看統一關係狀態。此連結僅適用於組成關係。

- 一致性組

對於受SnapMirror活動同步關係保護的磁碟區，此列顯示磁碟區的一致性群組。

- 觀點

顯示選定磁碟區的保護拓撲。拓撲包括與選定卷相關的所有捲的圖形表示。所選卷以深灰色邊框表示，拓撲中卷之間的線條表示保護關係類型。拓撲中關係的方向從左到右顯示，每個關係的來源在左側，目標在右側。

雙粗線指定非同步鏡像關係，單粗線指定非同步保險庫關係，雙單線指定非同步鏡像保險庫關係，粗線和非粗線指定同步關係。下表指示同步關係是 StrictSync 還是 Sync。

右鍵單擊卷將顯示一個選單，您可以從中選擇保護該卷或將資料恢復到該卷。右鍵點選某個關係將顯示一個選單，您可以從中選擇編輯、中止、停止、中斷、刪除或還原該關係。

在下列情況下，選單將不會顯示：

- 如果 RBAC 設定不允許此操作，例如，如果您只有操作員權限
- 如果磁碟區處於同步保護關係
- 當磁碟區 ID 未知時，例如，當您具有群集間關係且尚未發現目標群集時，按一下拓撲中的另一個磁碟區將選取並顯示該磁碟區的資訊。問號 (?) 位於磁碟區的左上角，表示該磁碟區遺失或尚未被發現。這也可能表明缺少容量資訊。將遊標放在問號上會顯示更多信息，包括補救措施的建議。

如果拓撲符合幾種常見拓撲範本之一，則會顯示有關磁碟區容量、延遲、Snapshot 副本和上次成功資料傳輸的資訊。如果拓撲不符合其中一個模板，則有關磁碟區滯後和上次成功資料傳輸的資訊將顯示在拓撲下的關聯表中。在這種情況下，表中反白的行表示所選卷，而在拓撲視圖中，帶有藍點的粗線表示所選卷與其來源卷之間的關係。

拓撲視圖包括以下資訊：


- 容量

顯示磁碟區使用的總容量。將遊標置於拓撲中的磁碟區上會在「目前閾值設定」對話方塊中顯示該磁碟區的目前警告和嚴重閾值設定。您也可以透過點擊「目前閾值設定」對話方塊中的「編輯閾值」連結來編輯閾值設定。清除「容量」複選框將隱藏拓撲中所有磁碟區的所有容量資訊。

- 落後

顯示傳入保護關係的滯後持續時間和滯後狀態。清除 **Lag** 複選框將隱藏拓撲中所有磁碟區的所有延遲資訊。當 **Lag** 複選框變暗時，所選卷的滯後資訊將顯示在拓撲下方的關係表中，以及所有相關磁碟區的延遲資訊。

- 快照

顯示磁碟區可用的 Snapshot 副本數。清除 **Snapshot** 複選框將隱藏拓撲中所有磁碟區的所有 Snapshot 副本資訊。點選 Snapshot 副本圖示 () 顯示磁碟區的 Snapshot 副本清單。圖示旁顯示的 Snapshot 副本計數大約每小時更新一次；但是，Snapshot 副本清單會在您點擊圖示時更新。這可能會導致拓撲中顯示的 Snapshot 副本數與單擊圖示時列出的 Snapshot 副本數有所不同。

- 上次成功轉移

顯示上次成功傳輸資料的數量、持續時間、時間和日期。當「上次成功傳輸」複選框變暗時，所選卷的上次成功傳輸訊息將顯示在拓撲下方的關係表中，以及所有相關卷的上次成功傳輸訊息。

- 歷史

以圖表形式顯示選定卷的傳入 SnapMirror 和 SnapVault 保護關係的歷史記錄。有三種歷史圖表可用：傳入關係延遲持續時間、傳入關係轉移持續時間和傳入關係轉移大小。僅當您選擇目標磁碟區時才會顯示歷史資訊。如果選擇主卷，則圖表為空，並顯示訊息「未找到資料」。如果磁碟區受一致性群組和 SnapMirror 同步關係保護，則不會顯示關係傳輸持續時間和關係傳輸大小的資訊。

您可以從歷史記錄窗格頂部的下拉清單中選擇圖表類型。您也可以透過選擇 1 週、1 個月或 1 年來查看特定時間段的詳細資訊。歷史圖表可以幫助您識別趨勢：例如，如果在一天或一周的同一時間傳輸大量數據，或者持續突破滯後警告或滯後錯誤閾值，您可以採取適當的措施。此外，您可以按一下「匯出」按鈕為您正在查看的圖表建立 CSV 格式的報表。

保護歷史圖表顯示以下資訊：

- 關係滯後持續時間

根據所選的持續時間，在垂直 (y) 軸上顯示秒、分鐘或小時，在水平 (x) 軸上顯示天、月或年。y 軸上方的數值表示 x 軸所示持續時間內達到的最大延遲持續時間。圖表上的水平橙色線表示滯後誤差閾值，水平黃色線表示滯後警告閾值。將遊標放在這些線上即可顯示閾值設定。水平藍線表示滯後持續時間。您可以將遊標放在感興趣的區域上來查看圖表上特定點的詳細資訊。

- 關係轉移持續時間

根據所選的持續時間，在垂直 (y) 軸上顯示秒、分鐘或小時，在水平 (x) 軸上顯示天、月或年。y 軸上方的數值表示 x 軸所示持續時間內達到的最大傳輸持續時間。您可以將遊標放在感興趣的區域上來查看圖表上特定點的詳細資訊。



對於處於同步保護關係的捲，此圖表不可用。

- 關係轉移大小

根據傳輸大小在垂直 (y) 軸上顯示位元組、千位元組、兆位元組等，並根據所選時間段在水平 (x) 軸上顯示天、月或年。y 軸上方的數值表示 x 軸所示持續時間內達到的最大傳輸大小。您可以將遊標放在感興趣的區域上來查看圖表上特定點的詳細資訊。



對於處於同步保護關係的捲，此圖表不可用。

歷史區

歷史記錄區域顯示提供有關選定磁碟區的容量和空間預留的資訊的圖表。此外，您可以按一下「匯出」按鈕為您正在查看的圖表建立 CSV 格式的報表。

當磁碟區的資料或狀態在一段時間內保持不變時，圖表可能為空，並顯示訊息「未找到資料」。

您可以從歷史記錄窗格頂部的下拉清單中選擇圖表類型。您也可以透過選擇 1 週、1 個月或 1 年來查看特定時間段的詳細資訊。歷史圖表可以幫助您識別趨勢 - 例如，如果磁碟區使用情況持續突破「幾乎滿」閾值，您可以採取適當的措施。

歷史圖表顯示以下資訊：

- 已使用的磁碟區容量

顯示磁碟區中的已使用容量以及基於使用歷史記錄的捲容量使用趨勢，在垂直 (y) 軸上以位元組、千位元組、兆位元組等為單位的折線圖。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下磁碟區已使用容量圖例時，磁碟區已使用容量圖形線將會被隱藏。

- 已使用磁碟區容量與總容量

根據使用歷史記錄顯示卷容量的使用趨勢，以及已用容量、總容量以及重複數據刪除和壓縮節省空間的詳細信息，以折線圖的形式在垂直 (y) 軸上以字節、千字節、兆字節等為單位顯示。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下「趨勢容量已使用」圖例時，「趨勢容量已使用」圖形線將會被隱藏。

- 已使用容量 (%)

顯示磁碟區中的已使用容量以及基於使用歷史記錄的捲容量使用趨勢，以百分比形式顯示在垂直 (y) 軸上。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下磁碟區已使用容量圖例時，磁碟區已使用容量圖形線將會被隱藏。

- 已使用快照容量 (%)

將 Snapshot 預留和 Snapshot 警告閾值顯示為折線圖，並將 Snapshot 副本使用的容量顯示為區域圖（以百分比表示，位於垂直 (y) 軸上）。快照溢位用不同的顏色表示。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下快照預留圖例時，快照預留圖形線將會被隱藏。

事件列表

事件清單顯示有關新事件和已確認事件的詳細資訊：

- 嚴重性

顯示事件的嚴重性。

- 事件

顯示事件名稱。

- 觸發時間

顯示事件產生以來經過的時間。如果時間超過一周，則會顯示事件產生的時間戳記。

相關註釋窗格

透過「相關註釋」窗格，您可以查看與所選卷相關的註釋詳細資訊。詳細資訊包括註釋名稱和應用於卷的註釋值。您也可以從「相關註釋」窗格中刪除手動註釋。

相關設備窗格

透過「相關設備」窗格，您可以檢視並導覽至與磁碟區相關的 SVM、聚合、qtree、LUN 和 Snapshot 副本：

- 儲存虛擬機器

顯示包含選定磁碟區的 SVM 的容量和運作狀況。

- 總計的

顯示包含選定磁碟區的聚合的容量和運作狀況。對於 FlexGroup 卷，列出了組成 FlexGroup 的聚合數量。

- 總量

顯示屬於選定磁碟區的父聚合的所有磁碟區的數量和容量。也會根據最高嚴重性等級顯示捲的健康狀況。例如，如果一個聚合包含十個卷，其中五個顯示警告狀態，其餘五個顯示嚴重狀態，則顯示的狀態為嚴重。FlexGroup 磁碟區中不會出現此元件。

- **Qtree**

顯示選定磁碟區所包含的 qtree 數量以及選定磁碟區所包含的具有配額的 qtree 容量。具有配額的 qtree 的容量相對於磁碟區資料容量顯示。也會根據最高嚴重程度顯示 qtree 的健康狀況。例如，如果某個磁碟區有 10 個 qtree，其中 5 個處於警告狀態，其餘 5 個處於嚴重狀態，則顯示的狀態為嚴重。

- **NFS 共享**

顯示與磁碟區關聯的 NFS 共享的數量和狀態。

- 中小企業股份

顯示 SMB/CIFS 共享的數量和狀態。

- LUN

顯示選定磁碟區中所有 LUN 的數量和總大小。也會根據最高嚴重性等級顯示 LUN 的健康狀況。

- 使用者和群組配額

顯示與磁碟區及其 qtree 關聯的使用者和使用者群組配額的數量和狀態。

- * FlexClone 卷*

顯示選定卷的所有克隆卷的數量和容量。僅當選定磁碟區包含任何複製磁碟區時才會顯示數量和容量。

- 家長卷

顯示選定FlexClone磁碟區的父磁碟區的名稱和容量。僅當選定的磁碟區是FlexClone磁碟區時才會顯示父磁碟區。

相關群組窗格

透過「相關群組」窗格，您可以查看與所選磁碟區關聯的群組的清單。

相關警報窗格

透過「相關警報」窗格，您可以查看為選定磁碟區建立的警報清單。您也可以透過點擊新增警報連結來新增警報，或透過點擊警報名稱來編輯現有警報。

儲存虛擬機器/運作狀況詳細資訊頁面

您可以使用儲存虛擬機器/運行狀況詳細資訊頁面查看有關所選儲存虛擬機器的詳細信息，例如其運行狀況、容量、配置、資料策略、邏輯介面 (LIF)、LUN、qtree、使用者、使用者群組配額和保護詳細資訊。您也可以查看有關儲存虛擬機器的相關物件和相關警報的資訊。



您只能監控資料儲存虛擬機器。

命令按鈕

命令按鈕可讓您對選取的儲存虛擬機器執行下列任務：

- 切換到效能視圖

使您能夠導航至儲存虛擬機器/效能詳細資訊頁面。

- 行動

- 添加警報

使您能夠為選定的儲存虛擬機器新增警報。

- 註解

使您能夠註解選定的儲存虛擬機器。

- 查看儲存虛擬機器

使您能夠導航至“運行狀況：所有儲存虛擬機器”視圖。

「健康」標籤

「運行狀況」標籤顯示有關各種物件（例如磁碟區、聚合、NAS LIF、SAN LIF、LUN、協定、服務、NFS 共用和 CIFS 共用）的資料可用性、資料容量和保護問題的詳細資訊。

您可以按一下物件的圖表來查看已篩選的物件清單。例如，您可以按一下顯示警告的磁碟區容量圖表來查看具有

嚴重程度為警告的容量問題的磁碟區清單。

- 可用性問題

以圖表形式顯示物件總數，包括有可用性問題的物件和不存在任何可用性相關問題的物件。圖表中的顏色代表問題的不同嚴重程度。圖表下方的信息提供了有關可用性問題的詳細信息，這些問題可能影響或已經影響了儲存虛擬機器中資料的可用性。例如，顯示有關已關閉的 NAS LIF 和 SAN LIF 以及離線的磁碟區的資訊。

您還可以查看當前正在運行的相關協定和服務的信息，以及NFS和CIFS共享的數量和狀態。

- 容量問題

以圖表形式顯示物件總數，包括存在容量問題的物件和不存在任何容量相關問題的物件。圖表中的顏色代表問題的不同嚴重程度。圖表下方的資訊提供了有關可能影響或已經影響儲存虛擬機器中資料容量的容量問題的詳細資訊。例如，顯示有關可能違反設定閾值的聚合的資訊。

- 保護問題

透過以欄位對話方塊的形式顯示關係總數（包括存在保護問題的關係和不存在任何保護相關問題的關係），快速概覽儲存虛擬機器保護相關的健康狀況。您也可以查看所選儲存虛擬機器的儲存虛擬機器 DR 關係的狀態。儲存 VM DR 關係事件顯示在此處，按一下事件將前往事件詳細資訊頁面。當存在不受保護的磁碟區時，按一下連結將前往「運行狀況：所有磁碟區」視圖，您可以在其中查看儲存虛擬機器上不受保護的磁碟區的篩選清單。圖表中的顏色代表問題的不同嚴重程度。點擊圖表將轉到“關係：所有關係”視圖，您可以在其中查看保護關係詳細資訊的篩選清單。圖表下方的資訊提供了可能影響或已經影響儲存虛擬機器中資料保護的保護問題的詳細資訊。例如，顯示有關 Snapshot 副本預留幾乎已滿的磁碟區或SnapMirror關係延遲問題的資訊。

容量選項卡

容量標籤顯示有關所選 SVM 的資料容量的詳細資訊。

對於具有FlexVol volume或FlexGroup磁碟區的儲存虛擬機，將顯示下列資訊：

- 容量

容量區域顯示有關從所有磁碟區分配的已使用容量和可用容量的詳細資訊：

- 總容量

顯示儲存虛擬機器的總容量。

- 用過的

顯示屬於儲存虛擬機器的磁碟區中資料所使用的空間。

- 保證可用

顯示儲存虛擬機器中磁碟區可用的保證資料空間。

- 無擔保

顯示儲存虛擬機器中精簡配置磁碟區所指派的資料剩餘可用空間。

- 存在容量問題的磁碟區

存在容量問題的磁碟區清單以表格形式顯示存在容量問題的磁碟區的詳細資訊：

- 地位

表示卷存在與容量相關的問題，且問題嚴重程度已指示。

您可以將指標移到狀態上以查看有關容量相關事件或為磁碟區產生的事件的事件的更多資訊。

如果磁碟區的狀態由單一事件決定，則可以查看事件名稱、觸發事件的時間和日期、分配事件的管理員的姓名以及事件的原因等資訊。您可以使用*查看詳細資訊*按鈕查看有關該事件的更多資訊。

如果磁碟區的狀態由多個相同嚴重程度的事件決定，則會顯示前三個事件，並顯示事件名稱、觸發事件的時間和日期以及分配事件的管理員的姓名等資訊。您可以透過點擊事件名稱來查看有關每個事件的更多詳細資訊。您也可以點擊「查看所有事件」連結來查看產生的事件清單。



一個卷可以有多个嚴重程度相同或不同的事件。但是，僅顯示最高嚴重程度。例如，如果某個磁碟區具有嚴重程度為「錯誤」和「警告」的兩個事件，則僅顯示「錯誤」嚴重程度。

- 體積

顯示卷的名稱。

- 已使用數據容量

以圖表形式顯示有關磁碟區容量使用情況的資訊（百分比）。

- 滿載天數

顯示捲達到最大容量之前預計剩餘的天數。

- 精簡配置

顯示是否為選定磁碟區設定了空間保證。有效值為“是”和“否”。

- 聚合

對於FlexVol卷，顯示包含該磁碟區的聚合的名稱。對於FlexGroup卷，顯示FlexGroup中使用的聚合數。

“配置”選項卡

配置標籤顯示有關所選儲存虛擬機器的配置詳細信息，例如其叢集、根磁碟區、其包含的磁碟區類型（FlexVol磁碟區）、策略以及在儲存虛擬機器上建立的保護：

- 概述

- 簇

顯示儲存虛擬機器所屬的叢集名稱。

- 允許的捲類型

顯示可以在儲存虛擬機器中建立的磁碟區的類型。型態可以是FlexVol或FlexVol/ FlexGroup。

- 根卷

顯示儲存虛擬機器的根磁碟區的名稱。

- 允許的協議

顯示可在儲存虛擬機器上設定的協定類型。此外，指示協議是否啟動 (●)，向下 (●)，或未配置 (●)。

- 資料網路介面

- 網路儲存

顯示與儲存虛擬機器關聯的 NAS 介面的數量。此外，指示介面是否已啟動 (●) 或向下 (●)。

- 儲存區域網絡

顯示與儲存虛擬機器關聯的 SAN 介面的數量。此外，指示介面是否已啟動 (●) 或向下 (●)。

- FC-NVMe

顯示與儲存虛擬機器關聯的 FC-NVMe 介面的數量。此外，指示介面是否已啟動 (●) 或向下 (●)。

- 管理網路介面

- 可用性

顯示與儲存虛擬機器關聯的管理介面的數量。此外，指示管理介面是否已啟動 (●) 或向下 (●)。

- 政策

- 快照

顯示在儲存虛擬機器上建立的快照策略的名稱。

- 出口政策

如果建立了單一策略，則顯示匯出策略的名稱；如果建立了多個策略，則顯示匯出策略的數量。

- 保護

- 儲存虛擬機器災難復原

顯示所選儲存虛擬機器是否受保護、目標或不受保護，以及受保護儲存虛擬機器的目標的名稱。如果選定的儲存虛擬機器是目標，則會顯示來源儲存虛擬機器的詳細資訊。在扇出的情況下，此欄位顯示受保護的儲存虛擬機器的目標儲存虛擬機器總數。計數連結將帶您進入按來源儲存虛擬機器過濾的儲存虛擬機器關係網格。

- 受保護的捲

顯示選定儲存虛擬機器上受保護磁碟區的數量 (佔總磁碟區的數量)。如果您正在查看目標儲存虛擬機，則數位連結代表所選儲存虛擬機的目標磁碟區。

- 未受保護的捲

顯示所選儲存虛擬機器上未受保護的磁碟區的數量。

- 服務

- 類型

顯示在儲存虛擬機器上配置的服務類型。類型可以是網域名稱系統 (DNS) 或網路資訊服務 (NIS)。

- 狀態

顯示服務的狀態，可以是「啟動」 (●)，向下 (●) 或未配置 (●)。

- 網域

顯示 DNS 服務的 DNS 伺服器或 NIS 服務的 NIS 伺服器的完全限定網域名稱 (FQDN)。啟用 NIS 伺服器後，將顯示 NIS 伺服器的活動 FQDN。當 NIS 伺服器被停用時，將顯示所有 FQDN 的清單。

- IP 位址

顯示 DNS 或 NIS 伺服器的 IP 位址。當 NIS 伺服器啟用時，顯示 NIS 伺服器的主用 IP 位址。當 NIS 伺服器被停用時，將顯示所有 IP 位址的清單。

網路介面選項卡

網路介面標籤顯示在選定儲存虛擬機器上建立的資料網路介面 (LIF) 的詳細資訊：

- 網路介面

顯示在選定儲存虛擬機器上建立的介面的名稱。

- 營運狀態

顯示介面的運作狀態，可以是 Up (↑)，向下 (↓) 或未知 (?)。介面的運作狀態由其實體連接埠的狀態決定。

- 行政地位

顯示介面的管理狀態，可以是 Up (↑)，向下 (↓) 或未知 (?)。介面的管理狀態由儲存管理員控制，以便變更配置或進行維護。管理狀態可以與操作狀態不同。但是，如果介面的管理狀態為 Down，則操作狀態預設為 Down。

- IP 位址/WWPN

顯示乙太網路介面的 IP 位址和 FC LIF 的全球連接埠名稱 (WWPN)。

- 協定

顯示為介面指定的資料協定列表，例如 CIFS、NFS、iSCSI、FC/FCoE、FC-NVMe 和 FlexCache。

- 角色

顯示介面角色。角色可以是資料或管理。

- 母港

顯示介面最初關聯的實體連接埠。

- 目前連接埠

顯示介面目前關聯的實體連接埠。如果介面遷移，目前連接埠可能與主連接埠不同。

- 連接埠設定

顯示介面映射到的連接埠集。

- 故障轉移策略

顯示為介面配置的故障轉移策略。對於 NFS、CIFS 和 FlexCache 接口，預設故障轉移策略是下一個可用。故障轉移策略不適用於 FC 和 iSCSI 介面。

- 路由群組

顯示路由組的名稱。您可以透過點擊路由群組名稱來查看有關路由和目標網關的更多資訊。

ONTAP 8.3 或更高版本不支援路由組，因此這些群集會顯示空白列。

- 故障轉移組

顯示故障轉移組的名稱。

qtree 選項卡

Qtrees 標籤顯示有關 qtree 及其配額的詳細資訊。如果要編輯一個或多個 qtree 的 qtree 容量的健康閾值設置，可以點擊「編輯閾值」按鈕。

使用「匯出」按鈕建立逗號分隔值 (.csv) 文件，其中包含所有受監控 qtree 的詳細資訊。匯出至 CSV 檔案時，您可以選擇為目前儲存虛擬機器、目前叢集中的所有儲存虛擬機器或資料中心中所有叢集的所有儲存虛擬機器建立 qtree 報表。在匯出的 CSV 檔案中出現了一些額外的 qtree 欄位。

- 地位

顯示 qtree 的目前狀態。狀態可以是「嚴重」 (❌)，錯誤 (⚠️)，警告 (⚠️) 或正常 (✅)。

您可以將指標移到狀態圖示上，以查看有關為 qtree 產生的事件的更多資訊。

如果 qtree 的狀態由單一事件決定，您可以查看事件名稱、觸發事件的時間和日期、分配事件的管理員的姓名以及事件的原因等資訊。您可以使用*查看詳細資訊*來查看有關該事件的更多資訊。

如果 qtree 的狀態由多個嚴重程度相同的事件決定，則會顯示前三個事件，其中包含事件名稱、觸發事件的時間和日期以及分配該事件的管理員的姓名等資訊。您可以透過點擊事件名稱來查看有關每個事件的更多詳細資訊。您也可以使用*查看所有事件*來查看產生的事件清單。



qtree 可以有多个严重程度相同或不同的事件。但是，仅显示最高严重程度。例如，如果 qtree 有两个事件，严重性分别为“错误”和“警告”，则仅显示“错误”严重性。

- **Qtree**

显示 qtree 的名称。

- **簇**

显示包含 qtree 的簇的名称。仅出现在匯出的 CSV 檔案中。

- **儲存虛擬機器**

显示包含 qtree 的儲存虛擬機器 (SVM) 名称。仅出现在匯出的 CSV 檔案中。

- **體積**

显示包含 qtree 的磁碟区的名称。

您可以將指標移到磁碟区名称上以查看有关该磁碟区的更多资讯。

- **配額設定**

指示 qtree 上是否启用或停用配額。

- **配額類型**

指定配額是針對使用者、使用者群組或 qtree。仅出现在匯出的 CSV 檔案中。

- **使用者或群組**

显示使用者或使用者群组的名称。每个使用者和使用者群组都会有多行。当配額类型为 qtree 或未设定配額時，此列为空。仅出现在匯出的 CSV 檔案中。

- **磁碟使用率%**

显示已使用磁碟空间的百分比。如果设定了磁碟硬限制，则该值基于磁碟硬限制。如果设定的配額没有磁碟硬限制，则该值会基于磁碟区资料空间。如果未设定配額，或 qtree 所属磁碟区上的配額已关闭，则网格式页面中將显示“不适用”，且 CSV 匯出资料中的欄位为空白。

- **磁碟硬限制**

显示为 qtree 分配的最大磁碟空间量。当达到此限制并且不允许进一步的磁碟写入时，Unified Manager 会产生一个严重事件。在下列情况下，该值显示为「Unlimited」：如果设定的配額没有磁碟硬限制、未设定配額或 qtree 所属磁碟区上的配額已关闭。

- **磁碟軟限制**

显示在产生警告事件之前为 qtree 分配的磁碟空间量。在下列情况下，该值显示为「Unlimited」：如果设定的配額没有磁碟軟限制、未设定配額或 qtree 所属磁碟区上的配額为关闭状态。预设情况下，此列是隐藏的。

- **磁碟閾值**

顯示磁碟空間設定的閾值。在下列情況下，該值顯示為「Unlimited」：如果設定的配額沒有磁碟閾值限制、未設定配額或 qtree 所屬磁碟區上的配額已關閉。預設情況下，此列是隱藏的。

- 使用的文件 %

顯示 qtree 中使用的文件的百分比。如果設定了檔案硬限制，則該值會基於檔案硬限制。如果設定的配額沒有檔案硬限制，則不會顯示任何值。如果未設定配額，或 qtree 所屬磁碟區上的配額已關閉，則網格頁面中將顯示“不適用”，且 CSV 匯出資料中的欄位為空白。

- 檔案硬限制

顯示 qtree 上允許的檔案數量的硬限制。在下列情況下，數值顯示為「Unlimited」：如果設定的配額沒有檔案硬限制、未設定配額或 qtree 所屬磁碟區上的配額已關閉。

- 檔案軟限制

顯示 qtree 上允許的檔案數量的軟限制。在下列情況下，該值顯示為「Unlimited」：如果設定了配額而沒有檔案軟限制，如果未設定配額，或如果 qtree 所屬磁碟區上的配額已關閉。預設情況下，此列是隱藏的。

使用者和群組配額選項卡

顯示所選儲存虛擬機器的使用者和使用者群組配額的詳細資訊。您可以查看配額狀態、使用者或使用者群組的名稱、磁碟和檔案上設定的軟硬限制、使用的磁碟空間量和檔案數以及磁碟閾值等資訊。您也可以變更與使用者或使用者群組關聯的電子郵件地址。

- 編輯電子郵件地址指令按鈕

開啟「編輯電子郵件地址」對話框，其中顯示所選使用者或使用者群組的目前電子郵件地址。您可以修改電子郵件地址。如果編輯電子郵件地址欄位為空，則使用預設規則為選定的使用者或使用者群組產生電子郵件地址。

如果多個使用者俱有相同的配額，則使用者名稱將顯示為逗號分隔的值。此外，預設規則不用於產生電子郵件地址；因此，您必須提供發送通知所需的電子郵件地址。

- 設定電子郵件規則指令按鈕

使您能夠建立或修改規則，為儲存虛擬機器上配置的使用者或使用者群組配額產生電子郵件地址。當配額超出時，會向指定的電子郵件地址發送通知。

- 地位

顯示配額的目前狀態。狀態可以是「嚴重」(✖)，警告(⚠)或正常(✔)。

您可以將指標移到狀態圖示上以查看有關為配額產生的事件的事件的更多資訊。

如果配額的狀態由單一事件決定，您可以查看事件名稱、觸發事件的時間和日期、分配事件的管理員的姓名以及事件的原因等資訊。您可以使用*查看詳細資訊*來查看有關該事件的更多資訊。

如果配額的狀態由多個相同嚴重程度的事件決定，則會顯示前三個事件，並顯示事件名稱、觸發事件的時間和日期以及分配事件的管理員的姓名等資訊。您可以透過點擊事件名稱來查看有關每個事件的更多詳細資訊。您也可以使用*查看所有事件*來查看產生的事件清單。



一個配額可以有幾個相同嚴重程度或不同嚴重程度的事件。但是，僅顯示最高嚴重程度。例如，如果配額有兩個事件，嚴重性分別為“錯誤”和“警告”，則僅顯示“錯誤”嚴重性。

- 使用者或群組

顯示使用者或使用者群組的名稱。如果多個使用者俱有相同的配額，則使用者名稱將顯示為逗號分隔的值。

當ONTAP由於 SecD 錯誤而未提供有效的使用者名稱時，該值顯示為「未知」。

- 類型

指定配額是針對使用者還是使用者群組。

- 卷或 qtree

顯示指定了使用者或使用者群組配額的磁碟區或 qtree 的名稱。

您可以將指標移到磁碟區或 qtree 的名稱上，以查看有關該磁碟區或 qtree 的更多資訊。

- 磁碟使用率%

顯示已使用磁碟空間的百分比。如果配額設定時沒有磁碟硬限制，則該值顯示為「不適用」。

- 磁碟硬限制

顯示為配額分配的最大磁碟空間量。當達到此限制並且不允許進一步的磁碟寫入時，Unified Manager 會產生一個嚴重事件。如果配額設定沒有磁碟硬限制，則該值顯示為「無限制」。

- 磁碟軟限制

顯示在產生警告事件之前為配額分配的磁碟空間量。如果配額設定時沒有磁碟軟限制，則該值顯示為「無限制」。預設情況下，此列是隱藏的。

- 磁碟閾值

顯示磁碟空間設定的閾值。如果配額設定沒有磁碟閾值限制，則該值顯示為「無限制」。預設情況下，此列是隱藏的。

- 使用的文件 %

顯示 qtree 中使用的文件的百分比。如果設定的配額沒有檔案硬限制，則該值顯示為「不適用」。

- 檔案硬限制

顯示配額允許的文件數量的硬限制。如果配額設定沒有檔案硬限制，則該值顯示為「無限制」。

- 檔案軟限制

顯示配額允許的文件數量的軟限制。如果配額設定時沒有檔案軟限制，則該值顯示為「無限制」。預設情況下，此列是隱藏的。

- 電子郵件

顯示在配額超出時向其發送通知的使用者或使用群組的電子郵件地址。

NFS 共享選項卡

NFS 共用標籤顯示有關 NFS 共享的信息，例如其狀態、與磁碟區（FlexGroup磁碟區或FlexVol磁碟區）關聯的路徑、用戶端對 NFS 共用的存取等級以及為匯出的磁碟區定義的匯出策略。在下列情況下，將不會顯示 NFS 共用：如果未安裝卷，或與磁碟區的匯出策略關聯的協定不包含 NFS 共用。

- 地位

顯示 NFS 共享的目前狀態。狀態可以是錯誤 (❗) 或正常 (✅)。

- 連接路徑

顯示磁碟區的安裝路徑。如果將明確的 NFS 匯出策略套用至 qtree，則該列將顯示可透過其存取 qtree 的磁碟區的路徑。

- 連線路徑已啟用

顯示訪問已安裝卷的路徑是活動的還是非活動的。

- 卷或 qtree

顯示套用 NFS 匯出策略的磁碟區或 qtree 的名稱。如果將 NFS 匯出策略套用至磁碟區中的 qtree，則該欄位會顯示磁碟區和 qtree 的名稱。

您可以點擊連結在相應詳細資訊頁面中查看有關該物件的詳細資訊。如果物件是 qtree，則會顯示 qtree 和磁碟區的連結。

- 音量狀態

顯示正在匯出的磁碟區的状态。状态可以是離線、線上、受限或混合。

- 離線

不允許對該卷進行讀取或寫入存取。

- 在線的

允許對該卷進行讀寫存取。

- 受限制的

允許進行有限的操作，例如奇偶校驗重建，但不允許存取資料。

- 混合

FlexGroup卷的組成部分並不都處於相同的狀態。

- 安全風格

顯示匯出的磁碟區的存取權限。安全模式可以是 UNIX、統一、NTFS 或混合。

- UNIX (NFS 用戶端)

卷中的檔案和目錄具有 UNIX 權限。

- 統一

卷中的文件和目錄具有統一的安全樣式。

- NTFS (CIFS 用戶端)

磁碟區中的檔案和目錄具有 Windows NTFS 權限。

- 混合

磁碟區中的檔案和目錄可以具有 UNIX 權限或 Windows NTFS 權限。

- **UNIX 權限**

以八進位字串格式顯示為匯出的磁碟區所設定的 UNIX 權限位元。它類似於 UNIX 風格的權限位元。

- **出口政策**

顯示定義匯出磁碟區的存取權限的規則。您可以點擊連結查看與匯出策略相關的規則的詳細信息，例如身份驗證協定和存取權限。

SMB 共享選項卡

顯示有關所選儲存虛擬機器上的 SMB 共享的資訊。您可以查看 SMB 共享的狀態、共享名稱、與儲存 VM 關聯的路徑、共享的連接路徑的狀態、包含物件、包含磁碟區的狀態、共享的安全資料以及為共享定義的匯出策略等資訊。您也可以確定是否存在 SMB 共享的等效 NFS 路徑。



資料夾中的共用不會顯示在 SMB 共用標籤中。

- **查看使用者映射命令按鈕**

啟動使用者映射對話框。

您可以查看儲存虛擬機器的使用者對應的詳細資訊。

- **顯示 ACL 指令按鈕**

啟動共享的存取控制對話框。

您可以查看所選共享的使用者和權限詳細資訊。

- **地位**

顯示共享的目前狀態。狀態可以是正常 (✓) 或錯誤 (!)。

- **共享名稱**

顯示 SMB 共享的名稱。

- 小路

顯示建立共享的連線路徑。

- 連線路徑已啟用

顯示存取共享的路徑是活動的還是非活動的。

- 包含物件

顯示共享所屬的包含物件的名稱。包含的物件可以是磁碟區或 qtree。

透過點擊鏈接，您可以在相應“詳細資料”頁面中查看包含物件的詳細資訊。如果包含的物件是 qtree，則會顯示 qtree 和磁碟區的連結。

- 音量狀態

顯示正在匯出的磁碟區的狀態。狀態可以是離線、線上、受限或混合。

- 離線

不允許對該卷進行讀取或寫入存取。

- 在線的

允許對該卷進行讀寫存取。

- 受限制的

允許進行有限的操作，例如奇偶校驗重建，但不允許存取資料。

- 混合

FlexGroup卷的組成部分並不都處於相同的狀態。

- 安全

顯示匯出的磁碟區的存取權限。安全模式可以是 UNIX、統一、NTFS 或混合。

- UNIX (NFS 用戶端)

卷中的檔案和目錄具有 UNIX 權限。

- 統一

卷中的文件和目錄具有統一的安全樣式。

- NTFS (CIFS 用戶端)

磁碟區中的檔案和目錄具有 Windows NTFS 權限。

- 混合

磁碟區中的檔案和目錄可以具有 UNIX 權限或 Windows NTFS 權限。

- 出口政策

顯示適用於共用的匯出策略的名稱。如果沒有為儲存虛擬機器指定匯出策略，則該值顯示為未啟用。

您可以單擊連結查看與匯出策略相關的規則的詳細信息，例如訪問協議和權限。如果所選儲存虛擬機器的導出策略已停用，則該連結也會停用。

- NFS 等效

指定共用是否存在 NFS 等效項。

SAN 選項卡

顯示所選儲存虛擬機器的 LUN、啟動器群組和啟動器的詳細資訊。預設情況下，顯示 LUN 視圖。您可以在「啟動器群組」標籤中查看有關啟動器群組的詳細信息，在「啟動器」標籤中查看有關啟動器的詳細資訊。

- LUN 選項卡

顯示屬於所選儲存虛擬機器的 LUN 的詳細資訊。您可以查看 LUN 名稱、LUN 狀態（線上或離線）、包含 LUN 的檔案系統（磁碟區或 qtree）的名稱、主機作業系統的類型、LUN 的總資料容量和序號等資訊。LUN 效能列提供了 LUN/效能詳細資訊頁面的連結。

您也可以查看有關 LUN 上是否啟用了精簡設定以及 LUN 是否已對應到啟動程式群組的資訊。如果對應到啟動器，則可以檢視對應到選定 LUN 的啟動器群組和啟動器。

- 發起者群組標籤

顯示有關啟動器組的詳細資訊。您可以查看啟動器群組的名稱、存取狀態、群組中所有啟動器使用的主機作業系統類型以及支援的協定等詳細資訊。點擊訪問狀態列的鏈接，可以查看發起者群組的當前訪問狀態。

- 普通的

啟動器群組連接到多個存取路徑。

- 單路徑

發起者群組連接到單一存取路徑。

- 無路徑

沒有連接到啟動器群組的存取路徑。

您可以查看啟動器群組是否已對應到所有介面或透過連接埠集對應到特定介面。當您按一下「映射介面」列中的計數連結時，將顯示所有介面或顯示連接埠集的特定介面。不顯示透過目標入口網站映射的介面。顯示對應到啟動器群組的啟動器和 LUN 的總數。

您也可以查看已對應到選定啟動程序群組的 LUN 和啟動程序。

- 發起者標籤

顯示選定儲存虛擬機器的啟動器的名稱和類型以及對應到該啟動器的啟動器群組總數。

```
initiator groups that are mapped to the selected initiator group.
```

相關註釋窗格

透過「相關註釋」窗格，您可以查看與所選儲存虛擬機器相關的註釋詳細資訊。詳細資訊包括註釋名稱和應用於儲存虛擬機器的註釋值。您也可以從「相關註釋」窗格中刪除手動註釋。

相關設備窗格

透過「相關設備」窗格，您可以查看與儲存虛擬機器相關的叢集、聚合和磁碟區：

- 簇

顯示儲存虛擬機器所屬叢集的健康狀態。

- 聚合

顯示屬於所選儲存虛擬機器的聚合數量。也會根據最高嚴重程度顯示聚合體的健康狀況。例如，如果儲存虛擬機器包含十個聚合，其中五個顯示「警告」狀態，其餘五個顯示「嚴重」狀態，則顯示的狀態為「嚴重」。

- 指派的聚合

顯示指派給儲存虛擬機器的聚合數量。也會根據最高嚴重程度顯示聚合體的健康狀況。

- 卷

顯示屬於所選儲存虛擬機器的磁碟區的數量和容量。也會根據最高嚴重性等級顯示捲的健康狀況。當儲存虛擬機器中存在FlexGroup磁碟區時，計數還包括 FlexGroup；但不包含FlexGroup組成部分。

相關群組窗格

透過「相關群組」窗格，您可以查看與所選儲存虛擬機器關聯的群組清單。

相關警報窗格

透過「相關警報」窗格，您可以查看為所選儲存虛擬機器建立的警報清單。您也可以透過點擊「新增警報」連結新增警報，或透過點擊警報名稱編輯現有警報。

集群/健康詳情頁面

集群/健康詳情頁面提供有關所選集群的詳細信息，例如健康、容量和配置詳情。您也可以查看有關叢集的網路介面 (LIF)、節點、磁碟、相關設備和相關警報的資訊。

叢集名稱旁邊的狀態（例如「良好」）表示通訊狀態；Unified Manager 是否可以與叢集通訊。它不代表群集的故障轉移狀態或整體狀態。

命令按鈕

命令按鈕可讓您對選取的叢集執行下列任務：

- 切換到效能視圖

使您能夠導航到集群/效能詳細資訊頁面。

- 行動

- 新增警報：開啟新增警報對話框，您可以為選定的叢集新增警報。
- 重新發現：啟動叢集的手動刷新，使 Unified Manager 能夠發現叢集的最新變更。

如果 Unified Manager 與 OnCommand Workflow Automation 配對，則重新發現操作也會從 WFA 重新取得快取資料（如果有）。

重新發現操作啟動後，將顯示指向相關作業詳細資訊的鏈接，以便追蹤作業狀態。

- 註釋：使您能夠註釋選定的叢集。

- 查看集群

使您能夠導航至“健康狀況：所有群集”視圖。

「健康」標籤

顯示有關各種叢集物件（例如節點、SVM 和聚合）的資料可用性和資料容量問題的詳細資訊。可用性問題與叢集物件的資料服務能力有關。容量問題與叢集物件的資料儲存能力有關。

您可以按一下物件的圖表來查看物件的篩選清單。例如，您可以按一下顯示警告的 SVM 容量圖表以查看經過篩選的 SVM 清單。此清單包含具有容量問題且嚴重程度為「警告」的磁碟區或 qtree 的 SVM。您也可以按一下顯示警告的 SVM 可用性圖表，查看存在嚴重程度為「警告」的可用性問題的 SVM 清單。

可用性問題

以圖形方式顯示物件的總數，包括可用性問題的物件和不存在任何可用性相關問題的物件。圖表中的顏色代表問題的不同嚴重程度。圖表下方的資訊提供了有關可能影響或已經影響叢集中資料可用性的可用性問題的詳細資訊。例如，顯示有關已關閉的磁碟架和離線的聚合的資訊。



SFO 條形圖顯示的資料是基於節點的 HA 狀態。所有其他長條圖顯示的數據都是根據生成的事件計算的。

容量問題

以圖形方式顯示物件的總數，包括有容量問題的物件和不存在任何容量相關問題的物件。圖表中的顏色代表問題的不同嚴重程度。圖表下方的資訊提供了有關可能影響或已經影響叢集中資料容量的容量問題的詳細資訊。例如，顯示有關可能違反設定閾值的聚合的資訊。

容量選項卡

顯示有關所選群集容量的詳細資訊。

容量

顯示有關所有已指派聚合的已使用容量和可用容量的資料容量圖：

- 已用邏輯空間

未應用ONTAP儲存效率技術節省的資料在該叢集的所有聚合上儲存的實際資料大小。這不包括 Snapshot 副本。

- 數據縮減

顯示不包含 Snapshot 副本且帶有兩個有效數字的比率，例如 1.8 比 1。此比率基於配置的ONTAP儲存效率設定。

- 用過的

所有聚合上的資料所使用的物理容量。這不包括用於奇偶校驗、正確大小調整和預留的容量。

- 可用的

顯示可用的資料容量。

- 備用零件

顯示所有備用磁碟中可用於儲存的可儲存容量。

- 已配置

顯示為所有底層磁碟區配置的容量。

細節

顯示已使用容量和可用容量的詳細資訊。此計算不包括根聚合資料。

- 總容量

顯示叢集的總容量。這不包括為奇偶校驗分配的容量。

- 用過的

顯示數據使用的容量。這不包括用於奇偶校驗、正確大小調整和預留的容量。

- 可用的

顯示可用的資料容量。

- 已配置

顯示為所有底層磁碟區配置的容量。

- 備用零件

顯示所有備用磁碟中可用於儲存的可儲存容量。

雲層

顯示已使用的雲層總容量，以及在叢集上啟用FabricPool的聚合的每個連接的雲層所使用的容量。FabricPool可以是已授權的，也可以是未經授權的。

按磁碟類型劃分的物理容量

按磁碟類型劃分的實體容量區域顯示有關叢集中各種類型磁碟的磁碟容量的詳細資訊。透過點選磁碟類型，您可以從「磁碟」標籤中查看有關磁碟類型的更多資訊。

- 總可用容量

顯示資料盤的可用容量和剩餘容量。

- 硬碟

圖形化展示叢集中所有HDD資料碟的已使用容量和可用容量。虛線表示HDD中資料盤的剩餘容量。

- 閃光

- SSD數據

圖形化展示叢集中SSD資料碟的已使用容量和可用容量。

- SSD 快取

以圖形方式顯示叢集中SSD快取磁碟的可儲存容量。

- SSD 備件

以圖形方式顯示叢集中SSD、資料和快取磁碟的備用容量。

- 未分配的磁碟

顯示集群中未分配的磁碟數。

具有容量問題的聚合列表

以表格形式顯示存在容量風險問題的聚合的已使用容量和可用容量的詳細資訊。

- 地位

表示聚合具有一定嚴重程度的容量相關問題。

您可以將指標移到狀態上以查看有關聚合生成的事件的更多資訊。

如果聚合的狀態由單一事件決定，則可以查看事件名稱、觸發事件的時間和日期、分配事件的管理員的姓名以及事件的原因等資訊。您可以點擊「查看詳細資料」按鈕以查看有關該事件的更多資訊。

如果聚合的狀態由多個相同嚴重程度的事件決定，則會顯示前三個事件，其中包含事件名稱、觸發事件的時間和日期以及分配事件的管理員的姓名等資訊。您可以透過點擊事件名稱來查看有關每個事件的更多詳細資訊。您也可以點擊「查看所有事件」連結來查看產生的事件清單。



一個聚合可以具有多個嚴重程度相同或不同的容量相關事件。但是，僅顯示最高嚴重程度。例如，如果聚合具有兩個事件，其嚴重性等級分別為“錯誤”和“嚴重”，則僅顯示“嚴重”嚴重性。

- 總計的

顯示聚合的名稱。

- 已使用數據容量

以圖形方式顯示總容量使用情況的資訊（百分比）。

- 滿載天數

顯示聚合達到滿載之前預計剩餘的天數。

“配置”選項卡

顯示有關所選集群的詳細信息，例如 IP 位址、聯絡人和位置：

集群概述

- 管理介面

顯示 Unified Manager 用於連接叢集的叢集管理 LIF。也顯示介面的運作狀態。

- 主機名稱或 IP 位址

顯示 Unified Manager 用於連接叢集的叢集管理 LIF 的 FQDN、簡稱或 IP 位址。

- 完全限定域名 (FQDN)

顯示集群的完全限定域名 (FQDN)。

- OS版本

顯示叢集正在運行的ONTAP版本。如果叢集中的節點運行不同版本的ONTAP，則顯示最早的ONTAP版本。

- 聯絡人

顯示有關叢集出現問題時應聯絡的管理員的詳細資訊。

- 地點

顯示集群的位置。

- 性格

確定這是否是全 SAN 陣列配置的叢集。

遠端集群概述

提供有關MetroCluster配置中遠端叢集的詳細資訊。僅針對MetroCluster配置顯示此資訊。

- 簇

顯示遠端集群的名稱。點擊集群名稱，可以跳到該集群的詳情頁面。

- 主機名稱或 IP 位址

顯示遠端叢集的 FQDN、簡稱或 IP 位址。

- 地點

顯示遠端集群的位置。

MetroCluster概述

提供有關MetroCluster over FC 或MetroCluster over IP 配置中的本地叢集的詳細資訊。僅針對 FC 或 IP 配置的MetroCluster顯示此資訊。

- 類型

顯示MetroCluster類型是雙節點還是四節點。對於MetroCluster over IP，僅支援四節點。

- 配置

顯示透過 FC 和 IP 的MetroCluster配置，可以具有以下值：

對於 FC

- 使用 SAS 纜線的延伸配置
- 使用 FC-SAS 橋接器的延伸配置
- 使用 FC 交換器的結構配置



對於四節點MetroCluster，僅支援具有 FC 交換器的結構配置。

對於 IP

- 使用乙太網路交換器的 IP 配置 (L2 或 L3，取決於叢集的設定方式)
 - 自動排程外切換 (AUSO)

顯示本地群集是否啟用了自動計劃外切換。預設情況下，Unified Manager 中雙節點MetroCluster配置中的所有叢集均啟用 AUSO。您可以使用命令列介面來變更 AUSO 設定。此功能僅支援 FC 上的MetroCluster。

- 切換模式

顯示MetroCluster over IP 配置的切換模式。可用的值有：Active，Negotiated Switchover，

和 Automatic Unplanned Switchover。

節點

- 可用性

顯示已啟動的節點數 (●) 或向下 (●) 在集群中。

- 作業系統版本

顯示節點正在運行的ONTAP版本以及運行特定版本ONTAP的節點數。例如，9.6 (2), 9.3 (1) 指定兩個節點正在執行ONTAP 9.6，一個節點正在執行ONTAP 9.3。

儲存虛擬機

- 可用性

顯示已啟動的 SVM 數量 (●) 或向下 (●) 在集群中。

網路介面

- 可用性

顯示已啟動的非資料 LIF 的數量 (●) 或向下 (●) 在集群中。

- 叢集管理介面

顯示集群管理 LIF 的數量。

- 節點管理介面

顯示節點管理 LIF 的數量。

- 叢集介面

顯示集群 LIF 的數量。

- 集群間接口

顯示集群間 LIF 的數量。

協定

- 數據協定

顯示為叢集啟用的許可資料協定清單。資料協定包括 iSCSI、CIFS、NFS、NVMe 和 FC/FCoE。

保護

- 調解員

顯示集群是否支援中介以及中介的連結狀態。它指示中介是否已配置，如果已配置，則顯示中介的狀態。

- 不適用

當集群不支援中介時顯示。

- 未配置

當叢集支援中介但未配置中介時顯示。

- IP 位址

當叢集支援調解器並且調解器已配置時顯示。調解員狀態透過顏色表示。綠色表示調解器狀態可達。紅色表示調解器狀態不可達。

雲層

列出此叢集所連接的雲層的名稱。它還列出了類型（Amazon S3、Microsoft Azure Cloud、IBM Cloud Object Storage、Google Cloud Storage、Alibaba Cloud Object Storage 或StorageGRID）以及雲層的狀態（可用或不可用）。

MetroCluster 連線選項卡

顯示MetroCluster over FC 配置中的叢集元件的問題和連線狀態。當叢集的災難復原夥伴出現問題時，叢集將顯示在紅色框中。



僅對於採用 FC 上的MetroCluster配置的集群，才會顯示MetroCluster連接選項卡。

您可以透過點選遠端叢集的名稱導航到遠端叢集的詳細資訊頁面。您也可以透過點擊組件的計數連結來查看組件的詳細資訊。例如，點擊叢集中節點的計數鏈接，即可顯示該叢集詳情頁中的節點標籤。點擊遠端集群中磁碟的數量鏈接，將在遠端集群的詳細資訊頁面中顯示磁碟標籤。



管理八節點MetroCluster配置時，按一下磁碟架元件的計數連結僅顯示預設 HA 對的本機磁碟架。此外，無法在另一對 HA 上顯示本地貨架。

您可以將指標移到元件上，以查看出現問題時叢集的詳細資訊和連線狀態，並查看有關該問題產生的事件的更多資訊。

如果元件之間的連線問題的狀態由單一事件決定，您可以查看事件名稱、觸發事件的時間和日期、分配事件的管理員的姓名以及事件的原因等資訊。查看詳細資訊按鈕提供有關該事件的更多資訊。

如果元件之間的連線問題的狀態由多個相同嚴重程度的事件決定，則會顯示前三個事件，其中包含事件名稱、觸發事件的時間和日期以及分配事件的管理員的姓名等資訊。您可以透過點擊事件名稱來查看有關每個事件的更多詳細資訊。您也可以點擊「查看所有事件」連結來查看產生的事件清單。

MetroCluster “複製”選項卡

顯示透過 FC 配置在MetroCluster中複製的資料的狀態。您可以使用MetroCluster Replication 標籤透過與已經對等的叢集同步鏡像資料來確保資料保護。當叢集的災難復原夥伴出現問題時，叢集將顯示在紅色框中。



僅對於採用 FC 上的MetroCluster配置的集群，才會顯示MetroCluster複製選項卡。

在MetroCluster環境中，您可以使用此標籤來驗證本機叢集與遠端叢集的邏輯連線和對等關係。您可以查看集群組件及其邏輯連接的客觀表示。這有助於識別元資料和資料鏡像期間可能出現的問題。

在MetroCluster Replication 標籤中，本地叢集提供所選叢集的詳細圖形表示，而MetroCluster夥伴叢集指的是遠端叢集。

網路介面選項卡

顯示在選定群集上建立的所有非資料 LIF 的詳細資訊。

網路介面

顯示在選定叢集上建立的 LIF 的名稱。

營運狀態

顯示介面的運作狀態，可以是 Up (↑) ， 向下 (↓) 或未知 (?) 。網路介面的運作狀態由其實體連接埠的狀態決定。

行政地位

顯示介面的管理狀態，可以是 Up (↑) ， 向下 (↓) 或未知 (?) 。當您變更設定或進行維護時，您可以控制介面的管理狀態。管理狀態可以與操作狀態不同。但是，如果 LIF 的管理狀態為 Down，則操作狀態預設為 Down。

IP 位址

顯示介面的IP位址。

角色

顯示介面的角色。可能的角色是叢集管理 LIF、節點管理 LIF、叢集 LIF 和叢集間 LIF。

母港

顯示介面最初關聯的實體連接埠。

目前連接埠

顯示介面目前關聯的實體連接埠。LIF 遷移後，目前連接埠可能與主連接埠不同。

故障轉移策略

顯示為介面配置的故障轉移策略。

路由群組

顯示路由組的名稱。您可以透過點擊路由群組名稱來查看有關路由和目標網關的更多資訊。

ONTAP 8.3 或更高版本不支援路由組，因此這些群集會顯示空白列。

故障轉移組

顯示故障轉移組的名稱。

節點選項卡

顯示有關所選集群中的節點的資訊。您可以查看有關 HA 對、磁碟架和連接埠的詳細資訊：

HA 詳細信息

提供 HA 狀態和 HA 對中節點的健康狀況的圖形表示。節點的健康狀態透過以下顏色表示：

- 綠色的
節點處於工作狀態。
- 黃色的
該節點已接管夥伴節點或該節點正面臨一些環境問題。
- 紅色的
節點已關閉。

您可以查看有關 HA 對可用性的資訊並採取必要的措施來防止任何風險。例如，在可能發生接管操作的情況下，會顯示下列訊息：可能發生儲存故障轉移。

您可以查看與 HA 對及其環境相關的事件列表，例如風扇、電源、NVRAM 電池、快閃卡、服務處理器和磁碟架的連接性。您也可以查看事件觸發的時間。

您可以查看其他與節點相關的信息，例如型號。

如果有單節點集群，還可以查看節點的詳細資訊。

磁碟架

顯示有關 HA 對中磁碟架的資訊。

您也可以查看磁碟架和環境元件產生的事件以及事件觸發的時間。

- 貨架編號
顯示磁碟所在機架的 ID。
- 組件狀態

顯示磁碟架的環境詳細資訊，例如電源、風扇、溫度感測器、電流感測器、磁碟連接和電壓感測器。環境詳細資訊顯示為以下顏色的圖示：

- 綠色的
環境組件運作正常。

- 灰色的

沒有關於環境成分的數據。

- 紅色的

一些環境因素已經下降。

- 狀態

顯示磁碟架的狀態。可能的狀態有離線、線上、無狀態、需要初始化、遺失和未知。

- 模型

顯示磁碟架的型號。

- 本機磁碟架

指示磁碟架位於本機叢集還是遠端叢集。此列僅對MetroCluster配置中的叢集顯示。

- 唯一ID

顯示磁碟架的唯一識別碼。

- 韌體版本

顯示磁碟架的韌體版本。

連接埠

顯示有關關聯的 FC、FCoE 和乙太網路連接埠的資訊。您可以透過點擊連接埠圖示來查看有關連接埠和關聯 LIF 的詳細資訊。

您也可以查看為連接埠產生的事件。

您可以查看以下連接埠詳細資訊：

- 連接埠 ID

顯示連接埠的名稱。例如，連接埠名稱可以是 e0M、e0a 和 e0b。

- 角色

顯示連接埠的角色。可能的角色有叢集、資料、叢集間、節點管理和未定義。

- 類型

顯示連接埠使用的實體層協定。可能的類型有乙太網路、光纖通道和 FCoE。

- WWPN

顯示連接埠的全球連接埠名稱 (WWPN)。

- 韌體版本

顯示 FC/FCoE 連接埠的韌體修訂版。

- 地位

顯示連接埠的目前狀態。可能的狀態包括「Up」、「Down」、「Link Not Connected」或「Unknown」(?)。

您可以從事件清單中查看與連接埠相關的事件。您還可以查看關聯的 LIF 詳細信息，例如 LIF 名稱、運行狀態、IP 位址或 WWPN、協定、與 LIF 關聯的 SVM 的名稱、當前連接埠、故障轉移策略和故障轉移群組。

磁碟選項卡

顯示有關所選叢集中磁碟的詳細資訊。可查看已使用磁碟數、備用磁碟數、損壞磁碟數、未分配磁碟數等磁碟相關資訊。您還可以查看其他詳細信息，例如磁碟名稱、磁碟類型和磁碟的所有者節點。

磁碟池摘要

顯示磁碟數量（以有效類型（FCAL、SAS、SATA、MSATA、SSD、NVMe SSD、SSD CAP、Array LUN 和 VMDISK）分類）和磁碟狀態。您還可以查看其他詳細信息，例如聚合、共享磁碟、備用磁碟、損壞磁碟、未分配磁碟和不受支援的磁碟的數量。如果按一下有效磁碟類型計數鏈接，則會顯示所選狀態和有效類型的磁碟。例如，如果按一下磁碟狀態為“Broken”且有效類型為“SAS”的計數鏈接，則會顯示磁碟狀態為“Broken”且有效類型為“SAS”的所有磁碟。

磁碟

顯示磁碟的名稱。

RAID 群組

顯示 RAID 群組的名稱。

所有者節點

顯示磁碟所屬節點的名稱。如果磁碟未分配，則此列中不顯示任何值。

狀態

顯示磁碟的狀態：聚合、共享、備用、損壞、未分配、不受支援或未知。預設情況下，此列會依下列順序排序顯示狀態：損壞、未指派、不支援、備用、聚合和共用。

本機磁碟

顯示「是」或「否」以指示磁碟位於本機叢集還是遠端叢集。此列僅對MetroCluster配置中的叢集顯示。

位置

根據磁碟的容器類型顯示磁碟的位置：例如，副本、資料或奇偶校驗。預設情況下，此列是隱藏的。

受影響的骨材

顯示因磁碟故障而受到影響的聚合數量。您可以將指標移到計數連結上以查看受影響的聚合，然後按一下聚合名稱以查看聚合的詳細資訊。您也可以按一下聚合計數以在「執行狀況：所有聚合」檢視中查看受影響聚合的清單。

在下列情況下，此列不顯示任何值：

- 對於損壞的磁碟，當包含此類磁碟的叢集新增至 Unified Manager 時
- 當沒有故障磁碟時

儲存池

顯示 SSD 所屬的儲存池的名稱。將滑鼠懸停在儲存池名稱上，可以查看該儲存池的詳細資訊。

可儲存容量

顯示可用的磁碟容量。

原始容量

顯示正確調整大小和 RAID 配置之前的原始、未格式化磁碟的容量。預設情況下，此列是隱藏的。

類型

顯示磁碟類型：例如 ATA、SATA、FCAL 或 VMDISK。

有效類型

顯示ONTAP分配的磁碟類型。

對於建立和新增聚合以及備用管理而言，某些ONTAP磁碟類型被視為等效的。ONTAP為每種磁碟類型指派一種有效的磁碟類型。

備用區塊消耗百分比

以百分比顯示 SSD 磁碟中已消耗的備用區塊。對於 SSD 磁碟以外的磁碟，此列為空白。

額定壽命使用 %

根據實際 SSD 使用情況和製造商對 SSD 壽命的預測，以百分比顯示已使用 SSD 壽命的估計值。大於 99 的值表示已消耗了估計的耐久度，但可能不表示 SSD 故障。如果值未知，則省略磁碟。

韌體

顯示磁碟的韌體版本。

轉速

顯示磁碟的每分鐘轉數 (RPM)。預設情況下，此列是隱藏的。

模型

顯示磁碟的型號。預設情況下，此列是隱藏的。

小販

顯示磁碟供應商的名稱。預設情況下，此列是隱藏的。

貨架編號

顯示磁碟所在機架的 ID。

灣

顯示磁碟所在托架的ID。

相關註釋窗格

使您能夠查看與所選集群相關的註釋詳細資訊。詳細資訊包括註釋名稱和應用於叢集的註釋值。您也可以從「相關註釋」窗格中刪除手動註釋。

相關設備窗格

使您能夠查看與選定集群關聯的設備詳細資訊。

詳細資訊包括連接到叢集的設備的屬性，例如設備類型、大小、數量和健康狀態。您可以點擊計數連結對該特定裝置進行進一步分析。

您可以使用MetroCluster合作夥伴窗格來取得遠端MetroCluster合作夥伴及其相關叢集元件（如節點、聚合和SVM）的數量和詳細資訊。MetroCluster合作夥伴窗格僅針對MetroCluster配置中的叢集顯示。

透過「相關設備」窗格，您可以檢視並導覽至與叢集相關的節點、SVM 和聚合：

MetroCluster合作夥伴

顯示MetroCluster夥伴的健康狀況。使用計數鏈接，您可以進一步導航並獲取有關集群組件的健康和容量的信息。

節點

顯示屬於所選集群的節點的數量、容量和健康狀態。容量表示可用容量與可用容量之比。

儲存虛擬機

顯示屬於選定群集的 SVM 的數量。

聚合

顯示屬於所選叢集的聚合的數量、容量和運作狀況。

相關群組窗格

使您能夠查看包含所選集群的群組清單。

相關警報窗格

透過「相關警報」窗格，您可以查看所選集群的警報清單。您也可以透過點擊新增警報連結來新增警報，或透過點擊警報名稱來編輯現有警報。

相關資訊

["卷頁面" "查看集群列表和詳細信息"](#)

聚合/健康詳情頁面

您可以使用聚合/健康詳細資訊頁面查看有關所選聚合的詳細信息，例如容量、磁碟資訊、配置詳細資訊和生成的事件。您也可以查看有關該聚合的相關物件和相關警報的資訊。

命令按鈕



監控啟用FabricPool的聚合時，此頁面上的已提交值和過量提交值僅與本地或效能層容量相關。雲層中可用的空間量未反映在超額承諾的值中。類似地，聚合閾值僅與本地效能層相關。

命令按鈕可讓您對選取的聚合執行下列任務：

- 切換到效能視圖

使您能夠導航至聚合/效能詳細資訊頁面。

- 行動

- 添加警報

使您能夠在選定的聚合中添加警報。

- 編輯閾值

使您能夠修改選定聚合的閾值設定。

- 查看聚合

使您能夠導航至“健康狀況：所有聚合”視圖。

容量選項卡

「容量」標籤顯示有關所選聚合的詳細信息，例如其容量、閾值和每日成長率。

預設情況下，不會為根聚合產生容量事件。此外，Unified Manager 使用的閾值不適用於節點根聚合。只有技術支援代表可以修改產生這些事件的設定。當技術支援代表修改設定時，閾值將應用於節點根聚合。

- 容量

顯示資料容量圖和 Snapshot 副本圖，其中顯示有關聚合的容量詳細資訊：

- 已用邏輯空間

未應用ONTAP儲存效率技術節省的成本，聚合上儲存的資料的實際大小。

- 用過的

聚合中資料使用的物理容量。

- 過度承諾

當聚合中的空間被過度使用時，圖表會顯示一個有過度使用量的標誌。

- 警告

在設定警告閾值的位置顯示一條虛線；表示聚合中的空間已快滿。如果超過此閾值，則會產生空間幾乎已滿事件。

- 錯誤

在設定錯誤閾值的位置顯示一條實線；表示聚合中的空間已滿。如果超出此閾值，則會產生空間已滿事件。

- Snapshot 副本圖

僅當已用快照容量或快照預留不為零時才會顯示此圖。

如果已使用的快照容量超過快照預留，則兩個圖表都會顯示快照容量超過快照預留的容量。

- 雲層

顯示啟用FabricPool的聚合的雲層中資料所使用的空間。FabricPool可以是已授權的，也可以是未經授權的。

當雲層鏡像到另一個雲端提供者（「鏡像層」）時，兩個雲層都會顯示在這裡。

- 細節

顯示有關容量的詳細資訊。

- 總容量

顯示聚合中的總容量。

- 數據容量

顯示聚合使用的空間量（已使用容量）和聚合中的可用空間量（可用容量）。

- 快照儲備

顯示聚合的已使用和可用快照容量。

- 超額承諾的產能

顯示總過量承諾。聚合過量使用使您能夠提供比給定聚合實際可用的更多的儲存空間，只要目前並非所有儲存空間都正在使用。使用精簡配置時，聚合中磁碟區的總大小可能會超過聚合的總容量。



如果您過度使用了聚合，則必須仔細監控其可用空間並根據需要添加存儲，以避免因空間不足而導致寫入錯誤。

- 雲層

顯示啟用FabricPool的聚合的雲層中資料所使用的空間。FabricPool可以是已授權的，也可以是未經授權的。當雲層鏡像到另一個雲端供應商（鏡像層）時，兩個雲層都會顯示在這裡

- 總緩存空間

顯示新增至 Flash Pool 聚合的固態硬碟 (SSD) 或分配單元的總空間。如果您已為聚合啟用 Flash Pool 但尚未新增任何 SSD，則快取空間將顯示為 0 KB。



如果為聚合停用了 Flash Pool，則此欄位將被隱藏。

- 聚合閾值

顯示以下聚合容量閾值：

- 接近滿閾值

指定聚合接近滿的百分比。

- 完整閾值

指定聚合已滿的百分比。

- 接近過度承諾的閾值

指定聚合接近過度承諾的百分比。

- 過度承諾閾值

指定聚合過度承諾的百分比。

- 其他詳情：每日成長率

如果最後兩個樣本之間的變化率持續 24 小時，則顯示聚合中使用的磁碟空間。

例如，如果某個聚合在下午 2 點使用 10 GB 磁碟空間，在下午 6 點使用 12 GB 磁碟空間，則該聚合的每日成長率 (GB) 為 2 GB。

- 音量移動

顯示目前正在進行的捲移動操作的數量：

- 輸出量

顯示正在移出聚合的磁碟區的數量和容量。

您可以單擊該連結以查看更多詳細信息，例如磁碟區名稱、磁碟區移動到的聚合、磁碟區移動操作的狀態以及預計結束時間。

- 收貨量

顯示正在移動到聚合中的磁碟區的數量和剩餘容量。

您可以單擊該連結以查看更多詳細信息，例如磁碟區名稱、移動磁碟區的聚合、磁碟區移動操作的狀態以及預計結束時間。

- 卷移動後的估計已用容量

顯示磁碟區移動作業完成後估計的已使用空間總量（以百分比表示，單位為 KB、MB、GB 等）。

- 容量概覽 - 卷

顯示提供有關聚合中包含的磁碟區容量的資訊的圖表。顯示磁碟區已使用的空間量（已使用容量）和磁碟區中可用空間量（可用容量）。當為精簡配置磁碟區產生「精簡配置磁碟區空間處於風險」事件時，將顯示磁碟區已使用的空間量（已使用容量）以及磁碟區中可用但因聚合容量問題而無法使用的空間量（不可用容量）。

您可以從下拉清單中選擇要查看的圖表。您可以對圖表中顯示的資料進行排序，以顯示已使用大小、已配置大小、可用容量、每日最快成長率和最慢成長率等詳細資訊。您可以根據包含聚合中的磁碟區的儲存虛擬機器 (SVM) 來篩選資料。您也可以查看精簡配置卷的詳細資訊。您可以將遊標放在感興趣的區域上來查看圖表上特定點的詳細資訊。預設情況下，圖表顯示總體排名前 30 的過濾卷。

磁碟資訊選項卡

顯示有關選定聚合中磁碟的詳細信息，包括 RAID 類型和大小以及聚合中使用的磁碟類型。此標籤也以圖形方式顯示 RAID 群組以及所使用的磁碟類型（例如 SAS、ATA、FCAL、SSD 或 VMDISK）。您可以將遊標放在奇偶校驗磁碟和資料磁碟上以查看更多信息，例如磁碟的托架、架子和旋轉速度。

- 數據

以圖形方式顯示有關專用資料磁碟、共用資料磁碟或兩者的詳細資訊。當資料磁碟包含共享磁碟時，顯示共享磁碟的圖形詳細資訊。當資料磁碟包含專用磁碟和共用磁碟時，會同時顯示專用磁碟和共用磁碟的圖形詳情。

- RAID 詳細資料

僅顯示專用磁碟的 RAID 詳細資訊。

- 類型

顯示 RAID 類型（RAID0、RAID4、RAID-DP 或 RAID-TEC）。

- 團體規模

顯示 RAID 群組中允許的最大磁碟數。

- 團體

顯示聚合中的 RAID 群組的數量。

- 使用的磁碟

- 有效類型

顯示聚合中的資料磁碟類型（例如，ATA、SATA、FCAL、SSD 或 VMDISK）。

- 資料磁碟

顯示指派給聚合的資料磁碟的數量和容量。當聚合僅包含共享磁碟時，不會顯示資料磁碟詳細資訊。

- 奇偶校驗磁碟

顯示指派給聚合的奇偶校驗磁碟的數量和容量。當聚合僅包含共用磁碟時，不會顯示奇偶校驗磁碟詳細資料。

- 共享磁碟

顯示指派給聚合的共享資料磁碟的數量和容量。僅當聚合包含共享磁碟時才會顯示共享磁碟詳細資訊。

- 備用磁碟

顯示選定聚合中節點可用的備用資料磁碟的有效類型、數量和容量。



當聚合故障轉移到配對節點時，Unified Manager 不會顯示與聚合相容的所有備用磁碟。

- SSD 快取

提供有關專用快取 SSD 磁碟和共享快取 SSD 磁碟的詳細資訊。

顯示專用快取 SSD 磁碟的以下詳細資訊：

- **RAID** 詳細資料

- 類型

顯示 RAID 類型（RAID0、RAID4、RAID-DP 或 RAID-TEC）。

- 團體規模

顯示 RAID 群組中允許的最大磁碟數。

- 團體

顯示聚合中的 RAID 群組的數量。

- 使用的磁碟

- 有效類型

表示聚合中用於快取的磁碟類型為 SSD。

- 資料磁碟

顯示指派給快取聚合的資料磁碟的數量和容量。

- 奇偶校驗磁碟

顯示指派給聚合用於快取的奇偶校驗磁碟的數量和容量。

- 備用磁碟

顯示選定聚合中可用於快取的節點的備用磁碟的有效類型、數量和容量。



當聚合故障轉移到配對節點時，Unified Manager 不會顯示與聚合相容的所有備用磁碟。

提供共享快取的以下詳細資訊：

- 儲存池

顯示儲存池的名稱。您可以將指標移到儲存池名稱上以查看以下詳細資訊：

- 地位

顯示儲存池的狀態，可以是健康或不健康。

- 總分配

顯示儲存池中的分配單元總數和大小。

- 分配單元大小

顯示儲存池中可指派給聚合的最小空間量。

- 磁碟

顯示用於建立儲存池的磁碟數量。如果儲存池列中的磁碟數量與該儲存池的「磁碟資訊」標籤中顯示的磁碟數量不匹配，則表示一個或多個磁碟損壞，儲存池不健康。

- 已用分配

顯示聚合使用的分配單元的數量和大小。您可以按一下聚合名稱以查看聚合詳細資訊。

- 可用分配

顯示節點可用的分配單元的數量和大小。您可以點擊節點名稱以查看聚合詳細資訊。

- 分配的快取

顯示聚合使用的分配單元的大小。

- 分配單位

顯示聚合使用的分配單元數。

- 磁碟

顯示儲存池中包含的磁碟數量。

- 細節

- 儲存池

顯示儲存池的數量。

- 總大小

顯示儲存池的總大小。

- 雲層

如果您已設定啟用FabricPool的聚合，則顯示雲層的名稱，並顯示已使用的總空間。當雲層鏡像到另一個雲端提供者（鏡像層）時，兩個雲層的詳細資訊都會顯示在這裡

“配置”選項卡

配置標籤顯示有關所選聚合的詳細信息，例如其叢集節點、區塊類型、RAID 類型、RAID 大小和 RAID 群組數量：

- 概述

- 節點

顯示包含選定聚合的節點的名稱。

- 區塊類型

顯示聚合的區塊格式：32 位元或 64 位元。

- RAID類型

顯示 RAID 類型（RAID0、RAID4、RAID-DP、RAID-TEC或混合 RAID）。

- RAID尺寸

顯示 RAID 群組的大小。

- RAID 群組

顯示聚合中的 RAID 群組的數量。

- SnapLock類型

顯示聚合的SnapLock類型。

- 雲層

如果這是啟用FabricPool的聚合，則會顯示雲層的詳細資訊。某些欄位因儲存提供者的不同而不同。當雲層

鏡像到另一個雲端提供者（「鏡像層」）時，兩個雲層都會顯示在這裡。

- 提供者

顯示儲存提供者的名稱，例如StorageGRID、Amazon S3、IBM Cloud Object Storage、Microsoft Azure Cloud、Google Cloud Storage 或 Alibaba Cloud Object Storage。

- Name

顯示由ONTAP建立雲層時的名稱。

- 伺服器

顯示雲層的 FQDN。

- 港口

用於與雲端提供者通訊的連接埠。

- 存取金鑰或帳戶

顯示雲層的存取金鑰或帳戶。

- 容器名稱

顯示雲層的儲存桶或容器名稱。

- SSL

顯示是否為雲層啟用了 SSL 加密。

歷史區

歷史記錄區域顯示提供有關所選聚合容量的資訊的圖表。此外，您可以按一下「匯出」按鈕為您正在查看的圖表建立 CSV 格式的報表。

您可以從歷史記錄窗格頂部的下拉清單中選擇圖表類型。您也可以透過選擇 1 週、1 個月或 1 年來查看特定時間段的詳細資訊。歷史圖表可以幫助您識別趨勢：例如，如果整體使用情況持續突破「接近滿」閾值，您可以採取適當的措施。

歷史圖表顯示以下資訊：

- 已使用總容量（%）

以百分比形式在垂直 (y) 軸上顯示已使用的容量總量和基於使用歷史記錄的容量總量使用趨勢（折線圖）。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下「已使用容量」圖例時，「已使用容量」圖形線將會被隱藏。

- 已使用總容量與總容量

根據使用歷史記錄顯示聚合容量的使用趨勢，以及已使用容量和總容量，以折線圖形式在垂直 (y) 軸上以位元組、千位元組、兆位元組等為單位顯示。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年

的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下「趨勢容量已使用」圖例時，「趨勢容量已使用」圖形線將會被隱藏。

- 已使用總容量 (%) 與已承諾容量 (%)

根據使用歷史記錄顯示聚合容量的使用趨勢，並以折線圖的形式顯示已提交空間（以百分比表示，位於垂直 (y) 軸上）。時間段顯示在水平 (x) 軸上。您可以選擇一周、一個月或一年的時間段。您可以將遊標放在特定區域上以查看圖表上特定點的詳細資訊。您可以透過點選對應的圖例來隱藏或顯示折線圖。例如，當您按一下「已承諾空間」圖例時，「已承諾空間」圖形線將會被隱藏。

事件列表

事件清單顯示有關新事件和已確認事件的詳細資訊：

- 嚴重性

顯示事件的嚴重性。

- 事件

顯示事件名稱。

- 觸發時間

顯示事件產生以來經過的時間。如果時間超過一周，則會顯示事件產生的時間戳記。

相關設備窗格

透過「相關設備」窗格，您可以查看與聚合相關的叢集節點、磁碟區和磁碟：

- 節點

顯示包含聚合的節點的容量和運作狀況。容量表示可用容量與可用容量之比。

- 節點中的聚合

顯示包含選定聚合的叢集節點中所有聚合的數量和容量。也會根據最高嚴重程度顯示聚合體的健康狀況。例如，如果一個叢集節點包含十個聚合，其中五個顯示「警告」狀態，其餘五個顯示「嚴重」狀態，則顯示的狀態為「嚴重」。

- 卷

顯示聚合中的FlexVol捲和FlexGroup磁碟區的數量和容量；數量不包括FlexGroup組成部分。也會根據最高嚴重性等級顯示捲的健康狀況。

- 資源池

顯示與聚合相關的資源池。

- 磁碟

顯示選定聚合中的磁碟數。

相關警報窗格

透過「相關警報」窗格，您可以查看為選定聚合所建立的警報清單。您也可以透過點擊新增警報連結來新增警報，或透過點擊警報名稱來編輯現有警報。

相關資訊

["查看儲存池詳細信息"](#)

保護和恢復數據

建立、監控和排除保護關係故障

Unified Manager 讓您能夠建立保護關係、監控和排除託管叢集上儲存的資料的鏡像保護和備份庫保護故障，並在資料被覆蓋或遺失時還原資料。

SnapMirror保護類型

根據資料儲存拓撲的部署，Unified Manager 可讓您設定多種類型的SnapMirror保護關係。SnapMirror保護的所有變體都提供故障轉移災難復原保護，但在效能、版本靈活性和多備份副本保護方面提供不同的功能。

傳統SnapMirror非同步保護關係

傳統的SnapMirror非同步保護在來源磁碟區和目標磁碟區之間提供區塊複製鏡像保護。

在傳統的SnapMirror關係中，鏡像操作的執行速度比在替代SnapMirror關係中更快，因為鏡像操作是基於區塊複製。但是，傳統的SnapMirror保護要求目標磁碟區在與同一主要版本中的來源磁碟區相同或更高版本的ONTAP軟體下運作（例如，版本 8.x 到 8.x，或 9.x 到 9.x）。不支援從 9.1 來源複製到 9.0 目標，因為目標正在運行早期主要版本。

SnapMirror非同步保護，具有版本靈活的複製

SnapMirror非同步保護與版本靈活的複製功能可在來源磁碟區和目標磁碟區之間提供邏輯複製鏡像保護，即使這些磁碟區在不同版本的ONTAP 8.3 或更高版本軟體下運作（例如，版本 8.3 到 8.3.1、8.3 到 9.1 或 9.2.2 到 9.2）。

在具有版本靈活複製的SnapMirror關係中，鏡像操作的執行速度不如傳統SnapMirror關係中那麼快。

由於執行速度較慢，具有版本靈活複製保護的SnapMirror不適合在以下任一情況下實施：

- 來源物件包含超過 1000 萬個需要保護的檔案。
- 受保護資料的恢復點目標是兩小時或更短。（也就是說，目標必須始終包含鏡像的、可恢復的數據，而這些數據的保存時間不能比來源數據早兩個小時。）

在列出的任何一種情況下，都需要基於更快的區塊複製執行預設SnapMirror保護。

SnapMirror非同步保護，具有版本靈活的複製和備份選項

SnapMirror非同步保護具有版本靈活的複製和備份選項，可在來源磁碟區和目標磁碟區之間提供鏡像保護，並能夠在目標位置儲存鏡像資料的多個副本。

儲存管理員可以指定從來源到目標鏡像哪些 Snapshot 副本，也可以指定在目標保留這些副本多長時間，即使它們在來源中被刪除。

在具有版本靈活複製和備份選項的SnapMirror關係中，鏡像操作的執行速度不如傳統SnapMirror關係中那麼快。

SnapMirror統一複製（鏡像和保管庫）

SnapMirror統一複製可讓您在同一目標磁碟區上設定災難復原和歸檔。與SnapMirror一樣，統一資料保護在第一次呼叫時執行基線傳輸。預設統一資料保護策略「MirrorAndVault」下的基準傳輸會對來源磁碟區進行快照複製，然後將該副本及其引用的資料區塊傳輸到目標磁碟區。與SnapVault一樣，統一資料保護不包括基線中的舊 Snapshot 副本。

SnapMirror同步保護，嚴格同步

SnapMirror同步保護採用「嚴格」同步，確保主磁碟區和輔助磁碟區始終是彼此的真實副本。如果在嘗試將資料寫入輔助磁碟區時發生複製失敗，則用戶端對主磁碟區的 I/O 將會中斷。

SnapMirror同步保護與定期同步

SnapMirror同步保護採用「常規」同步，不要求主磁碟區和輔助磁碟區始終是彼此的真實副本；從而確保主磁碟區的可用性。如果在嘗試將資料寫入輔助磁碟區時發生複製失敗，則主磁碟區和輔助磁碟區將不同步，且用戶端 I/O 將繼續至主磁碟區。



從「健康狀況：所有磁碟區」檢視或「磁碟區/健康狀況詳細資料」頁面監控同步保護關係時，「復原」按鈕和「關係操作」按鈕不可用。

SnapMirror主動同步

SnapMirror主動同步功能在ONTAP 9.8 及更高版本中可用，您可以使用它來保護具有 LUN 的應用程式，使應用程式能夠透明地進行故障轉移，確保在發生災難時業務連續性。

它可讓您從 Unified Manager 發現和監控叢集和儲存虛擬機器上可用的一致性群組 (CG) 的同步SnapMirror關係。AFF叢集或所有 SAN 陣列 (ASA) 叢集均支援SnapMirror主動同步，其中主叢集和輔助叢集可以是AFF或ASA。SnapMirror主動同步使用 iSCSI 或 FCP LUN 保護應用程式。

當您查看受SnapMirror主動同步關係保護的捲和 LUN 時，您可以獲得保護關係、卷清單中的一致性組的統一視圖，查看一致性組關係的保護拓撲，查看長達一年的一致性組關係的歷史資料。您也可以下載該報告。您也可以查看一致性群組關係的摘要、搜尋一致性群組關係的支持，並取得有關受一致性群組保護的磁碟區的資訊。

在「關係」頁面上，您還可以對一致性群組保護的來源和目標儲存物件及其關係進行排序、篩選和擴充保護。

要了解有關SnapMirror主動同步的更多信息，請參閱["Snapmirror 主動同步（以前稱為 SM-BC）的ONTAP 9 文檔"](#)。

在 Unified Manager 中設定保護關係

若要使用 Unified Manager 和OnCommand Workflow Automation設定SnapMirror和SnapVault關係來保護您的數據，您必須執行幾個步驟。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須在兩個叢集或兩個 Storage Virtual Machine (SVM) 之間建立對等關係。
- OnCommand Workflow Automation必須與 Unified Manager 整合：
 - ["設定OnCommand Workflow Automation"](#)。

- ["驗證工作流程自動化中的 Unified Manager 資料來源快取"](#)。

步驟

1. 根據您要建立的保護關係類型，請執行下列操作之一：
 - ["創建SnapMirror保護關係"](#)。
 - ["創建SnapVault保護關係"](#)。
2. 如果要為關係建立策略，請根據要建立的關係類型執行下列其中一項：
 - ["創建SnapVault策略"](#)。
 - ["創建SnapMirror策略"](#)。
3. ["創建SnapMirror或SnapVault計劃"](#)。

設定工作流程自動化和 **Unified Manager** 之間的連接

您可以在OnCommand Workflow Automation (WFA) 和 Unified Manager 之間設定安全連線。連接到工作流程自動化可讓您使用保護功能（例如SnapMirror和SnapVault配置工作流程）以及用於管理SnapMirror關係的命令。

開始之前

- 安裝的工作流程自動化版本必須為 5.1.1P6 或更高版本。



WFA 5.1.1P6 中包含“用於管理 Clustered Data ONTAP 的WFA 套件”，因此無需像過去那樣從 NetAppStorage Automation Store 下載此套件並將其單獨安裝到 WFA 伺服器上。 ["用於管理ONTAP 的WFA 包"](#)

- 您必須擁有在 Unified Manager 中建立的資料庫使用者的名稱才能支援 WFA 和 Unified Manager 連線。
必須已為該資料庫使用者指派整合模式使用者角色。
- 您必須被指派工作流程自動化中的管理員角色或架構師角色。
- 您必須擁有工作流程自動化設定的主機位址、連接埠號碼 443、使用者名稱和密碼。
- 您必須具有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「常規」>「工作流程自動化」。
2. 在「工作流程自動化頁面」的「資料庫使用者」區域中，選擇名稱並輸入您建立的用於支援 Unified Manager 和工作流程自動化連線的資料庫使用者的密碼。
3. 在頁面的*工作流程自動化憑證*區域中，輸入主機名稱或 IP 位址（IPv4 或 IPv6）以及工作流程自動化設定的使用者名稱和密碼。

您必須使用 Unified Manager 伺服器連接埠（連接埠 443）。

4. 點選“儲存”。
5. 如果您使用自簽名證書，請按一下「是」授權安全性證書。

顯示工作流程自動化頁面。

6. 按一下「是」重新載入 Web UI，並新增工作流程自動化功能。

相關資訊

["NetApp文件： OnCommand Workflow Automation \(目前版本\)"](#)

在工作流程自動化中驗證 **Unified Manager** 資料來源緩存

您可以透過檢查工作流程自動化中的資料來源取得是否成功來確定 Unified Manager 資料來源快取是否正常運作。您可以在將工作流程自動化與 Unified Manager 整合時執行此操作，以確保整合後工作流程自動化功能可用。

開始之前

您必須被指派工作流程自動化中的管理員角色或架構師角色才能執行此任務。

步驟

1. 從工作流程自動化 UI 中，選擇 執行 > 資料來源。
2. 右鍵點選 Unified Manager 資料來源的名稱，然後選擇 立即取得。
3. 驗證獲取是否成功且無錯誤。

必須解決取得錯誤才能使工作流程自動化與 Unified Manager 成功整合。

重新安裝或升級**OnCommand Workflow Automation**時會發生什麼情況

在重新安裝或升級OnCommand Workflow Automation之前，您必須先刪除OnCommand Workflow Automation與 Unified Manager 之間的連接，並確保所有目前正在執行或規劃的OnCommand Workflow Automation作業都已停止。

您也必須從OnCommand Workflow Automation中手動刪除 Unified Manager。

重新安裝或升級OnCommand Workflow Automation後，您必須再次建立與 Unified Manager 的連線。

從 **Unified Manager** 中刪除**OnCommand Workflow Automation**設置

當您不再想要使用工作流程自動化時，可以從 Unified Manager 中刪除OnCommand Workflow Automation設定。

開始之前

您必須具有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，按一下左側設定選單中的*常規*>*工作流程自動化*。
2. 在*工作流程自動化*頁面中，點選*刪除設定*。

執行保護關係故障轉移和故障回復

當保護關係中的來源磁碟區因硬體故障或災難而停用時，您可以使用 Unified Manager 中的保護關係功能使保護目標可讀/寫，並故障轉移到該磁碟區，直到來源再次聯機；然後，當原始來源可用於提供資料時，您可以故障還原至原始來源。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須設定 OnCommand Workflow Automation 才能執行此操作。

步驟

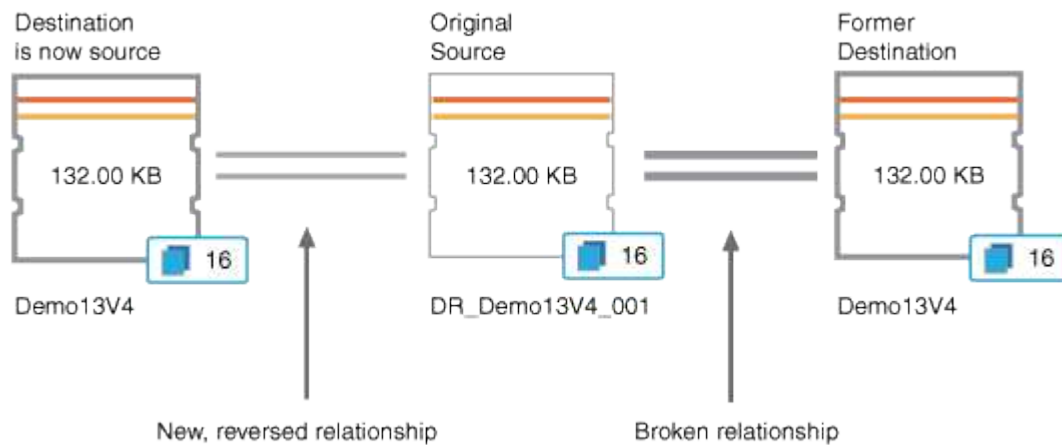
1. "中斷 SnapMirror 關係"。

您必須先中斷該關係，然後才能將目標從資料保護卷轉換為讀/寫卷，然後才能逆轉該關係。

2. "反轉保護關係"。

當原始來源磁碟區再次可用時，您可能決定透過復原來源磁碟區來重新建立原始保護關係。在恢復來源之前，您必須將其與寫入先前目標的資料同步。您可以使用反向重新同步操作來建立新的保護關係，方法是反轉原始關係的角色並將來源磁碟區與先前的目標同步。為新的關係建立一個新的基線 Snapshot 副本。

反向關係看起來類似級聯關係：



3. "中斷反向 SnapMirror 關係"。

當原始來源磁碟區重新同步並可以再次提供資料時，使用中斷操作來中斷反轉關係。

4. "刪除關係"。

當不再需要逆轉的關係時，您應該先刪除該關係，然後再重新建立原始關係。

5. "重新同步關係"。

使用重新同步操作將資料從來源同步到目標並重新建立原始關係。

從磁碟區/運作狀況詳細資料頁面中斷SnapMirror關係

您可以從「磁碟區/運行狀況詳細資料」頁面中斷保護關係，並停止SnapMirror關係中來源磁碟區和目標磁碟區之間的資料傳輸。當您想要遷移資料、進行災難復原或進行應用程式測試時，您可能會中斷關係。目標卷更改為讀寫卷。您不能破壞SnapVault關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 在「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，從拓撲中選擇要中斷的SnapMirror關係。
2. 右鍵單擊目標並從選單中選擇*Break*。

將顯示「中斷關係」對話框。

3. 點擊“繼續”即可斷開關係。
4. 在拓撲中，驗證關係是否中斷。

從卷/健康詳情頁面逆轉保護關係

當災難導致保護關係中的來源卷失效時，您可以在修復或更換來源卷的同時，將目標卷轉換為讀取/寫入卷，以提供資料。當來源再次可以接收資料時，您可以使用反向重新同步操作來建立反向關係，將來源上的資料與讀取/寫入目標上的資料同步。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 該關係不能是SnapVault關係。
- 保護關係必須已經存在。
- 保護關係必須被打破。
- 源和目標都必須在線。
- 來源不能是另一個資料保護卷的目標。
- 執行此任務時，來源上比通用 Snapshot 副本上的資料更新的資料將被刪除。
- 在反向重新同步關係上建立的策略和計劃與原始保護關係上的相同。

如果不存在策略和計劃，則建立它們。

步驟

1. 從「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，在拓撲中找到要反轉來源和目標的SnapMirror關係，然後右鍵單擊它。
2. 從選單中選擇*反向重新同步*。

將顯示“反向重新同步”對話框。

3. 驗證「反向重新同步」對話方塊中顯示的關係是您要執行反向重新同步操作的關係，然後按一下「提交」。

反向重新同步對話方塊關閉，作業連結顯示在磁碟區/健康詳情頁面頂部。

4. *可選：*按一下「磁碟區/健康」詳細資料頁面上的「檢視作業」以追蹤每個反向重新同步作業的狀態。

顯示經過篩選的作業清單。

5. *可選：*按一下瀏覽器上的*後退*箭頭返回*音量/健康*詳細資訊頁面。

當所有作業任務成功完成後，反向重新同步操作就完成了。

從卷/健康詳情頁面中刪除保護關係

您可以刪除保護關係以永久刪除所選來源和目標之間的現有關係：例如，當您想要使用不同的目標建立關係時。此操作將刪除所有元資料並且無法撤銷。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 在「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，從拓撲中選擇要刪除的SnapMirror關係。
2. 右鍵單擊目的地的名稱，然後從選單中選擇“刪除”。

將顯示「刪除關係」對話方塊。

3. 點擊“繼續”以刪除關係。

該關係已從卷/健康詳細資料頁面中刪除。

從卷/健康詳情頁面重新同步保護關係

您可以重新同步已中斷的SnapMirror或SnapVault關係上的數據，然後將目標設為讀/寫，以便來源上的資料與目標上的資料相符。當來源磁碟區上所需的通用 Snapshot 副本被刪除導致SnapMirror或SnapVault更新失敗時，您可能還需要重新同步。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已設定OnCommand Workflow Automation。

步驟

1. 從「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，在拓撲中找到要重新同步的保護關係並右鍵單擊它。
2. 從選單中選擇*重新同步*。

或者，從*操作*選單中，選擇*關係*>*重新同步*以重新同步您目前正在查看詳細資料的關係。

將顯示“重新同步”對話框。

3. 在「重新同步選項」標籤中，選擇傳輸優先權和最大傳輸速率。
4. 按一下「來源快照副本」；然後在「快照副本」欄位中按一下「預設」。

系統彈出「選擇來源Snapshot副本」對話框。

5. 如果您想要指定現有的 Snapshot 副本而不是傳輸預設的 Snapshot 副本，請按一下「現有 **Snapshot** 副本」並從清單中選擇一個 Snapshot 副本。
6. 點選“提交”。

您將返回「重新同步」對話方塊。

7. 如果您選擇了多個要重新同步的來源，請按一下「預設」以選擇要為其指定現有 Snapshot 副本的下一個來源。
8. 按一下「提交」開始重新同步作業。

重新同步作業已啟動，您將返回磁碟區/健康詳細資料頁面，並且頁面頂部會顯示作業連結。

9. *可選：*按一下「磁碟區/健康詳情」頁面上的「檢視作業」以追蹤每個重新同步作業的狀態。

顯示經過篩選的作業清單。

10. *可選：*按一下瀏覽器上的*後退*箭頭返回*音量/健康*詳細資訊頁面。

當所有作業任務成功完成後，重新同步作業即完成。

解決保護作業失敗

此工作流程提供了一個範例，說明如何從 Unified Manager 儀表板識別和解決保護作業失敗。

開始之前

由於此工作流程中的某些任務要求您使用管理員角色登錄，因此您必須熟悉使用各種功能所需的角色。

在這種情況下，您可以造訪儀表板頁面以查看您的保護作業是否有任何問題。在「保護事件」區域，您會注意到有一個「作業終止」事件，顯示磁碟區上出現「保護作業失敗」錯誤。您調查此錯誤以確定可能的原因和潛在的解決方案。

步驟

1. 在儀表板未解決的事件和風險區域的保護事件面板中，按一下*保護作業失敗*事件。



事件的連結文字以以下形式編寫 `object_name:/object_name - Error Name`，例如 `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`。

將顯示失敗的保護作業的事件詳細資訊頁面。

2. 查看「摘要」區域的「原因」欄位中的錯誤訊息，以確定問題並評估潛在的糾正措施。

看"[識別問題並對失敗的保護作業執行糾正措施](#)"。

識別問題並對失敗的保護作業執行糾正措施

您在「事件詳細資料」頁面的「原因」欄位中查看作業失敗錯誤訊息，並確定作業因 Snapshot 副本錯誤而失敗。然後，您可以進入「音量/健康詳細資料」頁面來收集更多資訊。

開始之前

您必須具有應用程式管理員角色。

事件詳細資訊頁面上的原因欄位中提供的錯誤訊息包含有關失敗作業的以下文字：

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

此訊息提供以下資訊：

- 備份或鏡像作業未成功完成。

此作業涉及來源磁碟區之間的保護關係 `cluster2_src_vol2`` 在虛擬伺服器上 ``cluster2_src_svm`` 以及目標卷 ``managed_svc2_vol3`` 在名為 ``cluster3_dst_svm``。

- Snapshot 複製作業失敗 `0426cluster2_src_vol2snap`` 在來源磁碟區上 ``cluster2_src_svm:/cluster2_src_vol2``。

在這種情況下，您可以確定作業失敗的原因和潛在的糾正措施。但是，解決故障需要您存取系統管理員 Web UI 或 ONTAP CLI 命令。

步驟

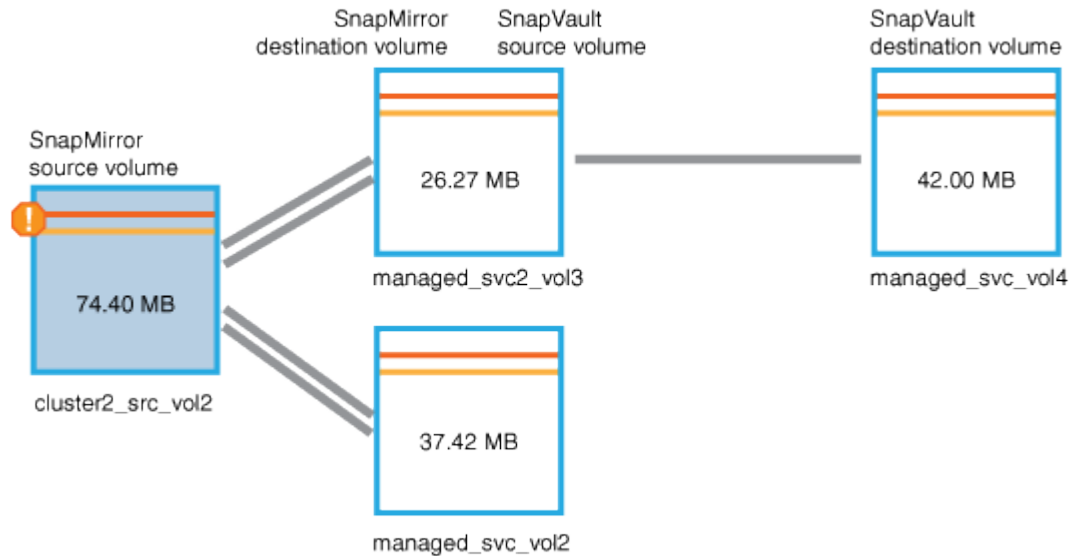
1. 您查看錯誤訊息並確定來源磁碟區上的 Snapshot 複製作業失敗，這表示來源磁碟區可能有問題。
或者，您可以單擊錯誤訊息末尾的“作業詳細資料”鏈接，但出於此場景的目的，您選擇不這樣做。
2. 您決定嘗試解決該事件，因此請執行以下操作：
 - a. 點擊“分配給”按鈕並從選單中選擇“我”。
 - b. 如果為該事件設定了警報，請按一下「確認」按鈕，這樣您就不會繼續收到重複的警報通知。
 - c. 您也可以選擇新增有關該事件的註解。
3. 按一下「摘要」窗格中的「來源」欄位可查看有關來源磁碟區的詳細資訊。

Source 欄位包含來源物件的名稱：在本例中，即計劃執行 Snapshot 複製作業的磁碟區。

音量/健康詳情頁面顯示 cluster2_src_vol2，顯示「保護」標籤的內容。

4. 查看保護拓撲圖，您會看到與拓撲中第一個磁碟區關聯的錯誤圖標，該磁碟區是 SnapMirror 關係的來源磁碟區。

您也會看到來源磁碟區圖示中的水平條，表示為該磁碟區設定的警告和錯誤閾值。



5. 將遊標放在錯誤圖示上，可以看到顯示閾值設定的彈出對話框，並看到磁碟區已超過錯誤閾值，表示存在容量問題。
6. 按一下“容量”標籤。

有關磁碟區的容量資訊 `cluster2_src_vol2` 顯示。

7. 在“容量”面板中，您會看到條形圖中有一個錯誤圖標，再次表明卷容量已超過為該卷設定的閾值水平。
8. 在容量圖下方，您可以看到磁碟區自動增長已停用，並且已設定磁碟區空間保證。

您可以決定啟用自動成長，但出於此場景的目的，您決定在決定如何解決容量問題之前進一步調查。

9. 您向下捲動到「事件」列表，會看到產生了「保護作業失敗」、「捲滿天數」和「磁碟區空間滿」事件。
10. 在*事件*列表中，點擊*卷空間已滿*事件以獲取更多信息，並確定此事件似乎與您的容量問題最相關。

事件詳細資料頁面顯示來源磁碟區的磁碟區空間已滿事件。

11. 在「摘要」區域中，您可以閱讀該事件的「原因」欄位：The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
12. 在摘要區域下方，您可以看到建議的糾正措施。



建議的糾正措施僅針對某些事件顯示，因此您不會看到針對所有類型事件的此區域。

按一下可執行的建議操作清單來解決磁碟區空間已滿事件：

- 在此磁碟區啟用自動增長。
 - 調整捲大小。
 - 在此磁碟區上啟用並執行重複資料刪除。
 - 在此磁碟區上啟用並運行壓縮。
13. 您決定在磁碟區上啟用自動成長，但要做到這一點，您必須確定父聚合上的可用空間和目前磁碟區成長率：
- a. 查看父聚合， `cluster2_src_aggr1` ，在「相關設備」窗格中。



您可以按一下聚合的名稱以取得有關聚合的更多詳細資訊。

您確定聚合具有足夠的空間來啟用磁碟區自動增長。

- b. 在頁面頂部，查看表示關鍵事件的圖示並查看圖示下方的文字。

您確定「滿員天數：少於一天 | 每日成長率：5.4%」。

14. 前往系統管理員或存取ONTAP CLI 以啟用 `volume autogrow` 選項。



記下磁碟區和聚合的名稱，以便在啟用自動增長時可以使用它們。

15. 解決容量問題後，返回 Unified Manager *事件*詳細資料頁面並將事件標記為已解決。

解決滯後問題

此工作流程提供如何解決滯後問題的範例。在這種情況下，您是管理員或操作員，請造訪 Unified Manager Dashboard 頁面以查看您的保護關係是否有問題，如果存在，請尋找解決方案。

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「儀表板」頁面中，您可以查看「未解決的事件和風險」區域，並在「保護風險」下的「保護」窗格中看到 SnapMirror 延遲錯誤。

步驟

1. 在「儀表板」頁面的「保護」窗格中，找到 SnapMirror 關係滯後錯誤並按一下它。

將顯示滯後錯誤事件的事件詳細資訊頁面。

2. 您可以在「*活動*詳細資料」頁面中執行以下一項或多項任務：

- 查看「摘要」區域的「原因」欄位中的錯誤訊息，以確定是否有任何建議的糾正措施。
- 按一下摘要區域的來源欄位中的物件名稱（在本例中為磁碟區）以取得有關該磁碟區的詳細資訊。
- 尋找可能已新增的有關此事件的註釋。
- 為事件新增註釋。
- 將事件指派給特定使用者。

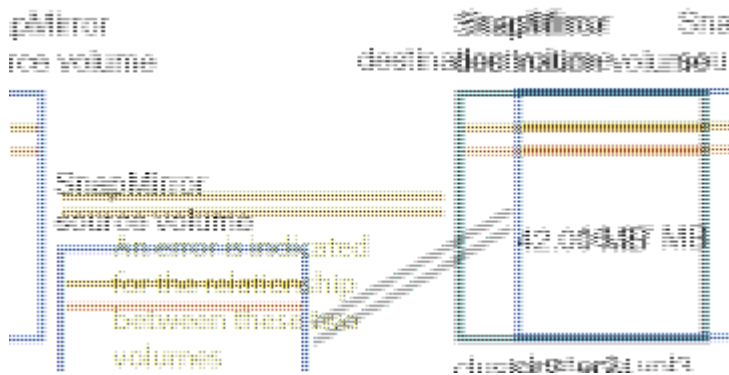
。確認或解決該事件。

3. 在這種情況下，您按一下「**Summary**」區域的「Source」欄位中的物件名稱（在本例中為磁碟區）以取得有關該磁碟區的詳細資訊。

顯示磁碟區/健康詳細資料頁面的保護標籤。

4. 在「保護」標籤中，您可以查看拓撲圖。

您注意到，具有滯後錯誤的磁碟區是三卷SnapMirror級聯中的最後一個磁碟區。您選擇的捲以深灰色勾勒，來源磁碟區的雙橘色線表示SnapMirror關係錯誤。



5. 點擊SnapMirror級聯中的每個磁碟區。

當您選擇每個磁碟區時，摘要、拓撲、歷史記錄、事件、相關設備和相關警報區域中的保護資訊會發生變化，以顯示與所選卷相關的詳細資訊。

6. 您查看*摘要*區域並將遊標放在每個磁碟區的*更新計畫*欄位中的資訊圖示上。

在此場景中，您注意到SnapMirror策略為 DPDefault，並且SnapMirror計劃每小時在整點後的五分鐘更新一次。您意識到關係中的所有磁碟區都在嘗試同時完成SnapMirror傳輸。

7. 為了解決滯後問題，您可以修改兩個級聯磁碟區的計劃，以便每個目標在其來源完成傳輸後開始SnapMirror傳輸。

管理和監控保護關係

Active IQ Unified Manager可讓您建立保護關係、監控和排除託管叢集上的SnapMirror和SnapVault關係故障，以及在資料被覆寫或遺失時復原資料。

對於SnapMirror操作，有兩種複製類型：

- 非同步

從主捲到輔助卷的複製由計劃決定。

- 同步

複製在主磁碟區和輔助磁碟區上同時執行。

您可以同時執行最多 10 項保護作業，而不會對效能產生任何影響。當您同時執行 11 到 30 個作業時，可能會遇到一些效能影響。不建議同時執行超過 30 個作業。

查看卷宗保護狀態

資料保護頁面提供了單一叢集中所有受保護磁碟區或資料中心中所有叢集的資料保護詳細資訊的整體視圖。

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 根據您是否要查看所有受監控集群或單一集群的資料保護狀態，選擇「所有集群」或從下拉式選單中選擇單一集群。
3. 按一下資料保護面板頂部的右箭頭。顯示“資料保護”頁面。

根據您在資料中心中選擇的是單一集群還是所有集群，此頁面顯示受 Snapshot 副本或 SnapMirror 策略保護的捲的資料保護狀態，同時顯示未受保護卷的數量。

從*單一叢集*清單中選擇一個叢集將顯示該叢集中受保護磁碟區的 Snapshot 保護和 SnapMirror 關係狀態。

點擊此頁面上的事件將帶您進入事件詳細資訊頁面。您可以點擊「查看全部」連結以查看事件管理庫存頁面中的所有活動保護事件。您可以將滑鼠懸停在螢幕上以查看相應的計數和圖例。您可以點選：

- 未受保護的捲和受 Snapshot 副本保護的捲的條形圖，可前往「卷」頁面並查看詳細資訊。
- 所有關係的長條圖都轉到「關係」頁面，其中詳細資訊由來源叢集過濾。

查看受 Snapshot 副本保護的捲的保護狀態

Snapshot 副本概述：受 Snapshot 副本保護的捲的概述，例如：

- 受 Snapshot 副本保護和未受 Snapshot 副本保護的捲總數。
- 正在使用或超出 Snapshot 副本的預留空間的磁碟區總數。

*快照副本分析*詳細說明了以下資訊：


- Snapshot 副本的單一事件，包括過去 24 小時內發生的事件。
- 受 Snapshot 副本保護和未受 Snapshot 副本保護的捲的詳細圖表。
- 磁碟區正在使用、未使用以及超出預留的 Snapshot 副本容量。
- 卷的分解是根據其 Snapshot 副本的數量進行的。

Snapshot 副本注意事項

- 為了計算受 Snapshot 副本保護的磁碟區數，需要同時考慮來源磁碟區和目標磁碟區。
- 傳回的 Snapshot 副本數僅適用於處於線上狀態且可用的磁碟區。
- Snapshot 副本數量的圖表範圍是動態的。它是根據所選集群中存在的快照數量生成的。
- 為了將磁碟區視為受保護的，應啟用該磁碟區的 Snapshot 副本計劃。
- Snapshot 副本的預留空間值對於查看已利用的磁碟空間量或計算刪除一個或多個 Snapshot 副本時可以回收

的空間非常重要。

查看SnapMirror關係的保護狀態

- SnapMirror概述*：受SnapMirror策略保護的捲的概述，例如：
- 受相應SnapMirror策略保護的磁碟區數，例如磁碟區SnapMirror關係、儲存 VM 災難復原 (SVM-DR) 及其組合。
- 根據滯後狀態，經歷恢復點目標 (RPO) 滯後的SnapMirror關係總數。
- SnapMirror分析* 詳細說明了以下資訊：
- 針對SnapMirror關係引發的單一事件，包括過去 24 小時內引發的事件
- 每種SnapMirror策略保護的捲數。
- SnapMirror關係型別保護的關係數，例如非同步鏡像、非同步保險庫、非同步 MirrorVault、StricxtSync、SnapMirror活動同步一致性群組和同步。
- 健康和不健康關係的數量。
- 分解成交量關係計數。您可以按 RPO 延遲時間和狀態切換圖表。
- 不受管理的關係的滯後閾值。您可以點選設定圖示 () 配置滯後閾值設定。有關詳細信息，請參閱 "[配置非託管保護關係的滯後閾值設置](#)"。

SnapMirror關係注意事項

- 為了計算SnapMirror關係的數量，將計算已啟用讀取和寫入的來源磁碟區。不考慮目標捲和根卷。
- 對於SnapMirror關係，將顯示來源叢集的事件。
- SnapMirror關係計數包括來源和目標位於相同或不同叢集上的磁碟區的數量。
- 資料複製中 RPO 滯後的滯後持續時間是基於SnapMirror關係。狀態分類為 ok，warning，或者 error，基於關係閾值的設定。您可以查看狀態以確定參數是否按預期工作，或者是否需要解決任何問題。
- 如果磁碟區具有多個SnapMirror關係，則每種關係類型都會被計算為 RPO 延遲。
- 如果來源和目標之間的資料複製存在問題（例如，當關係中斷時），則卷關係被視為不健康。

查看受MetroCluster配置保護的集群

資料保護*頁面上的 MetroCluster保護*面板顯示您的網站上透過 FC 或 IP 設定受MetroCluster保護或未受保護的叢集數量。點擊此面板上的條形圖將轉到「叢集」頁面，其中將根據受保護或不受保護的叢集來過濾叢集詳細資訊。有關監控MetroCluster配置的信息，請參閱"[監控MetroCluster配置](#)"。

查看卷宗保護關係

從「關係：所有關係」視圖和「磁碟區關係」頁面中，您可以查看現有捲SnapMirror和SnapVault關係的狀態。您還可以檢查有關保護關係的詳細信息，包括傳輸和滯後狀態、來源和目標詳細資訊、計劃和策略資訊等。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您也可以從此頁面啟動關係命令。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 從「檢視」功能表中，選擇「關係」>「所有關係」。

關係：顯示所有關係視圖。

3. 選擇以下方式之一來查看磁碟區保護詳細資訊：

- 要查看有關所有捲關係的當前信息，請保留預設的“所有關係”頁面。
- 要查看一段時間內卷宗轉移趨勢的詳細信息，請在「檢視」功能表中選擇「關係：過去 1 個月的轉移狀態視圖」。
- 要查看每天的捲傳輸活動的詳細信息，請在「查看」選單中選擇「關係：過去 1 個月的傳輸率視圖」。



卷傳輸視圖僅顯示非同步關係中的磁碟區的資訊 - 不顯示同步關係中的磁碟區。

監控一致性組關係中的 LUN

如果您的ONTAP環境支援SnapMirror主動同步來保護具有 LUN 的應用程式，則可以在Active IQ Unified Manager上檢視和監控這些 LUN。

SnapMirror主動同步可確保 SAN 環境中故障轉移期間的零復原時間目標 (RTO)。在支援SnapMirror主動同步的典型部署中，磁碟區上的 LUN 受一致性群組關係保護。

這些主 LUN 和從 LUN 是複合 LUN，或具有相同 UUID 和序號的副本 LUN 對。這些複合 LUN 上的來源站點和目標站點之間的 I/O 操作（讀取和寫入）均進行多路復用，以確保透明度。

若要查看複合 LUN，應在 Unified Manager 上新增和發現具有一致性群組關係一部分的 LUN 的主叢集和輔助叢集。僅支援 iSCSI 和 FCP LUN。

有關SnapMirror主動同步的信息，請參閱"[SnapMirror主動同步（以前稱為 SM-BC）的ONTAP 9 文檔](#)"。

若要查看您環境中的複合 LUN，請依照下列步驟操作：

步驟

1. 在左側導覽窗格中，按一下「儲存」>「LUN」。
2. 從「檢視」功能表中，選擇「關係」>「所有 LUN」。

關係：顯示所有 LUN 視圖。

您可以查看 LUN 詳細信息，例如 LUN 名稱、磁碟區、託管 LUN 的儲存 VM、叢集、一致性群組和合作夥伴 LUN。您可以點擊每個組件以深入了解詳細視圖。按一下一致性群組將轉到關係頁面。

點選合作夥伴 LUN 後，您可以在託管合作夥伴 LUN 的儲存虛擬機器的「儲存虛擬機器詳細資料」頁面的「SAN」標籤上查看其配置詳細資料。顯示啟動器、啟動器群組以及合作夥伴 LUN 的其他方面的資訊。

您可以對環境中受保護的 LUN 執行標準網格級功能，包括排序、篩選、產生和上傳報告。

從「Health: All Volumes」檢視建立SnapVault保護關係

您可以使用「運行狀況：所有磁碟區」視圖為同一儲存虛擬機器上的一個或多個磁碟區建立SnapVault關係，以啟用資料備份來保護資料。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示「保護」選單：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在*Health: All Volumes*檢視中，選擇要保護的捲，然後按一下*Protect*。

或者，若要在同一個儲存虛擬機器 (SVM) 上建立多個保護關係，請在「運作狀況：所有磁碟區」檢視中選取一個或多個卷，然後按一下工具列上的「保護」。

3. 從選單中選擇* SnapVault*。

啟動“配置保護”對話框。

4. 按一下 * SnapVault* 查看 * SnapVault* 標籤並配置二級磁碟區資訊。
5. 按一下「進階」根據需要設定重複資料刪除、壓縮、自動成長和空間保證，然後按一下「套用」。
6. 完成「SnapVault」標籤中的「目標資訊」區域和「關係設定」區域。
7. 按一下“應用”。

您將返回「健康狀況：所有磁碟區」視圖。

8. 按一下「Health: All Volumes」檢視頂部的保護配置作業連結。

如果您只建立一個保護關係，則會顯示「作業詳細資料」頁面；但是，如果您建立多個保護關係，則會顯示與保護操作相關的所有作業的篩選清單。

9. 執行下列操作之一：

- 如果您只有一項作業，請按一下「重新整理」以更新與保護設定作業相關的任務清單和任務詳細信息，並確定作業何時完成。
- 如果您有多份工作：
 - i. 按一下作業清單中的一項作業。
 - ii. 點擊“刷新”以更新與保護配置作業相關的任務列表和任務詳細信息，並確定作業何時完成。
 - iii. 使用“返回”按鈕返回過濾清單並查看另一項工作。

從磁碟區/運作狀況詳細資料頁面建立SnapVault保護關係

您可以使用磁碟區/運行狀況詳細資料頁面建立SnapVault關係，以便啟用資料備份來保護磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須設定工作流程自動化才能執行此任務。

在下列情況下不會顯示「保護」選單：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

步驟

1. 在「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，右鍵點選拓撲視圖中要保護的磁碟區。
2. 從選單中選擇*保護*>* SnapVault*。

啟動“配置保護”對話框。

3. 按一下「* SnapVault*」查看「* SnapVault*」選項卡，配置二級資源資訊。
4. 按一下「進階」根據需要設定重複資料刪除、壓縮、自動成長和空間保證，然後按一下「套用」。
5. 完成「配置保護」對話方塊中的「目標資訊」區域和「關係設定」區域。
6. 按一下“應用”。

您將返回「音量/健康」詳細資訊頁面。

7. 按一下「**Volume / Health**」詳細資料頁面頂部的保護配置作業連結。

將顯示「作業詳細資料」頁面。

8. 點擊“刷新”以更新與保護配置作業相關的任務列表和任務詳細信息，並確定作業何時完成。

當作業任務完成時，新的關係將顯示在磁碟區/健康詳細資料頁面拓撲視圖中。

從「Health: All Volumes」檢視建立SnapMirror保護關係

使用「運行狀況：所有磁碟區」視圖，您可以透過在同一儲存虛擬機器上選擇多個磁碟區來一次建立多個SnapMirror保護關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示「保護」選單：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

步驟

1. 在*Health:All Volumes*檢視中，選擇要保護的磁碟區。

或者，若要在同一個 SVM 上建立多個保護關係，請在「執行狀況：所有磁碟區」檢視中選取一個或多個捲，然後按一下工具列上的「保護」>「SnapMirror」。

彈出“配置保護”對話框。

2. 點擊 * SnapMirror* 以查看 * SnapMirror* 標籤並配置目標資訊。
3. 按一下「進階」根據需要設定空間保證，然後按一下「套用」。
4. 完成「SnapMirror」標籤中的「目標資訊」區域和「關係設定」區域。
5. 按一下“應用”。

您將返回「健康狀況：所有磁碟區」視圖。

6. 按一下「健康：所有磁碟區視圖」頂部的保護配置作業連結。

如果您只建立一個保護關係，則會顯示「作業詳細資料」頁面；但是，如果您建立多個保護關係，則會顯示與保護操作相關的所有作業的清單。

7. 執行下列操作之一：

- 如果您只有一項作業，請按一下「重新整理」以更新與保護設定作業相關的任務清單和任務詳細信息，並確定作業何時完成。
- 如果您有多份工作：
 - i. 按一下作業清單中的一項作業。
 - ii. 點擊“刷新”以更新與保護配置作業相關的任務列表和任務詳細信息，並確定作業何時完成。
 - iii. 使用“返回”按鈕返回過濾清單並查看另一項工作。

根據您在配置期間指定的目標 SVM 或在進階設定中啟用的選項，產生的SnapMirror關係可能是以下幾種可能的變更之一：

- 如果您指定的目標 SVM 在與來源磁碟區相同或更新版本的ONTAP下執行，則基於區塊複製的SnapMirror關係是預設結果。
- 如果您指定的目標 SVM 在與來源磁碟區相同或更新版本的ONTAP下運行，但在進階設定中啟用了版本彈性複製，則會產生具有版本靈活複製的SnapMirror關係。
- 如果您指定的目標 SVM 在比來源磁碟區更早的ONTAP版本下運行，並且早期版本支援版本靈活複製，則會自動產生具有版本靈活複製的SnapMirror關係。

從磁碟區/運行狀況詳細資料頁面建立SnapMirror保護關係

您可以使用磁碟區/運行狀況詳細資料頁面建立SnapMirror關係，以便啟用資料複製來保護目的。 SnapMirror複製可讓您在來源磁碟區上發生資料遺失時從目標磁碟區復原資料。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示「保護」選單：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

您可以同時執行最多 10 項保護作業，而不會對效能產生任何影響。當您同時執行 11 到 30 個作業時，可能會遇到一些效能影響。不建議同時執行超過 30 個作業。

步驟

1. 在「磁碟區/健康」詳細資料頁面的「保護」標籤中，在拓撲視圖中以滑鼠右鍵按一下要保護的磁碟區的名稱。
2. 從選單中選擇*保護* > * SnapMirror*。

彈出“配置保護”對話框。

3. 點擊 * SnapMirror* 以查看 * SnapMirror* 標籤並配置目標資訊。
4. 按一下「進階」根據需要設定空間保證，然後按一下「套用」。
5. 完成「配置保護」對話方塊中的「目標資訊」區域和「關係設定」區域。
6. 按一下“應用”。

您將返回「音量/健康」詳細資訊頁面。

7. 按一下「**Volume / Health**」詳細資料頁面頂部的保護配置作業連結。

作業的任務和詳細資料顯示在作業詳細資料頁面中。

8. 在「作業」詳細資料頁面中，按一下「重新整理」以更新與保護設定作業相關的任務列表和任務詳細信息，並確定作業何時完成。
9. 當作業任務完成後，按一下瀏覽器上的*返回*即可返回*Volume / Health*詳細資料頁面。

新的關係顯示在磁碟區/健康詳細資料頁面拓撲視圖中。

根據您在配置期間指定的目標 SVM 或在進階設定中啟用的選項，產生的SnapMirror關係可能是以下幾種可能的變更之一：

- 如果您指定的目標 SVM 在與來源磁碟區相同或更新版本的ONTAP下執行，則基於區塊複製的SnapMirror關係是預設結果。
- 如果您指定的目標 SVM 在與來源磁碟區相同或更新版本的ONTAP下運行，但在進階設定中啟用了版本彈性複製，則會產生具有版本靈活複製的SnapMirror關係。
- 如果您指定的目標 SVM 在ONTAP的早期版本或高於來源磁碟區的版本下運行，且早期版本支援版本靈活複製，則會自動產生具有版本靈活複製的SnapMirror關係。

創建具有版本靈活複製的SnapMirror關係

您可以建立具有版本靈活複製的SnapMirror關係。即使來源磁碟區和目標磁碟區在不同版本的ONTAP下運行，版本靈活的複製也使您能夠實施SnapMirror保護。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 來源 SVM 和目標 SVM 都必須啟用SnapMirror授權。
- 來源 SVM 和目標 SVM 必須分別在支援版本靈活複製的ONTAP軟體版本下運作。

具有版本靈活複製功能的SnapMirror使您即使在並非所有儲存都在一個版本的ONTAP下運行的異質儲存環境中也能實施SnapMirror保護；但是，在具有版本靈活複製功能的SnapMirror下執行的鏡像操作的執行速度不如在傳統區塊複製SnapMirror下那麼快。

步驟

1. 顯示您想要保護的磁碟區的「設定保護」對話方塊。
 - 如果您正在查看「磁碟區/運行狀況詳細資料」頁面的「保護」選項卡，請在具有要保護的磁碟區名稱的拓撲視圖中按一下滑鼠右鍵，然後從功能表中選擇「保護」>「* SnapMirror*」。
 - 如果您正在查看“運行狀況：所有磁碟區”視圖，請找到要保護的磁碟區並右鍵單擊它；然後從選單中選擇“保護”>“SnapMirror”。彈出“配置保護”對話框。
2. 點擊 * SnapMirror* 以查看 * SnapMirror* 標籤。
3. 完成「配置保護」對話方塊中的「目標資訊」區域和「關係設定」區域。

如果您指定的目標 SVM 在比要保護的來源磁碟區更早的ONTAP版本下運行，並且該早期版本支援版本的靈活複製，則此任務會自動使用版本靈活的複製配置SnapMirror。

4. 如果您指定的目標 SVM 與來源磁碟區運行在相同的ONTAP版本下，但仍想使用版本靈活的複製配置SnapMirror，請按一下「進階」以啟用版本靈活的複製，然後按一下「套用」。
5. 按一下“應用”。

您將返回「音量/健康」詳細資訊頁面。

6. 按一下「**Volume / Health**」詳細資料頁面頂部的保護配置作業連結。

作業任務和詳細資料顯示在作業詳細資料頁面中。

7. 在「作業」詳細資料頁面中，按一下「重新整理」以更新與保護設定作業相關的任務列表和任務詳細信息，並確定作業何時完成。
8. 當作業任務完成後，按一下瀏覽器上的*返回*即可返回*Volume / Health*詳細資料頁面。

新的關係顯示在磁碟區/健康詳細資料頁面拓撲視圖中。

使用備份選項建立具有版本靈活複製的SnapMirror關係

您可以建立具有版本靈活複製和備份選項功能的SnapMirror關係。備份選項功能可讓您實

施SnapMirror保護，並在目標位置保留多個版本的備份副本。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 來源 SVM 和目標 SVM 都必須啟用SnapMirror授權。
- 來源 SVM 和目標 SVM 都必須啟用SnapVault授權。
- 來源 SVM 和目標 SVM 必須分別在支援版本靈活複製的ONTAP軟體版本下運作。

配置具有備份選項功能的SnapMirror可讓您使用SnapMirror災難復原功能（例如磁碟區故障轉移功能）保護您的數據，同時提供SnapVault功能（例如多個備份副本保護）。

步驟

1. 顯示您想要保護的磁碟區的「設定保護」對話方塊。
 - 如果您正在查看「磁碟區/運行狀況詳細資料」頁面的「保護」標籤，請在拓撲視圖中以滑鼠右鍵按一下要保護的磁碟區的名稱，然後從功能表中選擇「保護」>「* SnapMirror*」。
 - 如果您正在查看“健康狀況：所有磁碟區”視圖，請找到要保護的捲並右鍵單擊它；然後從選單中選擇“保護”>“SnapMirror”。彈出“配置保護”對話框。
2. 點擊 * SnapMirror* 以查看 * SnapMirror* 標籤。
3. 完成「配置保護」對話方塊中的「目標資訊」區域和「關係設定」區域。
4. 按一下“進階”以顯示“進階目標設定”對話方塊。
5. 如果尚未選取「**Version-Flexible Replication**」複選框，請立即選取它。
6. 選取「使用備份選項」複選框以啟用備份選項功能；然後按一下「套用」。
7. 按一下“應用”。

您將返回「音量/健康」詳細資訊頁面。

8. 按一下「**Volume / Health**」詳細資料頁面頂部的保護配置作業連結。

作業任務和詳細資料顯示在作業詳細資料頁面中。

9. 在「作業」詳細資料頁面中，按一下「重新整理」以更新與保護設定作業相關的任務列表和任務詳細信息，並確定作業何時完成。
10. 當作業任務完成後，按一下瀏覽器上的*返回*即可返回*Volume / Health*詳細資料頁面。

新的關係顯示在磁碟區/健康詳細資料頁面拓撲視圖中。

配置目標效率設定

您可以使用「進階目標設定」對話框在保護目標上配置目標效率設置，例如重複資料刪除、壓縮、自動增長和空間保證。當您想要最大化目標磁碟區或輔助磁碟區的空間使用率時，可以使用這些設定。

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，效率設定與來源磁碟區的設定相匹配，但SnapVault關係中的壓縮設定除外，此設定預設為停用。

步驟

1. 根據您正在設定的關係類型，按一下「設定保護」對話方塊中的「* SnapMirror*」標籤或「* SnapVault*」標籤。
2. 按一下「目標資訊」區域中的「進階」。
將開啟“進階目標設定”對話框。
3. 根據需要啟用或停用重複資料刪除、壓縮、自動成長和空間保證的效率設定。
4. 點擊“應用”儲存您的選擇並返回“配置保護”對話框。

創建SnapMirror和SnapVault計劃

您可以建立基本或進階SnapMirror和SnapVault計劃，以在來源磁碟區或主磁碟區上啟用自動資料保護傳輸，以便傳輸更頻繁或更少地進行，具體取決於磁碟區上資料變更的頻率。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經完成了配置保護對話方塊中的目標資訊區域。
- 您必須設定工作流程自動化才能執行此任務。

步驟

1. 在「配置保護」對話方塊的「SnapMirror」標籤或「SnapVault」標籤中，按一下「關係設定」區域中的「建立計畫」連結。
彈出“建立計畫”對話框。
2. 在「計畫名稱」欄位中，輸入您想要賦予計畫的名稱。
3. 選擇下列選項之一：
 - 基本的
如果您想建立基本間隔式時間表，請選擇。
 - 先進的
如果您想要建立 cron 風格的計畫，請選擇。
4. 按一下“建立”。
新的計畫將顯示在SnapMirror計畫或SnapVault計畫下拉清單中。

建立級聯或扇出關係，以擴展現有保護關係的保護

您可以透過從來源磁碟區建立扇出或從現有關係的目標磁碟區建立級聯來擴展對現有關係

的保護。當您需要將資料從一個網站複製到多個網站或透過建立更多備份來提供額外保護時，您可能會這樣做。

您可以使用一致性群組將保護擴展到卷，一致性群組是一個包含多個磁碟區的容器，以便您可以將所有磁碟區作為一個實體進行管理。您可以在 Unified Manager 的關係頁面中查看 SnapMirror 活動同步一致性群組和同步一致性群組關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 點選*保護* > 關係。或者，您可以從卷詳細資料頁面查看關係。
2. 從「卷關係」頁面中，選擇要擴充保護的 SnapMirror 關係。
3. 在操作列上，按一下「擴充保護」。
4. 在選單中，選擇“從來源”或“從目標”，取決於您是從來源建立磁軌還是從目標建立級聯關係。
5. 根據您正在建立的保護關係類型，選擇「使用 SnapMirror」或「使用 SnapVault」。

將顯示“配置保護”對話框。



這可以從統一關係/卷關係和卷/健康詳細資訊頁面實現。

6. 依照「配置保護」對話方塊中的指示填寫資訊。

從卷關係頁面編輯保護關係

您可以編輯現有的保護關係來變更最大傳輸速率、保護策略或保護計畫。您可以編輯關係以減少用於傳輸的頻寬，或增加計劃傳輸的頻率，因為資料經常變化。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

所選卷必須是保護關係目標。當選擇來源磁碟區、負載共享磁碟區或非 SnapMirror 或 SnapVault 關係目標的磁碟區時，您無法編輯關係。

步驟

1. 在「卷關係」頁面中，在卷清單中選擇同一 SVM 中要編輯關係設定的一個或多個卷，然後從工具列中選擇「編輯」。

將顯示「編輯關係」對話方塊。

2. 在*編輯關係*對話方塊中，根據需要編輯最大傳輸速率、保護策略或保護計畫。
3. 按一下“應用”。

更改將應用於選定的關係。

從卷/健康詳情頁面編輯保護關係

您可以編輯現有的保護關係來變更目前的最大傳輸速率、保護策略或保護計畫。您可以編輯關係以減少用於傳輸的頻寬，或增加計劃傳輸的頻率，因為資料經常變化。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已安裝並設定工作流程自動化。

所選卷必須是保護關係目標。當選擇來源磁碟區、負載共享磁碟區或非SnapMirror或SnapVault關係目標的磁碟區時，您無法編輯關係。

步驟

1. 從「Volume / Health」詳細資料頁面的「Protection」標籤中，在拓撲中找到要編輯的保護關係並右鍵單擊它。
2. 從選單中選擇*編輯*。

或者，從*操作*選單中，選擇*關係*>*編輯*來編輯您目前正在查看詳細資訊的關係。

將顯示「編輯關係」對話方塊。

3. 在「編輯關係」對話方塊中，根據需要編輯最大傳輸速率、保護策略或保護計畫。
4. 按一下“應用”。

更改將應用於選定的關係。

創建SnapMirror策略以最大程度提高傳輸效率

您可以建立SnapMirror策略來指定保護關係的SnapMirror傳輸優先順序。SnapMirror策略可讓您透過指派優先權來最大限度地提高從來源到目標的傳輸效率，以便將較低優先權的傳輸安排在正常優先權的傳輸之後運作。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 此任務假定您已經完成了「設定保護」對話方塊中的「目標資訊」區域。

步驟

1. 在「設定保護」對話方塊的「SnapMirror」標籤中，按一下「關係設定」區域中的「建立原則」連結。
系統彈出「建立SnapMirror策略」對話框。
2. 在「策略名稱」欄位中，輸入您想要賦予策略的名稱。
3. 在*轉移優先權*欄位中，選擇您想要指派給策略的轉移優先權。
4. 在「註釋」欄位中，輸入該策略的選用註解。

5. 按一下“建立”。

新策略顯示在SnapMirror策略下拉清單中。

創建SnapVault策略以最大程度提高傳輸效率

您可以建立新的SnapVault策略來設定SnapVault傳輸的優先順序。您可以使用策略來最大程度地提高保護關係中從主節點到次節點的傳輸效率。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 您必須已經完成了配置保護對話方塊中的目標資訊區域。

步驟

1. 在「配置保護」對話方塊的「SnapVault」標籤中，按一下「關係設定」區域中的「建立政策」連結。

將顯示SnapVault選項卡。

2. 在「策略名稱」欄位中，輸入您想要賦予該策略的名稱。
3. 在*轉移優先權*欄位中，選擇您想要指派給策略的轉移優先權。
4. *可選：*在*註釋*欄位中，輸入該政策的註解。
5. 在「複製標籤」區域中，根據需要新增或編輯複製標籤。
6. 按一下“建立”。

新策略顯示在「建立策略」下拉清單中。

從卷宗關係頁面中止活動資料保護傳輸

當您想要停止正在進行的SnapMirror複製時，可以中止活動資料保護傳輸。您也可以清除基線傳輸之後的傳輸的重新啟動檢查點。當傳輸與其他操作（例如磁碟區移動）衝突時，您可能會中止傳輸。



您無法中止受一致性群組保護的磁碟區關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示中止操作：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

您無法清除基線傳輸的重新啟動檢查點。

步驟

1. 若要中止一個或多個保護關係的傳輸，請從「卷關係」頁面中選擇一個或多個卷，然後在工具列上按一下「中止」。

將顯示「中止傳輸」對話方塊。

2. 如果要清除非基線傳輸的重新啟動檢查點，請選擇*清除檢查點*。
3. 按一下“繼續”。

「中止傳輸」對話方塊關閉，中止作業的狀態顯示在「磁碟區關係」頁面頂部，同時顯示作業詳細資料的連結。

4. 可選：*點擊“*查看詳細資訊”連結前往“工作”詳細資訊頁面以獲取更多詳細資訊並查看工作進度。

從卷/健康詳情頁面中止活動資料保護傳輸

當您想要停止正在進行的SnapMirror複製時，可以中止活動資料保護傳輸。如果不是基準傳輸，您也可以清除傳輸的重新啟動檢查點。當傳輸與其他操作（例如磁碟區移動）衝突時，您可能中止傳輸。



您無法中止受一致性群組保護的磁碟區關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示中止操作：

- 如果 RBAC 設定不允許此操作：例如，如果您只有操作員權限
- 當磁碟區 ID 未知時：例如，當您具有群集間關係且尚未發現目標群集時

您無法清除基線傳輸的重新啟動檢查點。

步驟

1. 在「Volume / Health」詳細資料頁面的「Protection」標籤中，右鍵點選拓撲視圖中要中止的資料傳輸的關係，然後選擇「Abort」。

將顯示「中止傳輸」對話方塊。

2. 如果要清除非基線傳輸的重新啟動檢查點，請選擇*清除檢查點*。
3. 按一下“繼續”。

中止傳輸對話方塊關閉，中止操作的狀態顯示在磁碟區/健康詳細資料頁面的頂部，以及指向作業詳細資料的連結。

4. 可選：*點擊“*查看詳細資訊”連結前往“工作”詳細資訊頁面以獲取更多詳細資訊並查看工作進度。

5. 點擊每個作業任務即可查看其詳細資訊。
6. 點擊瀏覽器上的「後退」箭頭返回*Volume / Health*詳細資訊頁面。

當所有作業任務成功完成後，中止操作就完成了。

從卷關係頁面停止保護關係

在「卷關係」頁面中，您可以暫停保護關係以暫時阻止資料傳輸的發生。當您想要建立包含資料庫的SnapMirror目標磁碟區的 Snapshot 副本時，您可能會停頓關係，並且您希望確保其內容在 Snapshot 副本作業期間保持穩定。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示靜默操作：

- 如果 RBAC 設定不允許此操作；例如，如果您只有操作員權限
- 當磁碟區 ID 未知時；例如，當您具有群集間關係且尚未發現目標群集時
- 當您尚未配對 Workflow Automation 和 Unified Manager 時

步驟

1. 若要使一個或多個保護關係的傳輸處於靜止狀態，請從「卷關係」頁面中選擇一個或多個卷，然後在工具列上按一下「靜止」。

將顯示“靜默”對話框。

2. 按一下“繼續”。

靜默作業的狀態顯示在磁碟區/健康詳情頁面的頂部，同時顯示作業詳情的連結。

3. 點擊「查看詳細資料」連結前往「工作」詳細資料頁面，查看更多詳細資料和工作進度。
4. *選用：*按一下瀏覽器上的*後退*箭頭返回*磁碟區關係*頁面。

當所有作業任務成功完成後，靜默作業即完成。

從卷/健康詳情頁暫停保護關係

您可以停止保護關係以暫時阻止資料傳輸的發生。當您想要建立包含資料庫的SnapMirror目標磁碟區的 Snapshot 副本時，您可能會停頓關係，並且您希望確保其內容在 Snapshot 副本期間保持穩定。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

在下列情況下不會顯示靜默操作：

- 如果 RBAC 設定不允許此操作，例如，如果您只有操作員權限
- 當磁碟區 ID 未知時，例如，當您具有群集間關係且尚未發現目標群集時
- 當您尚未配對 Workflow Automation 和 Unified Manager 時

步驟

1. 在「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，右鍵點選拓撲視圖中要靜止的保護關係的關係。
2. 從選單中選擇*靜默*。
3. 點選“是”繼續。

靜默作業的狀態顯示在磁碟區/健康詳情頁面的頂部，同時顯示作業詳情的連結。

4. 點擊「查看詳細資料」連結前往「工作」詳細資料頁面，查看更多詳細資料和工作進度。
5. 可選：*按一下瀏覽器上的「後退」箭頭返回「*Volume / Health」詳細資料頁面。

當所有作業任務成功完成後，靜默作業即完成。

從卷關係頁面斷開SnapMirror關係

您可以中斷保護關係以停止SnapMirror關係中來源磁碟區和目標磁碟區之間的資料傳輸。當您想要遷移資料、進行災難復原或進行應用程式測試時，您可能會中斷關係。目標卷更改為讀/寫卷。您無法中斷SnapVault關係。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 從「卷關係」頁面中，選擇一個或多個具有要停止資料傳輸的保護關係的捲，然後在工具列上按一下「中斷」。

將顯示「中斷關係」對話框。

2. 點擊“繼續”即可斷開關係。
3. 在「卷關係」頁面中，在「關係狀態*」欄位中驗證關係是否已中斷。

關係狀態列預設是隱藏的，因此您可能需要在顯示/隱藏列清單中選擇它。

從卷關係頁面中刪除保護關係

在「磁碟區關係」頁面中，您可以刪除保護關係以永久刪除所選來源和目標之間的現有關係：例如，當您想要使用不同的目標建立關係時。此操作將刪除所有元資料並且無法撤銷。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 從「卷關係」頁面中，選擇一個或多個要刪除的具有保護關係的捲，然後在工具列上按一下「刪除」。

將顯示「刪除關係」對話方塊。

2. 點擊“繼續”以刪除關係。

該關係已從卷關係頁面中刪除。

從卷關係頁面恢復靜止關係上的計劃傳輸

在您停止關係以停止發生計劃的傳輸後，您可以使用*恢復*重新啟用計劃的傳輸，以便保護來源或主磁碟區上的資料。如果存在檢查點，則在下一個預定的傳輸間隔從檢查點恢復傳輸。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

您可以選擇最多 10 個靜止關係來恢復傳輸。

步驟

1. 從卷*關係*頁面中，選擇一個或多個具有靜止關係的捲，然後在工具列上按一下*恢復*。
2. 在「恢復」對話方塊中，按一下「繼續」。

您將返回到卷宗關係頁面。

3. 若要查看相關的作業任務並追蹤其進度，請按一下「磁碟區關係」頁面上方顯示的作業連結。
4. 執行下列操作之一：
 - 如果僅顯示一個作業，請在「作業詳細資料」頁面中按一下「重新整理」以更新與保護配置作業相關的任務列表和任務詳細信息，並確定作業何時完成。
 - 如果顯示多個作業，
 - i. 在「作業」頁面中，按一下要查看其詳細資料的作業。
 - ii. 在「作業詳細資料」頁面中，按一下「重新整理」以更新與保護配置作業相關的任務列表和任務詳細信息，並確定作業何時完成。作業完成後，資料傳輸將在下一個預定的傳輸間隔恢復。

從卷/健康詳情頁面恢復已暫停關係的預定傳輸

在您停止關係以停止發生計劃的傳輸後，您可以使用磁碟區/健康詳細資料頁面上的*還原*重新啟用計劃的傳輸，以便保護來源或主磁碟區上的資料。如果存在檢查點，則在下一個預定的傳輸間隔從檢查點恢復傳輸。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 在「**Volume / Health**」詳細資訊頁面的「**Protection**」標籤中，在拓樸視圖中右鍵點選要恢復的靜止關係。
或者，從 操作 > 關係 選單中選擇 恢復。
2. 在「恢復」對話方塊中，按一下「繼續」。
您將返回「音量/健康」詳細資訊頁面。
3. 若要查看相關的工作任務並追蹤其進度，請按一下「**Volume / Health**」詳細資料頁面頂部顯示的作業連結。
4. 在「作業」詳細資料頁面中，按一下「重新整理」以更新與保護設定作業相關的任務列表和任務詳細信息，並確定作業何時完成。

作業完成後，資料傳輸將在下一個預定的傳輸間隔恢復。

從磁碟區關係頁面初始化或更新保護關係

在「卷宗關係」頁面中，您可以對新的保護關係執行首次基線傳輸，或者如果關係已經初始化並且您想要執行手動、非計劃增量更新以立即傳輸，則可以更新關係。



您無法初始化或更新受一致性群組保護的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已設定OnCommand Workflow Automation。

步驟

1. 在「卷關係」頁面上，右鍵單擊一個卷並選擇一個或多個具有要更新或初始化的關係的捲，然後在工具列上按一下「初始化/更新」。
將顯示“初始化/更新”對話框。
2. 在「傳輸選項」標籤中，選擇傳輸優先權和最大傳輸速率。
3. 按一下「來源快照副本」；然後在「快照副本」欄位中按一下「預設」。
系統彈出「選擇來源Snapshot副本」對話框。
4. 如果您想要指定現有的 Snapshot 副本而不是傳輸預設的 Snapshot 副本，請按一下「現有 **Snapshot** 副本」並從清單中選擇一個 Snapshot 副本。
5. 點選“提交”。

您將返回*初始化/更新*對話框。

6. 如果您選擇了多個來源進行初始化或更新，請按一下「預設」以選擇要為其指定現有 Snapshot 副本的下一個來源。
7. 按一下「提交」開始初始化或更新作業。

初始化或更新作業已啟動，您將返回捲關係頁面，並且頁面頂部會顯示作業連結。

8. *可選：*按一下*Health: All Volumes*視圖上的*View Jobs*來追蹤每個初始化或更新作業的狀態。

顯示經過篩選的作業清單。

9. *可選：*按一下每個作業以查看其詳細資訊。

10. *選用：*按一下瀏覽器上的*後退*箭頭返回*磁碟區關係*頁面。

當所有任務成功完成後，初始化或更新操作就完成了。

從卷/健康詳情頁面初始化或更新保護關係

您可以對新的保護關係執行首次基線傳輸，或者如果關係已初始化並且您想要執行手動、非計劃增量更新以立即傳輸數據，則更新關係。

注意：您無法初始化或更新受一致性群組保護的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已設定OnCommand Workflow Automation。

步驟

1. 從「**Volume / Health**」詳細資料頁面的「**Protection**」標籤中，在拓撲中找到要初始化或更新的保護關係，然後右鍵單擊它。
2. 從選單中選擇*初始化/更新*。

或者，從*操作*選單中，選擇*關係*>*初始化/更新*來初始化或更新您目前正在查看詳細資訊的關係。

將顯示“初始化/更新”對話框。

3. 在「傳輸選項」標籤中，選擇傳輸優先權和最大傳輸速率。
4. 按一下「來源快照副本」；然後在「快照副本」欄位中按一下「預設」。

系統彈出「選擇來源Snapshot副本」對話框。

5. 如果您想要指定現有的 Snapshot 副本而不是傳輸預設的 Snapshot 副本，請按一下「現有 **Snapshot** 副本」並從清單中選擇一個 Snapshot 副本。
6. 點選“提交”。

您將返回初始化/更新對話框。

7. 如果您選擇了多個來源進行初始化或更新，請按一下「預設」以選擇下一個要為其指定現有 Snapshot 副本的讀取/寫入來源。

您不能為資料保護磁碟區選擇不同的 Snapshot 副本。

8. 按一下「提交」開始初始化或更新作業。

初始化或更新作業已啟動，您將返回捲/健康詳細資料頁面，並且頁面頂部會顯示作業連結。

9. *可選：*按一下「磁碟區/健康」詳細資料頁面上的「檢視作業」以追蹤每個初始化或更新作業的狀態。

顯示經過篩選的作業清單。

10. *可選：*按一下每個作業以查看其詳細資訊。

11. 可選：*按一下瀏覽器上的「後退」箭頭返回「*Volume / Health」詳細資料頁面。

當所有作業任務成功完成後，初始化或更新操作就完成了。

從磁碟區關係頁面重新同步保護關係

在「磁碟區關係」頁面中，您可以重新同步關係，以便從停用來源磁碟區的事件中恢復，或者當您想要將目前來源變更為其他磁碟區時。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。

步驟

1. 從「卷關係」頁面中，選擇一個或多個具有靜止關係的捲，然後從工具列中按一下「重新同步」。

將顯示“重新同步”對話框。

2. 在「重新同步選項」標籤中，選擇傳輸優先權和最大傳輸速率。
3. 按一下「來源快照副本」；然後在「快照副本」欄位中按一下「預設」。

系統彈出「選擇來源Snapshot副本」對話框。

4. 如果您想要指定現有的 Snapshot 副本而不是傳輸預設的 Snapshot 副本，請按一下「現有 **Snapshot** 副本」並從清單中選擇一個 Snapshot 副本。
5. 點選“提交”。

您將返回「重新同步」對話方塊。

6. 如果您選擇了多個要重新同步的來源，請按一下「預設」以選擇要為其指定現有 Snapshot 副本的下一個來源。
7. 按一下「提交」開始重新同步作業。

重新同步作業已啟動，您將返回「磁碟區關係」頁面，並且頁面頂部會顯示作業連結。

8. *選用：*按一下「磁碟區關係」頁面上的「檢視作業」以追蹤每個重新同步作業的狀態。

顯示經過篩選的作業清單。

9. *選用：*按一下瀏覽器上的*後退*箭頭返回*磁碟區關係*頁面。

當所有作業任務成功完成後，重新同步操作就完成了。

從「卷關係」頁面反向保護關係

當災難導致保護關係中的來源卷失效時，您可以在修復或更換來源卷的同時，將目標卷轉換為讀取/寫入卷，以提供資料。當來源再次可以接收資料時，您可以使用反向重新同步操作來建立反向關係，將來源上的資料與讀取/寫入目標上的資料同步。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已經設定了工作流程自動化。
- 該關係不能是SnapVault關係。
- 保護關係必須已經存在。
- 保護關係必須被打破。
- 源和目標都必須在線。
- 來源不能是另一個資料保護卷的目標。
- 執行此任務時，來源上比通用 Snapshot 副本上的資料更新的資料將被刪除。
- 在反向重新同步關係上建立的策略和計劃與原始保護關係上的相同。

如果不存在策略和計劃，則建立它們。

步驟

1. 從「卷關係」頁面中，選擇一個或多個要反轉關係的捲，然後在工具列上按一下「反轉重新同步」。

將顯示“反向重新同步”對話框。

2. 驗證「反向重新同步」對話方塊中顯示的關係是您要執行反向重新同步操作的關係，然後按一下「提交」。

反向重新同步操作啟動後，您將返回磁碟區關係頁面，並在頁面頂部顯示作業連結。

3. *選用：*按一下「磁碟區關係」頁面上的「檢視作業」以追蹤每個反向重新同步作業的狀態。

顯示與此操作相關的作業的過濾清單。

4. *選用：*按一下瀏覽器上的*後退*箭頭返回*磁碟區關係*頁面。

當所有作業任務成功完成後，反向重新同步操作就完成了。

使用捲和卷/健康詳細資料頁面恢復數據

您可以使用磁碟區和磁碟區/執行狀況詳細資料頁面上的還原功能從 Snapshot 副本還原已

覆寫或刪除的檔案、目錄或整個磁碟區。

開始之前

您必須具有應用程式管理員或儲存管理員角色。



請注意以下幾點：

- 您無法恢復 NTFS 檔案流。
- 在以下情況下，恢復選項不可用：
 - 卷 ID 未知：例如，當您具有群集間關係且尚未發現目標群集時。
 - 該磁碟區配置為SnapMirror同步複製。

步驟

1. 從左側導覽窗格，前往*儲存>磁碟區*。
2. 選擇磁碟區並點選“恢復”按鈕。或者，按一下磁碟區前往*磁碟區/健康詳情>操作>復原*。系統彈出“恢復”對話框。有關此頁面的信息，請參閱["恢復對話框"](#)。
3. 如果與預設值不同，請選擇要從中還原資料的磁碟區和 Snapshot 副本。
4. 選擇要還原的項目，例如來源 LUN。

您可以還原整個磁碟區，也可以指定要復原的資料夾和檔案。

5. 選擇要將選取項目還原到的位置：原始位置*或*備用現有位置。
6. 如果選擇備用現有位置，請執行下列其中一項操作：
 - 在「恢復路徑」文字欄位中，鍵入要恢復資料的位置的路徑，然後按一下「選擇目錄」。
 - 按一下「瀏覽」啟動「瀏覽目錄」對話方塊並完成以下步驟：
 - i. 選擇要還原到的目標叢集、儲存虛擬機器 (SVM) 和磁碟區。
 - ii. 在名稱表中，選擇要還原的目錄名稱。
 - iii. 按一下“選擇目錄”。
7. 按一下“恢復”。

恢復過程開始。在後端建立一個作業來完成復原過程。

8. 如果您想查看作業進度，請從左側導覽窗格導覽至*保護>作業*，從作業清單中查看還原作業的狀態。



如果Cloud Volumes ONTAP HA 叢集之間的還原操作因 NDMP 錯誤而失敗，則可能需要在目標叢集中新增明確的 AWS 路由，以便目標可以與來源系統的叢集管理 LIF 進行通訊。您可以使用NetApp Console執行此設定步驟。

什麼是資源池

資源池是由儲存管理員使用 Unified Manager 建立的聚合群組，用於為合作夥伴應用程式提供備份管理的配置。

您可以根據效能、成本、實體位置或可用性等屬性來匯集資源。透過將相關資源分組到一個池中，您可以將該池視為一個單獨的單元進行監控和配置。這簡化了這些資源的管理，並允許更靈活、更有效地使用儲存。

在二級儲存配置期間，Unified Manager 使用下列標準來確定資源池中最適合保護的聚合：

- 此聚合是資料聚合（不是根聚合）並且處於線上狀態。
- 聚合位於目標叢集節點上，其ONTAP版本與來源叢集主版本相同或更高。
- 此聚合具有資源池中所有聚合中最大的可用空間。
- 配置目標磁碟區後，聚合空間處於為聚合定義的接近滿和接近過量使用的閾值內（全域或本地閾值，以適用者為準）。
- 目標節點上的FlexVol磁碟區數量不得超過平台限制。

建立資源池

您可以使用「建立資源池」對話方塊對聚合進行分組以用於配置目的。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

步驟

資源池可以包含來自不同叢集的聚合，但同一個聚合不能屬於不同的資源池。

1. 在左側導覽窗格中，按一下「保護」>「資源池」。
2. 在「資源池」頁面中，按一下「建立」。
3. 依照「建立資源池」對話方塊中的說明提供名稱和描述，並將聚合作為成員新增至要建立的資源池中。

編輯資源池

當您想要變更資源池名稱和描述時，您可以編輯現有的資源池。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

僅當選擇資源池時，「編輯」按鈕才可用。如果選擇了多個資源池，則「編輯」按鈕將被停用。

步驟

1. 在左側導覽窗格中，按一下「保護」>「資源池」。
2. 從清單中選擇一個資源池。
3. 按一下“編輯”。

將顯示「編輯資源池」視窗。

4. 根據需要編輯資源池名稱和描述。
5. 點選“儲存”。

資源池清單中顯示新的名稱和描述。

查看資源池清單

您可以使用資源池頁面查看資源池庫存並監控每個資源池的剩餘容量。

開始之前

您必須具有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「保護」>「資源池」。

顯示資源池庫存。

新增資源池成員

資源池由多個成員聚合組成。您可以將聚合新增至現有資源池，以增加可用於二級磁碟區配置的空間量。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

一次最多可以向資源池新增 200 個聚合。「聚合」對話方塊中顯示的聚合不屬於任何其他資源池。

步驟

1. 在左側導覽窗格中，按一下「保護」>「資源池」。
2. 從「資源池」清單中選擇一個資源池。

資源池成員顯示在資源池清單下方區域。

3. 在資源池成員區，按一下*新增*。

將顯示“聚合”對話框。

4. 選擇一個或多個聚合。
5. 按一下“新增”。

對話方塊關閉並且聚合顯示在所選資源池的成員清單中。

從資源池移除聚合

您可以從現有資源池中刪除聚合：例如，當您想要將聚合用於其他目的時。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

僅當選擇資源池時才會顯示資源池成員。

步驟

1. 在左側導覽窗格中，按一下「保護」>「資源池」。
2. 選擇要從中刪除成員聚合的資源池。

成員聚合清單顯示在「成員」窗格中。

3. 選擇一個或多個聚合。

*刪除*按鈕已啟用。

4. 按一下“刪除”。

將顯示一個警告對話框。

5. 點選“是”繼續。

選定的聚合將從成員窗格中刪除。

刪除資源池

當不再需要資源池時，您可以刪除它。例如，您可能想要將成員聚合從一個資源池重新指派到其他幾個資源池，從而使原始資源池變得過時。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

僅當選擇至少一個資源池時，「刪除」按鈕才可用。

步驟

1. 在左側導覽窗格中，按一下「保護」>「資源池」。
2. 選擇要刪除的資源池。
3. 按一下“刪除”。

此資源池從資源池清單中刪除，其聚合也從成員清單中刪除。

監控儲存虛擬機器災難復原保護關係

Active IQ Unified Manager支援監控儲存虛擬機器災難復原關係，從而以儲存虛擬機器層級提供災難復原。儲存虛擬機器災難復原可以恢復儲存虛擬機器組成磁碟區中存在的資料以及復原儲存虛擬機器配置。

從來源儲存虛擬機器到目標儲存虛擬機器建立儲存虛擬機器 DR 關係，以提供非同步災難復原。您可以根據叢集設定選擇複製儲存虛擬機器配置的全部或部分（不包括網路和協定配置）以及資料磁碟區。

配置儲存虛擬機器災難復原關係後，當來源儲存虛擬機器因硬體故障或環境災難而變得不可用時，目標儲存虛擬機器將啟動，以提供資料存取的最小中斷。類似地，當來源儲存虛擬機器可用時，它會與目標儲存虛擬機器重新同步，然後來源重新啟動以提供資料。您可以使用SnapMirror指令來設定和管理儲存虛擬機器災難復原關係。

使用「關係」頁面監控儲存虛擬機

您可以從 INVENTORY 的 PROTECTION 部分中的關係頁面監控您的儲存 VM 災難復原關係。預設情況下，關係頁面僅列出頂級關係，因為套用了組成關係過濾器。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您可以使用篩選器來查看儲存虛擬機器災難復原關係。

步驟

1. 在左側導覽窗格中，按一下「保護」>「關係」。

此頁面顯示所有類型的關係：磁碟區、一致性群組和儲存虛擬機器關係。

2. 按一下“篩選器”，然後選擇“關係物件類型”和“儲存虛擬機器”以僅查看儲存虛擬機器災難復原關係。
3. 按一下“套用過濾器”。



您應該清除組成關係過濾器以查看所有保護關係。

此頁面僅展示儲存虛擬機器容災關係。

從儲存虛擬機器頁面查看保護關係

使用儲存虛擬機器頁面，您可以查看現有儲存虛擬機器的災難復原關係的狀態。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

您還可以檢查保護關係的詳細信息，包括傳輸和滯後狀態、來源和目標詳細資訊。您可以安排報告或以所需的格式下載現有報告。使用“顯示/隱藏”按鈕可以將所需的列新增到報表中，因為預設情況下它們不會顯示。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 從 **VIEW** 選單中，選擇 **Relationship > All Relationships**。

關係：所有關係視圖顯示所有已設定的儲存虛擬機器。

根據保護狀態查看儲存虛擬機

您可以使用清單的「儲存虛擬機」頁面查看Active IQ Unified Manager中的所有儲存虛擬機，並根據其保護狀態篩選儲存虛擬機。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

儲存虛擬機器視圖中新增了一個新的欄位“保護角色”，提供有關儲存虛擬機器是否受保護或不受保護的資訊。



如果未將來源叢集新增至Active IQ Unified Manager，則與該叢集相關的所有資訊在網格中均不可用。

步驟

1. 在左側導覽窗格中，按一下「儲存」 > 「儲存虛擬機器」。
2. 從 **VIEW** 選單中，選擇 **Health > All Storage VMs**。

顯示健康狀況：所有儲存虛擬機器。

3. 按一下「篩選器」以查看以下儲存虛擬機器之一。

查看	過濾值
受保護的儲存虛擬機	保護角色 是 受保護
未受保護的儲存虛擬機	保護角色*處於*未受保護狀態



您不能同時查看受保護和不受保護的儲存虛擬機器。您需要清除現有過濾器才能重新套用新的過濾器選項。

4. 按一下“套用過濾器”。

未儲存視圖可根據您的篩選器選擇顯示所有受儲存虛擬機器災難復原保護或不受保護的儲存虛擬機器。

了解儲存虛擬機器關聯

儲存虛擬機器（儲存 VM）關聯是從來源儲存 VM 到目標儲存 VM 的映射，合作夥伴應用程式使用它來進行資源選擇和輔助磁碟區配置。

無論目標儲存虛擬機器是二級目標還是三級目標，都會在來源儲存虛擬機器和目標儲存虛擬機器之間建立關聯。您不能使用二級目標儲存虛擬機器作為來源來建立與三級目標儲存虛擬機器的關聯。

身為應用程式管理員或儲存管理員，您可以在*保護* > *儲存虛擬機器關聯*頁面上查看您環境中的儲存虛擬機器關聯。

您可以透過三種方式關聯 SVM：

- 關聯任何儲存虛擬機器：您可以在任何主來源儲存虛擬機器和一個或多個目標 SVM 之間建立關聯。這意味著目前需要保護的所有現有 SVM 以及將來建立的任何 SVM 都與指定的目標 SVM 相關聯。例如，您可能希望將來自不同位置的多個不同來源的應用程式備份到一個位置的一個或多個目標 SVM。
- 關聯特定儲存虛擬機器：您可以在特定來源儲存虛擬機器和一個或多個特定目標 SVM 之間建立關聯。例如，如果您為許多用戶端提供儲存服務，而這些用戶端的資料必須彼此分開，則可以選擇此選項將特定的來源儲存虛擬機器與僅指派給該用戶端的特定目標儲存虛擬機器關聯。
- 與外部儲存虛擬機器關聯：您可以在來源儲存虛擬機器和目標儲存虛擬機器的外部靈活磁碟區之間建立關聯。

建立儲存虛擬機器關聯

建立儲存虛擬機器關聯精靈可讓合作夥伴保護應用程式能夠將來源儲存虛擬機器與目標儲存虛擬機器關聯，以便與SnapMirror和SnapVault關係一起使用。合作夥伴應用程式在初始配置目標磁碟區時使用這些關聯來決定選擇哪些資源。 dd

開始之前

- 您要關聯的儲存虛擬機器必須已經存在。
- 您必須具有應用程式管理員或儲存管理員角色。

對於任何來源儲存虛擬機器和關係類型，您只能在每個目標叢集上選擇一個目標儲存虛擬機器。

使用刪除和建立功能變更關聯只會影響未來的配置操作。它不會移動現有的目標磁碟區。

步驟

1. 在左側導覽窗格中，按一下「保護」>「儲存虛擬機器關聯」。
2. 在「儲存虛擬機器關聯」頁面上，按一下「建立」。

*建立儲存虛擬機器關聯*精靈已啟動。

3. 選擇以下來源之一：

- 任何

當您想要在任何主儲存 VM 來源和一個或多個目標儲存 VM 之間建立關聯時，請選擇此選項。這意味著目前需要保護的所有現有儲存虛擬機器以及將來建立的任何儲存虛擬機器都與指定的目標儲存虛擬機器相關聯。例如，您可能希望將來自不同位置的多個不同來源的應用程式備份到一個位置的一個或多個目標儲存虛擬機器。

- 單身的

當您想要選擇與一個或多個目標儲存虛擬機器關聯的特定來源儲存虛擬機器時，請選擇此選項。例如，如果您要為許多用戶端提供儲存服務，而這些用戶端的資料必須彼此分開，請選擇此選項將特定的儲存 VM 來源與僅指派給該用戶端的特定儲存 VM 目標相關聯。

- 無（外部）

當您想要在來源儲存虛擬機器和目標儲存虛擬機器的外部彈性磁碟區之間建立關聯時，請選擇此選項。

4. 選擇要建立的一種或兩種保護關係類型：

- * SnapMirror*
- * SnapVault*

5. 按一下“下一步”。
6. 選擇一個或多個儲存虛擬機器保護目標。
7. 按一下“完成”。

刪除儲存虛擬機器關聯

您可以刪除合作夥伴應用程式的儲存虛擬機器關聯，以刪除來源和目標儲存虛擬機器之間的輔助配置關係；例如

，當目標儲存虛擬機器已滿並且您想要建立新的儲存虛擬機器保護關聯時，您可能會執行此操作。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

在選擇至少一個儲存虛擬機器關聯之前，「刪除」按鈕將被停用。使用刪除和建立功能變更關聯只會影響未來的配置操作；它不會移動現有的目標磁碟區。

步驟

1. 在左側導覽窗格中，按一下「保護」>「儲存虛擬機器關聯」。
2. 選擇至少一個儲存虛擬機器關聯。

*刪除*按鈕已啟用。

3. 按一下“刪除”。

將顯示一個警告對話框。

4. 點選“是”繼續。

選定的儲存虛擬機器關聯將從清單中刪除。

支援儲存服務的 SVM 和資源池需求

如果您觀察到某些特定於儲存服務的 SVM 關聯和資源池需求，則可以更好地確保合作夥伴應用程式中的一致性：例如，當您關聯 SVM 並在 Unified Manager 中建立資源池以支援合作夥伴應用程式提供的儲存服務中的保護拓撲時。

一些應用程式與 Unified Manager 伺服器合作，提供在來源磁碟區和二級或三級位置的保護磁碟區之間自動設定和執行 SnapMirror 或 SnapVault 備份保護的服務。為了支援這些保護儲存服務，您必須使用 Unified Manager 設定必要的 SVM 關聯和資源池。

若要支援儲存服務單跳或級聯保護（包括從 SnapMirror 來源或 SnapVault 主磁碟區複製到目標 SnapMirror 或位於二級或三級位置的 SnapVault 備份磁碟區），請遵守下列要求：

- 必須在包含 SnapMirror 來源或 SnapVault 主磁碟區的 SVM 與任何二級磁碟區或三級磁碟區所在的 SVM 之間設定 SVM 關聯。
 - 例如，要支援來源磁碟區 Vol_A 位於 SVM_1 上、SnapMirror 二級目標磁碟區 Vol_B 位於 SVM_2 上、三級 SnapVault 備份磁碟區 Vol_C 位於 SVM_3 上的保護拓撲，您必須使用 Unified Manager Web UI 在 SVM_1 和 SVM_2 之間設定的保護拓撲，您必須使用 Unified Manager Web UI 在 SVM_1 和 SVM_2 之間設定關聯配置。

在此範例中，SVM_2 和 SVM_3 之間的任何 SnapMirror 關聯或 SnapVault 備份關聯都不是必需的，也不會使用。

- 若要支援來源磁碟區 Vol_A 和 SnapMirror 目標磁碟區 Vol_B 都位於 SVM_1 上的保護拓撲，您必須在 SVM_1 和 SVM_1 之間設定 SnapMirror 關聯。
- 資源池必須包含可供關聯 SVM 使用的叢集聚合資源。

您可以透過 Unified Manager Web UI 設定資源池，然後透過合作夥伴應用程式指派儲存服務二級目標和三

級目標節點。

哪些工作

作業是您可以使用 Unified Manager 監控的一系列任務。查看作業及其相關任務可讓您確定它們是否已成功完成。

當您建立 SnapMirror 和 SnapVault 關係、當您執行任何關係操作（中斷、編輯、靜默、刪除、復原、重新同步和反向重新同步時）、當您執行資料復原任務時、當您登入叢集時等等時，都會啟動作業。

啟動作業時，您可以使用「作業」頁面和「作業詳細資料」頁面來監控該作業以及相關作業任務的進度。

監控作業

您可以使用「作業」頁面來監視作業狀態並查看作業屬性（例如儲存服務類型、狀態、提交時間和完成時間），以確定作業是否已成功完成。

開始之前

您必須具有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「保護」>「作業」。

將顯示「作業」頁面。

2. 查看*狀態*列以確定目前正在執行的作業的狀態。
3. 點擊工作名稱即可查看有關該特定工作的詳細資訊。

將顯示「作業詳細資料」頁面。

查看職位詳情

開始工作後，您可以從「工作詳情」頁面追蹤其進度，並監控相關任務是否有錯誤。

開始之前

您必須具有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「保護」>「作業」。
2. 在「作業」頁面中，按一下「名稱」欄位中的作業名稱以顯示與該作業相關的任務清單。
3. 按一下某個任務即可在任務清單右側的「任務詳細資料」窗格和「任務訊息」窗格中顯示其他資訊。

中止作業

如果某項作業花費的時間太長、遇到太多錯誤或不再需要，您可以使用「作業」頁面中止該作業。只有當作業的狀態和類型允許時，您才可以中止作業。您可以中止任何正在執行

的作業。

開始之前

您必須具有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「保護」>「作業」。
2. 從作業清單中選擇一項作業，然後按一下「中止」。
3. 在確認提示下，按一下「是」以中止所選作業。

重試失敗的保護作業

採取措施修復失敗的保護作業後，您可以使用*重試*再次執行該作業。重試作業將使用原始作業 ID 建立新作業。

開始之前

您必須具有應用程式管理員或儲存管理員角色。

每次只能重試一項失敗的作業。選擇多個作業將停用「重試」按鈕。僅可重試保護配置和保護關係操作類型的作業。

步驟

1. 在左側導覽窗格中，按一下「保護」>「作業」。
2. 從作業清單中，選擇單一失敗的保護配置或保護關係操作類型作業。

*重試*按鈕已啟用。

3. 按一下“重試”。

工作重新開始。

保護關係視窗和對話框的描述

您可以查看和管理與保護相關的詳細信息，例如資源池、SVM 關聯和保護作業。您可以使用適當的「健康閾值」頁面來設定聚合、磁碟區和關係的全域健康閾值。

資源池頁面

資源池頁面顯示現有的資源池及其成員，並使您能夠建立、監控和管理資源池以進行設定。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 創造

啟動「建立資源池」對話框，您可以使用該對話框建立資源池。

- 編輯

使您能夠編輯所建立的資源池的名稱和描述。

- 刪除

使您能夠刪除一個或多個資源池。

資源池列表

資源池清單顯示（以表格形式）現有資源池的屬性。

- 資源池

顯示資源池的名稱。

- 描述

描述資源池。

- * SnapLock類型*

顯示資源池中聚合正在使用的SnapLock類型。 SnapLock類型的有效值為 Compliance、Enterprise 和 Non-SnapLock。一個資源池只能包含一種SnapLock類型的聚合。

- 總容量

顯示資源池的總容量（以 MB、GB 等為單位）。

- 已使用容量

顯示資源池中使用的空間量（以 MB、GB 等為單位）。

- 可用容量

顯示資源池中可用的空間量（以 MB、GB 等為單位）。

- 用過的 %

顯示資源池中已使用的空間百分比。

成員清單指令按鈕

成員清單命令按鈕使您能夠執行以下任務：

- 添加

使您能夠為資源池新增成員。

- 刪除

使您能夠從資源池中刪除一個或多個成員。

成員名單

選擇資源池後，成員清單會顯示（表格格式）資源池成員及其屬性。

- 地位

顯示成員聚合的目前狀態。狀態可以是「嚴重」（），錯誤（），警告（）或正常（）。

- 聚合名稱

顯示成員聚合的名稱。

- 狀態

顯示聚合的目前狀態，可以是以下其中之一：

- 離線

不允許讀取或寫入存取。

- 在線的

允許對該聚合上託管的磁碟區進行讀寫存取。

- 受限制的

允許有限的操作（例如奇偶校驗重建），但不允許資料存取。

- 創建

正在創建聚合。

- 摧毀

聚合體正在被破壞。

- 失敗的

聚合無法聯機。

- 《冰雪奇緣》

聚合（暫時）不處理請求。

- 不一致

該聚合已被標記為損壞；您應該聯絡技術支援。

- 鐵限制

診斷工具無法在聚合上運作。

- 安裝

骨材正在安裝過程中。

- 部分的

至少為聚合找到了一個磁碟，但缺少兩個或更多磁碟。

- 靜默

整體已處於靜止狀態。

- 靜默

總體已靜止。

- 已恢復

聚合的恢復已完成。

- 未安裝

聚合已被卸載。

- 解除安裝

聚合正在離線。

- 未知

已發現聚合，但 Unified Manager 伺服器尚未檢索聚合資訊。

預設情況下，此列是隱藏的。

- 簇

顯示聚合所屬叢集的名稱。

- 節點

顯示聚合所在節點的名稱。

- 總容量

顯示聚合的總容量（以 MB、GB 等為單位）。

- 已使用容量

顯示聚合中使用的空間量（以 MB、GB 等為單位）。

- 可用容量

顯示聚合中可用的空間量（以 MB、GB 等為單位）。

- 用過的 %

顯示聚合中使用的空間百分比。

- 磁碟類型

顯示 RAID 配置類型，可以是以下其中之一：

- RAID0：所有 RAID 群組均為 RAID0 類型。
- RAID4：所有 RAID 群組均為 RAID4 類型。
- RAID-DP：所有 RAID 群組均為 RAID-DP 類型。
- RAID-TEC：所有 RAID 群組都屬於 RAID-TEC 類型。
- 混合 RAID：聚合包含不同 RAID 類型（RAID0、RAID4、RAID-DP 和 RAID-TEC）的 RAID 群組。預設情況下，此列是隱藏的。

建立資源池對話框

您可以使用「建立資源池」對話方塊來命名和描述新的資源池，以及向該資源池新增聚合和從中刪除聚合。

資源池名稱

文字方塊可讓您新增以下資訊來建立資源池：

使您能夠指定資源池名稱。

描述

使您能夠描述資源池。

成員

顯示資源池的成員。您也可以新增和刪除成員。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 添加

開啟「聚合」對話框，以便您可以將特定叢集中的聚合新增至資源池。您可以從不同的叢集新增聚合，但不能將相同的聚合新增至多個資源池。

- 消除

使您能夠從資源池中刪除選定的聚合。

- 創造

建立資源池。直到在資源池名稱或描述欄位中輸入資訊後，此按鈕才會啟用。

- 取消

放棄變更並關閉「建立資源池」對話方塊。

編輯資源池對話框

您可以使用「編輯資源池」對話方塊來變更現有資源池的名稱和描述。例如，如果原始名稱和描述不準確或不正確，您可以更改它們以使其更精確。

文字方塊

您可以使用文字方塊變更所選資源池的以下資訊：

- 資源池名稱

使您能夠輸入新名稱。

- 描述

使您能夠輸入新的描述。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 節省

儲存資源池名稱和描述的變更。

- 取消

放棄變更並關閉「編輯資源池」對話方塊。

“聚合”對話框

您可以使用「聚合」對話方塊來選擇要新增至資源池的聚合。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 添加

將選定的聚合新增至資源池。至少選擇一個聚合後，「新增」按鈕才會啟用。





- 取消

放棄更改並關閉“聚合”對話框。

聚合列表

聚合清單顯示（以表格形式）受監控聚合的名稱和屬性。

- 地位

顯示卷的目前狀態。狀態可以是「嚴重」（），錯誤（），警告（）或正常（）。

您可以將指標移到狀態上以查看有關該磁碟區產生的事件的更多資訊。

- 聚合名稱

顯示聚合的名稱。

- 狀態

顯示聚合的目前狀態，可以是以下其中之一：

- 離線

不允許讀取或寫入存取。

- 受限制的

允許有限的操作（例如奇偶校驗重建），但不允許資料存取。

- 在線的

允許對該聚合上託管的磁碟區進行讀寫存取。

- 創建

正在創建聚合。

- 摧毀

聚合體正在被破壞。

- 失敗的

聚合無法聯機。

- 《冰雪奇緣》

聚合（暫時）不處理請求。

- 不一致

該聚合已被標記為損壞；您應該聯絡技術支援。

- 鐵限制

診斷工具無法在聚合上運作。

- 安裝

骨材正在安裝過程中。

- 部分的

至少為聚合找到了一個磁碟，但缺少兩個或更多磁碟。

- 靜默

整體已處於靜止狀態。

- 靜默

總體已靜止。

- 已恢復

聚合的恢復已完成。

- 未安裝

聚合處於離線狀態。

- 解除安裝

聚合正在離線。

- 未知

已發現聚合，但 Unified Manager 伺服器尚未檢索聚合資訊。

- 簇

顯示聚合所在叢集的名稱。

- 節點

顯示包含聚合的儲存控制器的名稱。

- 總容量

顯示聚合的總資料大小（以 MB、GB 等為單位）。預設情況下，此列是隱藏的。

- 承諾容量

顯示聚合中所有磁碟區的已提交總空間（以 MB、GB 等為單位）。預設情況下，此列是隱藏的。

- 已使用容量

顯示聚合中使用的空間量（以 MB、GB 等為單位）。

- 可用容量

顯示可用於聚合中的資料的空間量（以 MB、GB 等為單位）。預設情況下，此列是隱藏的。

- 可用的 %

顯示聚合中可用於資料的空間百分比。預設情況下，此列是隱藏的。

- 用過的 %

顯示聚合中資料使用的空間百分比。

- **RAID 類型**

顯示選定磁碟區的 RAID 類型。RAID 類型可以是 RAID0、RAID4、RAID-DP、RAID-TEC 或混合 RAID。

工作頁面

透過「作業」頁面，您可以查看所有正在執行的合作夥伴應用程式保護作業以及已完成的作業的目前狀態和其他資訊。您可以使用此資訊查看哪些作業仍在運作以及作業是否成功或失敗。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 中止

中止選定的作業。僅當選定的作業正在執行時此選項才可用。

- 重試

重新啟動保護配置或保護關係操作類型失敗的作業。每次只能重試一項失敗的作業。如果選擇了多個失敗的作業，則「重試」按鈕將被停用。您無法重試失敗的儲存服務作業。

- 重新整理

刷新作業清單及其相關資訊。

作業列表

作業清單以表格形式顯示正在進行的作業清單。預設情況下，清單僅顯示過去一週內產生的作業。您可以使用列排序和過濾來自訂要顯示的作業。

- 地位

顯示作業的目前狀態。狀態可以是錯誤 (❗) 或正常 (✅)。

- 職位編號

顯示作業的識別號碼。預設情況下，此列是隱藏的。

作業識別號碼是唯一的，由伺服器在啟動作業時分配。您可以透過在列過濾器提供的文字方塊中輸入職位識

別號碼來搜尋特定職位。

- 姓名

顯示作業的名稱。

- 類型

顯示作業類型。工作類型如下：

- 集群獲取

工作流程自動化作業正在重新發現叢集。

- 保護配置

保護作業正在啟動工作流程自動化工作流程，例如 cron 計畫、SnapMirror策略建立等。

- 保護關係操作

保護作業正在執行SnapMirror操作。

- 保護工作流程鏈

工作流程自動化作業正在執行多個工作流程。

- 恢復

恢復作業正在運作。

- 清理

這項工作正在清理不再需要用於復原目的的儲存服務成員工件。

- 符合

這項工作是檢查儲存服務成員的配置以確保它們符合要求。

- 破壞

這項工作正在破壞儲存服務。

- 進口

該作業正在將非託管儲存物件匯入現有儲存服務。

- 調整

該作業正在修改現有儲存服務的屬性。

- 訂閱

這項工作是為會員訂閱儲存服務。

- 取消訂閱

這項工作是取消會員的儲存服務訂閱。

- 更新

保護更新作業正在運行。

- **WFA** 配置

工作流程自動化作業正在推送叢集憑證並同步資料庫快取。

- 狀態

顯示作業的運作狀態。狀態選項如下：

- 已中止

工作已中止。

- 中止

作業正在中止中。

- 完全的

工作已經完成了。

- 跑步

工作正在運行。

- 提交時間

顯示作業提交的時間。

- 期間

顯示完成作業所花費的時間。預設顯示此列。

- 完成時間

顯示作業完成的時間。預設情況下，此列是隱藏的。

職位詳情頁面

透過「作業詳細資料」頁面，您可以查看正在執行、排隊或已完成的特定保護作業任務的狀態和其他資訊。您可以使用此資訊來監控保護作業進度並排除作業故障。

工作摘要

作業摘要顯示以下資訊：

- 作業 ID
- 類型
- 狀態
- 提交時間
- 完成時間
- 期間

命令按鈕

命令按鈕使您能夠執行以下任務：

- 重新整理

刷新任務清單和與每個任務相關的屬性。

- 查看職位

返回“工作”頁面。

工作任務清單

作業任務清單在表格中顯示與特定作業相關的所有任務以及與每個任務相關的屬性。

- 開始時間

顯示任務開始的日期和時間。預設情況下，最近的任務顯示在列的頂部，較舊的任務顯示在底部。

- 類型

顯示任務的類型。

- 狀態

特定任務的狀態：

- 完全的

任務已完成。

- 排隊

任務即將運行。

- 跑步

任務正在運行。

- 等待


作業已提交，一些相關任務正在等待排隊和執行。

- 地位

顯示任務狀態：

- 錯誤 ()

任務失敗。

- 普通的 ()

任務成功。

- 跳過 ()

某項任務失敗，導致後續任務被跳過。

- 期間

顯示任務開始以來經過的時間。

- 完成時間

顯示任務完成的時間。預設情況下，此列是隱藏的。

- 任務 ID

顯示標識作業的單一任務的 GUID。該列可以進行排序和過濾。預設情況下，此列是隱藏的。

- 依賴順序

顯示一個表示圖表中任務序列的整數，其中第一個任務分配零。預設情況下，此列是隱藏的。

- 任務詳細資料窗格

顯示有關每個作業任務的附加信息，包括任務名稱、任務描述以及失敗的原因（如果任務失敗）。

- 任務訊息窗格

顯示特定於選定任務的訊息。訊息可能包括錯誤的原因和解決錯誤的建議。並非所有任務都會顯示任務訊息。

進階輔助設定對話框

您可以使用「進階輔助設定」對話方塊在輔助磁碟區上啟用版本彈性複製、多副本備份和空間相關設定。當您想要變更、啟用或停用目前設定時，可以使用「進階輔助設定」對話方塊。

與空間相關的設定可最大限度地增加儲存的資料量，包括：重複資料刪除、資料壓縮、自動增長和空間保證。

此對話方塊包括以下欄位：

- 啟用版本靈活複製

啟用具有版本靈活複製功能的SnapMirror。即使目標磁碟區運行的ONTAP版本低於來源磁碟區的版本，版本靈活的複製也能為來源磁碟區提供SnapMirror保護。

- 啟用備份

如果啟用了版本靈活複製，也可以將SnapMirror來源資料的多個 Snapshot 副本傳輸到SnapMirror目標並保留在該目標。

- 啟用重複資料刪除

在SnapVault關係中的二級磁碟區上啟用重複資料刪除，以便消除重複的資料區塊，從而節省空間。當空間節省至少 10% 且資料覆蓋率不是很快時，您可以使用重複資料刪除。重複資料刪除通常用於虛擬化環境、檔案共用和備份資料。預設情況下，此設定為停用。啟用後，每次傳輸後都會啟動此操作。

- 啟用壓縮

啟用透明資料壓縮。當空間節省至少 10%、潛在開銷可以接受、並且在非高峰時段有足夠的系統資源來完成壓縮時，您可以使用壓縮。在SnapVault關係中，此設定預設為停用狀態。僅當選擇重複資料刪除時才可以使用壓縮。

- 在線壓縮

透過在將資料寫入磁碟之前壓縮資料來立即節省空間。當您的系統在高峰時段的使用率不超過 50% 時，以及當系統在高峰時段可以容納新的寫入和額外的 CPU 時，您可以使用內聯壓縮。僅當選擇“啟用壓縮”時，此設定才可用。

- 啟用自動增長

當可用空間百分比低於指定閾值時，只要關聯聚合上有可用空間，您就可以自動增加目標磁碟區。

- 最大尺寸

設定卷可以增長的最大百分比。預設值比來源磁碟區大小大 20%。如果目前大小大於或等於最大自動增長百分比，則磁碟區不會自動增長。僅當啟用自動增長設定時，此欄位才可用。

- 增加尺寸

指定在達到來源磁碟區的最大百分比之前磁碟區自動成長的百分比增量。

- 艙位保證

確保在輔助磁碟區上分配足夠的空間，以便資料傳輸始終成功。空間保證設定可以是以下其中之一：

- 文件

- 體積

- 無 + 例如，您可能有一個 200 GB 的捲，其中包含總計 50 GB 的檔案；但是，這些檔案僅包含 10 GB 的資料。無論來源磁碟區上的內容如何，磁碟區保證都會為目標磁碟區分配 200 GB。文件保證分配 50 GB 以確保為來源上的檔案保留足夠的空間；在這種情況下選擇「無」意味著在目標上僅為來源上的檔案資料實際使用的空間分配 10 GB。

空間保證預設為磁碟區。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 申請

儲存選定的效率設置，並在按一下「配置保護」對話方塊中的「套用」時套用這些設定。

- 取消

放棄您的選擇並關閉“高級目標設定”對話框。

進階目標設定對話框

您可以使用「進階目標設定」對話方塊在目標磁碟區上啟用空間保證設定。當來源上停用空間保證但希望在目標上啟用它時，您可能會選擇進階設定。SnapMirror關係中的重複資料刪除、壓縮和自動增長設定從來源磁碟區繼承且無法變更。

艙位保證

確保在目標磁碟區上分配足夠的空間，以便資料傳輸始終成功。空間保證設定可以是以下其中之一：

- 文件
- 體積
- 沒有任何

例如，您可能有一個 200 GB 的捲，其中包含總計 50 GB 的文件；但是，這些文件僅包含 10 GB 的資料。無論來源磁碟區上的內容如何，磁碟區保證都會為目標磁碟區分配 200 GB。檔案保證分配 50 GB 以確保在目標上為來源檔案保留足夠的空間；在這種情況下選擇 無 意味著在目標上僅為來源上的檔案資料實際使用的空間分配 10 GB。

空間保證預設為磁碟區。

恢復對話框

您可以使用「還原」對話方塊將資料從特定的 Snapshot 副本還原到磁碟區。

恢復自

“恢復自”區域可讓您指定要從哪裡恢復資料。

- 體積

指定要從中復原資料的磁碟區。預設情況下，選擇您啟動還原作業的磁碟區。您可以從下拉清單中選擇不同的捲，該清單包含與您啟動還原作業的磁碟區具有保護關係的所有磁碟區。

- 快照副本

指定要使用哪個 Snapshot 副本來還原資料。預設情況下，選擇最新的 Snapshot 副本。您也可以從下拉清單中選擇不同的 Snapshot 副本。Snapshot 副本清單會根據所選磁碟區而變更。


- 列出最多 **995** 個檔案和目錄

預設情況下，清單中最多顯示 995 個物件。如果您想要查看選取磁碟區內的所有對象，可以取消選取此核取方塊。如果項目數量非常大，此操作可能需要一些時間。

選擇要恢復的項目

透過「選擇要還原的項目」區域，您可以選擇要還原的整個磁碟區或特定檔案和資料夾。您最多可以選擇 10 個檔案、資料夾或兩者的組合。當選擇了最大項目數時，項目選擇複選框將被停用。

- 路徑欄位

顯示要恢復的資料的路徑。您可以導覽到要復原的資料夾和文件，也可以鍵入路徑。在您選擇或輸入路徑之前，此欄位為空。點選  選擇路徑後，您將在目錄結構中向上移動一級。

- 資料夾和檔案清單

顯示您輸入的路徑的內容。預設情況下，首先顯示根資料夾。按一下資料夾名稱即可顯示該資料夾的內容。

您可以如下選擇要復原的項目：

- 當您在路徑欄位中輸入具有特定檔案名稱的路徑時，指定的檔案將顯示在資料夾和檔案中。
- 當您輸入路徑而不指定特定檔案時，資料夾的內容將顯示在資料夾和檔案清單中，並且您最多可以選擇 10 個檔案、資料夾或兩者的組合進行還原。

如果資料夾包含超過 995 個項目，則會顯示一則訊息，指示項目太多而無法顯示，如果繼續執行該操作，則會還原指定資料夾中的所有項目。如果您想查看所選卷內的所有對象，可以取消選取「列出最多 995 個檔案和目錄」複選框。



您無法恢復 NTFS 檔案流。

恢復至

恢復至區域可讓您指定要復原資料的位置。

- **Volume_Name** 中的原始位置

將選定的資料還原到最初備份資料的來源目錄中。

- 備用地點

將選定的資料恢復到新位置：

- 恢復路徑

指定用於恢復選定資料的備用路徑。該路徑必須已經存在。您可以使用*瀏覽*按鈕導覽至要復原資料的位置，也可以使用格式 `cluster://svm/volume/path` 手動輸入路徑。

- 保留目錄層次結構

選取後，保留原始檔案或目錄的結構。例如，如果來源是 /A/B/C/myFile.txt，目標是 /X/Y/Z，則 Unified Manager 將使用目標上的下列目錄結構來還原資料：/X/Y/Z/A/B/C/myFile.txt。

命令按鈕


命令按鈕使您能夠執行以下任務：

- 取消
放棄您的選擇並關閉“還原”對話框。
- 恢復
應用您的選擇並開始恢復過程。

瀏覽目錄對話框

當您想要將資料還原到與原始來源不同的叢集和 SVM 上的目錄時，可以使用瀏覽目錄對話方塊。預設選擇原始來源集群和磁碟區。

透過瀏覽目錄對話框，您可以選擇要將資料還原到的叢集、SVM、磁碟區和目錄路徑。

- 簇
列出可以恢復到的可用叢集目標。預設情況下，選擇原始來源磁碟區的叢集。
- SVM 下拉清單
列出選定叢集可用的 SVM。預設情況下，選擇原始來源磁碟區的 SVM。
- 體積
列出選定 SVM 中的所有讀/寫磁碟區。您可以按名稱和可用空間過濾磁碟區。具有最大空間的捲將首先列出，依此類推，按降序排列。預設情況下，選擇原始來源磁碟區。
- 檔案路徑文字方塊
使您能夠鍵入要將資料還原到的檔案路徑。您輸入的路徑必須已經存在。
- 姓名
顯示選定磁碟區的可用資料夾的名稱。按一下名稱清單中的資料夾將顯示子資料夾（如果存在）。資料夾中包含的檔案不會顯示。點選  選擇資料夾後，您將在目錄結構中向上移動一級。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 選擇目錄
套用您的選擇並關閉「瀏覽目錄」對話框。如果沒有選擇目錄，則此按鈕將被停用。

- 取消

放棄您的選擇並關閉“瀏覽目錄”對話框。

配置保護對話框

您可以使用「設定保護」對話方塊為叢集上的所有讀取、寫入和資料保護磁碟區建立SnapMirror和SnapVault關係，以確保複製來源磁碟區或主磁碟區上的資料。

來源選項卡

- 拓樸視圖

顯示您正在建立的關係的視覺表示。拓樸中的來源預設為突出顯示。

- 來源資訊

顯示有關所選來源磁碟區的詳細信息，包括以下資訊：

- 來源叢集名稱
- 來源 SVM 名稱
- 累計卷總大小

顯示所有選定來源磁碟區的總大小。

- 累計已用卷大小

顯示所有選定來源磁碟區的累計已使用磁碟區大小。

- 來源磁碟區

在表中顯示以下資訊：

- 源體積

顯示選定來源磁碟區的名稱。

- 類型

顯示卷類型。

- SnapLock類型

顯示磁碟區的SnapLock類型。選項包括 Compliance、Enterprise 和 Non- SnapLock。

- 快照複製

顯示用於基線傳輸的 Snapshot 副本。如果來源磁碟區是讀取/寫入的，則 Snapshot 副本列中的 Default 值表示預設建立新的 Snapshot 副本，並用於基線傳輸。如果來源磁碟區是資料保護磁碟區，則 Snapshot 副本列中的值 Default 表示不會建立新的 Snapshot 副本，並且所有現有的 Snapshot 副本都會傳送到目標。點擊 Snapshot 副本值將顯示 Snapshot 副本列表，您可以從中選擇一個現有

Snapshot 副本用於基線傳輸。如果來源類型是資料保護，則無法選擇不同的預設 Snapshot 副本。

SnapMirror 選項卡

使您能夠在建立 SnapMirror 關係時指定保護關係的目標叢集、儲存虛擬機器 (SVM) 和聚合，以及目標的命名約定。您也可以指定 SnapMirror 策略和計畫。

- 拓撲視圖

顯示您正在建立的關係的視覺表示。拓撲中的 SnapMirror 目標資源預設為反白顯示。

- 目的地資訊

使您能夠選擇保護關係的目標資源：

- 高級連結

建立 SnapMirror 關係時啟動「進階目標設定」對話框。

- 簇

列出可作為保護目標主機的叢集。此欄位是必需的。

- 儲存虛擬機器 (SVM)

列出選定叢集上可用的 SVM。必須先選擇一個集群，然後才能填入 SVM 清單。此欄位是必需的。

- 總計的

列出選定 SVM 上可用的聚合。必須先選擇一個集群，然後才能填入聚合清單。此欄位是必需的。匯總清單顯示以下資訊：

- 秩

當多個聚合滿足目標的所有要求時，排名表示聚合列出的優先級，根據以下條件：

- A. 最好使用與來源磁碟區節點位於不同節點上的聚合來實現故障域分離。
- B. 優先選擇具有較少磁碟區的節點上的聚合，以便在叢集中的節點之間實現負載平衡。
- C. 為了實現容量平衡，優先選擇比其他聚合具有更多可用空間的聚合。排名為 1 表示根據這三個標準，該集合是最受歡迎的。

- 聚合名稱

聚合的名稱

- 可用容量

- 聚合上可用於資料的空間量

- 資源池

聚合所屬的資源池的名稱

- 命名約定

指定套用於目標磁碟區的預設命名約定。您可以接受提供的命名約定，也可以建立自訂的命名約定。命名約定可以具有以下屬性：%C、%M、%V 和 %N，其中 %C 是叢集名稱，%M 是 SVM 名稱，%V 是來源卷，%N 是拓撲目標節點名稱。

如果您的輸入無效，則命名約定欄位將以紅色突出顯示。按一下「預覽名稱」連結將顯示您輸入的命名約定的預覽，並且當您在文字欄位中鍵入命名約定時，預覽文字會動態更新。建立關係時，會在目標名稱後面附加 001 至 999 之間的后綴，以取代預覽文字中顯示的 nnn，其中首先分配 001，其次分配 002，依此類推。

- 關係設定

使您能夠指定保護關係使用的最大傳輸速率、SnapMirror策略和計劃：

- 最大傳輸速率

指定透過網路在集群之間傳輸資料的最大速率。如果您選擇不使用最大轉移率，則關係之間的基準轉移是無限制的。

- SnapMirror策略

指定該關係的ONTAP SnapMirror策略。預設值為 DPDefault。

- 創建策略

啟動「建立SnapMirror策略」對話框，在此可以建立和使用新的SnapMirror策略。

- SnapMirror計劃

指定該關係的ONTAP SnapMirror策略。可用的時間表包括無、5 分鐘、8 小時、每天、每小時和每週。預設值為 None，表示沒有與該關係關聯的計劃。沒有時間表的關係沒有滯後狀態值，除非它們屬於儲存服務。

- 創建時間表

啟動「建立計畫」對話框，在此可以建立新的SnapMirror計畫。

SnapVault選項卡

使您能夠在建立SnapVault關係時指定保護關係的二級叢集、SVM 和聚合，以及二級磁碟區的命名約定。您也可以指定SnapVault策略和計劃。

- 拓樸視圖

顯示您正在建立的關係的視覺表示。拓樸中的SnapVault二級資源預設為突出顯示。

- 次要訊息

使您能夠選擇保護關係的輔助資源：

- 高級連結

啟動“進階輔助設定”對話框。

- 簇

列出可用作輔助保護主機的叢集。此欄位是必需的。

- 儲存虛擬機器 (SVM)

列出選定叢集上可用的 SVM。必須先選擇一個集群，然後才能填入 SVM 清單。此欄位是必需的。

- 總計的

列出選定 SVM 上可用的聚合。必須先選擇一個集群，然後才能填入聚合清單。此欄位是必需的。匯總清單顯示以下資訊：

- 秩

當多個聚合滿足目標的所有要求時，排名表示聚合列出的優先級，根據以下條件：

- A. 最好使用與主磁碟區節點位於不同節點上的聚合來實現故障域分離。
- B. 優先選擇具有較少磁碟區的節點上的聚合，以便在叢集中的節點之間實現負載平衡。
- C. 為了實現容量平衡，優先選擇比其他聚合具有更多可用空間的聚合。排名為 1 表示根據這三個標準，該集合是最受歡迎的。

- 聚合名稱

聚合的名稱

- 可用容量

- 聚合上可用於資料的空間量

- 資源池

聚合所屬的資源池的名稱

- 命名約定

指定套用於輔助磁碟區的預設命名約定。您可以接受提供的命名約定，也可以建立自訂的命名約定。命名約定可以具有以下屬性：%C、%M、%V 和 %N，其中 %C 是叢集名稱，%M 是 SVM 名稱，%V 是來源卷，%N 是拓撲輔助節點名稱。

如果您的輸入無效，則命名約定欄位將以紅色突出顯示。按一下「預覽名稱」連結將顯示您輸入的命名約定的預覽，並且當您在文字欄位中鍵入命名約定時，預覽文字會動態更新。如果輸入無效值，無效資訊將在預覽區域中顯示為紅色問號。建立關係時，會在輔助名稱後面附加 001 至 999 之間的后綴，以取代預覽文字中顯示的 nnn，其中首先分配 001，其次分配 002，依此類推。

- 關係設定

使您能夠指定保護關係使用的最大傳輸速率、SnapVault策略和SnapVault計劃：

- 最大傳輸速率

指定透過網路在集群之間傳輸資料的最大速率。如果您選擇不使用最大轉移率，則關係之間的基準轉移是無限制的。

- SnapVault策略

指定該關係的ONTAP SnapVault策略。預設值為 XDPDefault。

- 創建策略

啟動「建立SnapVault策略」對話框，您可以建立和使用新的SnapVault策略。

- SnapVault計劃

指定關係的ONTAP SnapVault計劃。可用的時間表包括無、5 分鐘、8 小時、每天、每小時和每週。預設值為 None，表示沒有與該關係關聯的計劃。沒有時間表的關係沒有滯後狀態值，除非它們屬於儲存服務。

- 創建時間表

啟動「建立計畫」對話框，在此可以建立SnapVault計畫。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 取消

放棄您的選擇，並關閉“配置保護”對話框。

- 申請

應用您的選擇並開始保護過程。

建立計劃對話框

使用「建立計畫」對話方塊可以為SnapMirror和SnapVault關係傳輸建立基本或進階保護計畫。您可以建立一個新的計劃來增加資料傳輸的頻率（因為資料更新頻繁），或者當資料不頻繁更改時，您可以建立一個不太頻繁的計劃。

無法為SnapMirror同步關係配置計劃。

- 目標集群

您在「配置保護」對話方塊的SnapVault標籤或SnapMirror標籤中選擇的叢集的名稱。

- 日程表名稱

您為計劃提供的名稱。計劃名稱可以由字元 A 到 Z、a 到 z、0 到 9 以及以下任何特殊字元組成：! @#%{插入符號}&*()_-。計劃名稱不得包含以下字元：<>。

- 基礎版或進階版

您想要使用的計劃模式。

基本模式包含以下元素：

- 重複

預定的轉移發生的頻率。選擇包括每小時、每天和每週。

- 天

當選擇每週重複時，傳輸將在星期幾發生。

- 時間

當選擇每日或每週時，傳輸發生的時間是一天中的時間。

進階模式包括以下內容：

- 月

以逗號分隔的數字列表，代表一年中的月份。有效值為 0 到 11，其中零代表一月，依此類推。此元素是可選的。將此欄位留空表示每月都會發生轉帳。

- 天

以逗號分隔的數字列表，表示月份中的日期。有效值為 1 至 31。此元素是可選的。將該欄位留空意味著每月每天都會發生轉帳。

- 工作日

以逗號分隔的數字列表，表示一週的每一天。有效值為 0 到 6，其中 0 代表星期日，依此類推。此元素是可選的。將該欄位留空意味著每週每天都會發生轉帳。如果指定了星期幾，但未指定月份中的某天，則轉移僅在指定的星期幾發生，而不是每天發生。

- 小時

以逗號分隔的數字列表，表示一天的小時數。有效值為 0 到 23，其中 0 代表午夜。此元素是可選的。

- 分分鐘

以逗號分隔的數字列表，表示一小時內的分鐘數。有效值為 0 到 59。此元素是必需的。

建立SnapMirror策略對話框

透過「建立SnapMirror策略」對話框，您可以建立策略來設定SnapMirror傳輸的優先順序。您可以使用策略來最大限度地提高從來源到目標的傳輸效率。

- 目標集群

您在「配置保護」對話方塊的SnapMirror標籤中選擇的叢集的名稱。

- 目標 SVM

您在「設定保護」對話方塊的SnapMirror標籤中所選的 SVM 的名稱。

- 政策名稱

您為新策略提供的名稱。策略名稱可以由字元 A 到 Z、a 到 z、0 到 9、句點 (.)、連字號 (-) 和底線 (_) 組成。

- 轉移優先權

傳輸對於非同步操作的運作優先權。您可以選擇正常或低。具有指定正常傳輸優先權的策略的傳輸關係先於具有指定低傳輸優先權的策略的傳輸關係運作。

- 評論

可選字段，您可以在其中添加有關該政策的評論。

- 重新開始傳輸

指示當傳輸因中止操作或任何類型的故障（例如網路中斷）而中斷時要採取的重新啟動操作。您可以選擇以下選項之一：

- 總是

指定在重新開始傳輸之前建立新的 Snapshot 副本，然後（如果存在）從檢查點重新開始傳輸，接著從新建立的 Snapshot 副本進行增量傳輸。

- 絕不

指定中斷的傳輸永遠不會重新啟動。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 取消

放棄選擇並關閉“配置保護”對話框。

- 申請

應用您的選擇並開始保護過程。

建立SnapVault策略對話框

透過「建立SnapVault策略」對話框，您可以建立策略來設定SnapVault傳輸的優先順序。您可以使用策略來最大程度地提高從主磁碟區到輔助磁碟區的傳輸效率。

- 目標集群

您在「配置保護」對話方塊的SnapVault標籤中選擇的叢集的名稱。

- 目標 SVM

您在「配置保護」對話方塊的SnapVault標籤中所選的 SVM 的名稱。

- 政策名稱

您為新策略提供的名稱。策略名稱可以由字元 A 到 Z、a 到 z、0 到 9、句點 (.)、連字號 (-) 和底線 (_) 組成。

- 轉移優先權

傳輸運行的優先權。您可以選擇正常或低。具有指定正常傳輸優先權的策略的傳輸關係先於具有指定低傳輸優先權的策略的傳輸關係運作。預設為正常。

- 評論

可選字段，您可以在其中添加有關SnapVault策略的最多 255 個字元的註釋。

- 忽略訪問時間

指定是否忽略僅存取時間變更的檔案的增量傳輸。

- 複製標籤

在表中列出與ONTAP選擇的在政策中具有特定複製標籤的 Snapshot 副本關聯的規則。還可以提供以下資訊和操作：

- 命令按鈕

命令按鈕使您能夠執行以下操作：

- 添加

使您能夠建立 Snapshot 副本標籤和保留計數。

- 編輯保留計數

使您能夠變更現有 Snapshot 副本標籤的保留計數。保留計數必須是 1 到 251 之間的數字。所有規則的保留計數總和不能超過 251。

- 刪除

使您能夠刪除現有的 Snapshot 副本標籤。

- 快照複製標籤

顯示 Snapshot 副本標籤。如果您選擇一個或多個具有相同本機 Snapshot 副本原則的卷，則會顯示該原則中每個標籤的項目。如果您選擇具有兩個或更多本機 Snapshot 副本原則的多個卷，則該表將顯示所有策略的所有標籤

- 行程

顯示與每個 Snapshot 副本標籤相關的計劃。如果某個標籤關聯有多個計劃，則該標籤的計劃將顯示在以逗號分隔的清單中。如果選擇具有相同標籤但具有不同計劃的多個卷，則計劃將顯示「各種」以指示有多個計劃與所選卷相關聯。

- 目的地保留計數

顯示保留在SnapVault輔助節點上的指定標籤的 Snapshot 副本的數量。具有多個計劃的標籤的保留計數顯示每個標籤和計劃對的保留計數總和。如果您選擇具有兩個或更多本機 Snapshot 副本原則的多個卷，則保留計數為空。

編輯關係對話框

您可以編輯現有的保護關係來變更最大傳輸速率、保護策略或保護計畫。

目的地資訊

- 目標集群

所選目標群集的名稱。

- 目標 SVM

所選 SVM 的名稱

- 關係設定

使您能夠指定保護關係使用的最大傳輸速率、SnapMirror策略和計劃：

- 最大傳輸速率

指定基線資料透過網路在集群之間傳輸的最大速率。選取後，網路頻寬將限制為您指定的值。您可以輸入一個數值，然後選擇每秒千位元組 (KBps)、每秒兆位元組 (MBps)、每秒千兆位元組 (GBps) 或每秒太字節 (TBps)。您指定的最大傳輸速率必須大於 1 KBps 且小於 4 TBps。如果您選擇不使用最大轉移率，則關係之間的基準轉移是無限制的。如果主集群和輔助集群相同，則此設定已停用。

- SnapMirror策略

指定該關係的ONTAP SnapMirror策略。預設值為 DPDefault。

- 創建策略

啟動「建立SnapMirror策略」對話框，在此可以建立和使用新的SnapMirror策略。

- SnapMirror計劃

指定該關係的ONTAP SnapMirror策略。可用的時間表包括無、5 分鐘、8 小時、每天、每小時和每週。預設值為 None，表示沒有與該關係關聯的計劃。沒有時間表的關係沒有滯後狀態值，除非它們屬於儲存服務。

- 創建時間表

啟動「建立計畫」對話框，在此可以建立新的SnapMirror計畫。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 取消

放棄選擇並關閉“配置保護”對話框。

- 提交

應用您的選擇並關閉“編輯關係”對話框。

初始化/更新對話框

初始化/更新對話方塊可讓您對新的保護關係執行首次基準傳輸，或在關係已經初始化且您想要執行手動、非計劃、增量更新的情況下更新關係。

傳輸選項選項卡

透過「傳輸選項」選項卡，您可以變更傳輸的初始化優先順序並變更傳輸期間使用的頻寬。

- 轉移優先權

傳輸運行的優先權。您可以選擇正常或低。指定正常傳輸優先權的策略關係在指定低傳輸優先權的策略關係之前執行。預設選擇“正常”。

- 最大傳輸速率

指定透過網路在集群之間傳輸資料的最大速率。如果您選擇不使用最大轉移率，則關係之間的基準轉移是無限制的。如果選擇具有不同最大傳輸速率的多個關係，則可以指定下列最大傳輸速率設定之一：

- 使用在個人關係設定期間指定的值或編輯

選擇後，初始化和更新操作將使用每個關係建立或編輯時指定的最大傳輸速率。僅當初始化或更新具有不同傳輸速率的多個關係時，此欄位才可用。

- 無限

表示關係之間的傳輸沒有頻寬限制。僅當初始化或更新具有不同傳輸速率的多個關係時，此欄位才可用。

- 將頻寬限制為

選取後，網路頻寬將限制為您指定的值。您可以輸入一個數值，然後選擇每秒千位元組 (KBps)、每秒兆位元組 (MBps)、每秒千兆位元組 (GBps) 或每秒太字節 (TBps)。您指定的最大傳輸速率必須大於 1 KBps 且小於 4 TBps。

來源 Snapshot 副本選項卡

「來源 Snapshot 副本」標籤顯示用於基準傳輸的來源 Snapshot 副本的下列資訊：

- 來源磁碟區

顯示對應來源磁碟區的名稱。

- 目標音量

顯示選定目標磁碟區的名稱。

- 來源類型

顯示卷類型。類型可以是讀/寫或資料保護。

- 快照副本

顯示用於資料傳輸的 Snapshot 副本。按一下 Snapshot 副本值將顯示「選擇來源 Snapshot 副本」對話框，您可以在其中根據您擁有的保護關係類型和正在執行的操作選擇要傳輸的特定 Snapshot 副本。對於資料保護類型來源，指定不同 Snapshot 副本的選項不可用。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 取消

放棄您的選擇並關閉初始化/更新對話框。

- 提交

儲存您的選擇並開始初始化或更新作業。

重新同步對話框

透過重新同步對話框，您可以重新同步先前已中斷且隨後目標變為讀/寫卷的 SnapMirror 或 SnapVault 關係上的資料。當來源磁碟區上所需的通用 Snapshot 副本被刪除導致 SnapMirror 或 SnapVault 更新失敗時，您可能還需要重新同步。

重新同步選項選項卡

透過「重新同步選項」標籤，您可以設定正在重新同步的保護關係的傳輸優先順序和最大傳輸速率。

- 轉移優先權

傳輸運行的優先權。您可以選擇正常或低。具有指定正常傳輸優先權的策略的關係先於具有指定低傳輸優先權的策略的關係運作。

- 最大傳輸速率

指定透過網路在集群之間傳輸資料的最大速率。選取後，網路頻寬將限制為您指定的值。您可以輸入一個數值，然後選擇每秒千位元組 (KBps)、每秒兆位元組 (MBps)、每秒千兆位元組 (GBps) 或 TBps。如果您選擇不使用最大轉移率，則關係之間的基準轉移是無限制的。

來源 Snapshot 副本選項卡

「來源 Snapshot 副本」標籤顯示用於基準傳輸的來源 Snapshot 副本的下列資訊：

- 來源磁碟區

顯示對應來源磁碟區的名稱。

- 目標音量

顯示選定目標磁碟區的名稱。

- 來源類型

顯示磁碟區類型：讀取/寫入或資料保護。

- 快照副本

顯示用於資料傳輸的 Snapshot 副本。按一下 Snapshot 副本值將顯示「選擇來源 Snapshot 副本」對話框，您可以在其中根據您擁有的保護關係類型和正在執行的操作選擇要傳輸的特定 Snapshot 副本。

命令按鈕

- 提交

開始重新同步程序並關閉「重新同步」對話方塊。

- 取消

取消您的選擇並關閉“重新同步”對話框。

選擇來源 Snapshot 副本對話框

您可以使用「選擇來源 Snapshot 副本」對話方塊選擇特定的 Snapshot 副本以在保護關係之間傳輸數據，或選擇預設行為，該行為取決於您是初始化、更新還是重新同步關係，以及關係是 SnapMirror 還是 SnapVault。

預設

使您能夠選擇預設行為來確定使用哪個 Snapshot 副本來初始化、更新和重新同步 SnapVault 和 SnapMirror 關係的傳輸。

如果您正在執行 SnapVault 傳輸，則每個操作的預設行為如下：

手術	來源為讀/寫時的預設 SnapVault 行為	來源為資料保護 (DP) 時的預設 SnapVault 行為
初始化	建立新的 Snapshot 副本並傳輸它。	傳輸最後匯出的 Snapshot 副本。
更新	僅傳輸策略中指定的標記的 Snapshot 副本。	傳輸最後匯出的 Snapshot 副本。
重新同步	傳輸在最新的通用 Snapshot 副本之後建立的所有帶有標籤的 Snapshot 副本。	傳輸最新的標記 Snapshot 副本。

如果您正在執行 SnapMirror 傳輸，則每個操作的預設行為如下：

手術	預設 SnapMirror 行為	當關係是 SnapMirror 到 SnapMirror 級聯中的第二跳時，預設的 SnapMirror 行為
初始化	建立新的 Snapshot 副本並傳輸該副本以及在該新 Snapshot 副本之前建立的所有 Snapshot 副本。	從來源傳輸所有 Snapshot 副本。
更新	建立新的 Snapshot 副本並傳輸該副本以及在該新 Snapshot 副本之前建立的所有 Snapshot 副本。	傳輸所有 Snapshot 副本。
重新同步	建立新的 Snapshot 副本，然後從來源傳輸所有 Snapshot 副本。	將所有 Snapshot 副本從二級卷傳輸到三級卷，並刪除在創建最新通用 Snapshot 副本後添加的任何資料。

現有快照副本

如果該操作允許選擇 Snapshot 副本，則您可以從清單中選擇現有的 Snapshot 副本。

- 快照副本

顯示現有的 Snapshot 副本，您可以從中選擇進行傳輸。

- 建立日期

顯示建立 Snapshot 副本的日期和時間。快照副本按從最新到最早的順序列出，最新的副本位於清單頂部。

如果您正在執行SnapVault傳輸，並且想要選擇現有的 Snapshot 副本從來源傳輸到目標，則每個操作的行為如下：

手術	指定 Snapshot 副本時的 SnapVault 行為	在級聯中指定 Snapshot 副本時的 SnapVault 行為
初始化	傳輸指定的 Snapshot 副本。	資料保護卷不支援來源 Snapshot 副本選擇。
更新	傳輸指定的 Snapshot 副本。	資料保護卷不支援來源 Snapshot 副本選擇。
重新同步	傳輸選定的 Snapshot 副本。	資料保護卷不支援來源 Snapshot 副本選擇。

如果您正在執行SnapMirror傳輸，並且想要選擇現有的 Snapshot 副本從來源傳輸到目標，則每個操作的行為如下：

手術	指定 Snapshot 副本時的 SnapMirror 行為	在級聯中指定 Snapshot 副本時的 SnapMirror 行為
初始化	傳輸來源上的所有 Snapshot 副本，直到指定的 Snapshot 副本。	資料保護卷不支援來源 Snapshot 副本選擇。
更新	傳輸來源上的所有 Snapshot 副本，直到指定的 Snapshot 副本。	資料保護卷不支援來源 Snapshot 副本選擇。
重新同步	將所有 Snapshot 副本從來源傳輸到選定的 Snapshot 副本，然後刪除在建立最新的通用 Snapshot 副本後新增的任何資料。	資料保護卷不支援來源 Snapshot 副本選擇。

命令按鈕

命令按鈕使您能夠執行以下任務：

- 提交

提交您的選擇並關閉「選擇來源 Snapshot 副本」對話框。
- 取消

放棄您的選擇並關閉「選擇來源 Snapshot 副本」對話框。

反向重新同步對話框

當因來源磁碟區已停用且目標變成讀取/寫入磁碟區而導致保護關係中斷時，反向重新同步可讓您反轉關係的方向，以便目標成為新的來源，來源成為新的目標。

當災難導致保護關係中的來源磁碟區失效時，您可以使用目標磁碟區將資料轉換為讀取/寫入形式來提供數據，同時修復或更換來源、更新來源並重新建立關係。執行反向重新同步操作時，來源上比通用 Snapshot 副本上的資料更新的資料將被刪除。

反向重新同步之前

顯示反向重新同步操作之前關係的來源和目標。

- 來源磁碟區

反向重新同步操作之前來源磁碟區的名稱和位置。
- 目標音量

反向重新同步操作之前目標磁碟區的名稱和位置。

反向重新同步後

顯示保留重新同步操作後關係的來源和目標。

- 來源磁碟區

反向重新同步操作後來源磁碟區的名稱和位置。

- 目標音量

反向重新同步操作後目標磁碟區的名稱和位置。

命令按鈕

命令按鈕使您能夠執行以下操作：

- 提交

開始反向重新同步過程。

- 取消

關閉“反向重新同步”對話方塊而不啟動反向重新同步操作。

關係：所有關係視圖

關係：所有關係視圖顯示有關儲存系統上的保護關係的資訊。

預設情況下，當您造訪「關係」頁面時，顯示的報告包括磁碟區和儲存虛擬機器的頂級保護關係。頁面頂部的控制項可讓您選擇特定視圖、執行搜尋以定位特定物件、建立和套用篩選器以縮小顯示資料的清單、新增/刪除/重新排序頁面上的資料列以及將頁面上的資料匯出為 .csv、.pdf 或 .xlsx 檔案。自訂頁面後，您可以將結果儲存為自訂視圖，然後安排定期產生並透過電子郵件發送此資料的報告。預設情況下，當您選擇「關係」功能表時，顯示的報告包括資料中心中捲和儲存虛擬機器的保護關係。您可以使用*篩選器*選項僅查看選定的儲存系統，例如僅磁碟區或僅儲存虛擬機器。相同的報告顯示在儲存頁面中，並且僅針對選定的儲存實體。如果您想要查看磁碟區或儲存虛擬機器關係，您可以存取 儲存 > 磁碟區 > 關係：所有關係 頁面或存取 保護 > 關係 > 關係：所有關係，然後使用 篩選器 中的 關聯物件類型 選項僅過濾掉磁碟區或儲存裝置資料。

列出所有保護關係的關係頁面具有目標群集的連結*在系統管理員中查看*，可讓您在ONTAP系統管理員中查看相同的物件。

- 地位

顯示保護關係的目前狀態。

狀態可以是錯誤 (❗)，警告 (⚠)，或確定 (✅)。

- 來源儲存虛擬機器

顯示來源 SVM 的名稱。您可以透過點擊 SVM 名稱來查看有關來源 SVM 的更多詳細資訊。

如果叢集上存在 SVM 但尚未新增至 Unified Manager 清單，或 SVM 是在叢集上次刷新後建立的，則此欄位將為空白。您必須確保 SVM 存在，或在叢集上執行重新發現以刷新資源清單。

- 來源

根據您的選擇顯示受保護的來源磁碟區或來源儲存虛擬機器。您可以透過點擊磁碟區或儲存虛擬機器名稱來查看有關來源磁碟區或儲存虛擬機器的更多詳細資訊。

如果訊息 `Resource-key not discovered` 顯示，這可能表示該磁碟區存在於叢集上，但尚未新增至 Unified Manager 庫存中，或該磁碟區是在叢集上次刷新後建立的。您必須確保該磁碟區存在，或在叢集上執行重新發現以刷新資源清單。

- 目標儲存虛擬機器

顯示目標 SVM 的名稱。您可以透過點擊 SVM 名稱來查看有關目標 SVM 的更多詳細資訊。

- 目的地

根據您的選擇顯示目標磁碟區或儲存虛擬機器的名稱。您可以透過點擊對應的物件名稱來查看有關目標磁碟區或儲存虛擬機器的更多詳細資訊。

- 關係物件類型

顯示關係中使用的物件類型，例如儲存虛擬機器、磁碟區和一致性群組。對於一致性關係中的對象，關係來源和目標顯示一致性群組，按一下它們將轉到 LUN 頁面以查看關係。

- 政策

顯示SnapMirror關係的保護策略的名稱。您可以單擊策略名稱以查看與該策略相關的詳細信息，包括以下信息：

- 轉移優先權

指定非同步操作傳輸運行的優先權。傳輸優先權為正常或低。正常優先權傳輸被安排在低優先權傳輸之前。預設為正常。

- 忽略訪問時間

僅適用於SnapVault關係。這指定增量傳輸是否忽略僅存取時間變化的檔案。值要么為 True，要么為 False。預設值為 False。

- 當關係不同步時

指定當同步關係無法同步時ONTAP執行的操作。如果與輔助卷同步失敗，StrictSync 關係將限制對主磁碟區的存取。如果與輔助伺服器同步失敗，同步關係不會限制對主伺服器的存取。

- 嘗試限制

指定SnapMirror關係中每次手動或計畫傳輸的最大嘗試次數。預設值為 8。

- 評論

提供一個文字字段，用於對所選策略進行特定的註釋。

- SnapMirror標籤

指定與 Snapshot 副本原則關聯的第一個計劃的SnapMirror標籤。當您將 Snapshot 副本備份到SnapVault目標時， SnapMirror標籤由SnapVault子系統使用。

- 保留設定

根據時間或備份數量指定備份的保留時間。

- 實質快照副本

指定此磁碟區上與指定標籤相符的 Snapshot 副本的數量。

- 保留快照副本

指定即使達到策略的最大限制也不會自動刪除的SnapVault Snapshot 副本的數量。值要么為 True，要么為 False。預設值為 False。

- 保留警告閾值

指定 Snapshot 副本限制，達到該限制時將發送警告，以指示即將達到最大保留限制。

- 滯後持續時間

顯示鏡像上的資料落後於來源的時間量。

對於 StrictSync 關係，滯後持續時間應接近或等於 0 秒。

- 滯後狀態

顯示託管關係以及具有與該關係關聯的計劃的非託管關係的延遲狀態。滯後狀態可以是：

- 錯誤

滯後持續時間大於或等於滯後誤差閾值。

- 警告

滯後持續時間大於或等於滯後警告閾值。

- 好的

滯後持續時間在正常範圍內。

- 不適用

滯後狀態不適用於同步關係，因為無法配置計畫。

- 上次成功更新

顯示上次成功執行SnapMirror或SnapVault操作的時間。

上次成功更新不適用於同步關係。

- 組成關係

顯示選取物件中是否有任何磁碟區。

- 關係類型

顯示用於複製磁碟區的關係類型。關係類型包括：

- 非同步鏡像
- 非同步保險庫
- 異步 MirrorVault
- 嚴格同步
- 同步

- 轉移狀態

顯示保護關係的傳輸狀態。傳輸狀態可以是以下之一：

- 正在中止

SnapMirror傳輸已啟用；但是，傳輸中止操作（可能包括刪除檢查點）正在進行中。

- 檢查

目標磁碟區正在進行診斷檢查，並且沒有正在進行的傳輸。

- 最終確定

SnapMirror傳輸已啟用。該磁碟區目前處於增量SnapVault傳輸的後傳輸階段。

- 閒置的

傳輸已啟用並且沒有正在進行的傳輸。

- 同步

處於同步關係的兩個磁碟區中的資料是同步的。

- 不同步

目標磁碟區中的資料與來源磁碟區不同步。

- 準備

SnapMirror傳輸已啟用。該磁碟區目前處於增量SnapVault傳輸的預傳輸階段。

- 排隊

SnapMirror傳輸已啟用。目前沒有正在進行的轉移。

- 靜默

SnapMirror傳輸已停用。目前沒有正在進行的轉移。

- 靜默

SnapMirror傳輸正在進行中。附加傳輸已停用。

- 轉移

SnapMirror傳輸已啟用且傳輸正在進行中。

- 過渡

從來源到目標磁碟區的非同步資料傳輸已完成，並且已開始轉換到同步操作。

- 等待

SnapMirror傳輸已啟動，但一些相關任務正在等待排隊。

- 最後轉接時長

顯示上次資料傳輸完成所花費的時間。

傳輸持續時間不適用於 StrictSync 關係，因為傳輸應該是同時的。

- 上次傳輸大小

顯示上次資料傳輸的大小（以位元組為單位）。

傳輸大小不適用於 StrictSync 關係。

- 調解員

顯示調解員狀態。

- 不適用

如果叢集不支援SnapMirror主動同步。

- 未配置

如果未配置，或已配置但僅新增了目標叢集而未在 Unified Manager 中新增來源叢集。

- 中介 IP 位址

如果已配置，則來源叢集和目標叢集都會新增至 Unified Manager 中。

- 狀態

顯示SnapMirror或SnapVault關係的狀態。狀態可以是未初始化、SnapMirrored 或 Broken-Off。如果選擇了來源卷，則關係狀態不適用且不會顯示。

- 關係健康

顯示集群的關係健康狀況。

- 不健康的原因

關係處於不健康狀態的原因。

- 轉移優先權

顯示傳輸運行的優先權。傳輸優先權為正常或低。正常優先權傳輸被安排在低優先權傳輸之前。

傳輸優先權不適用於同步關係，因為所有傳輸都具有相同的優先權。

- 日程

顯示指派給該關係的保護計畫的名稱。

此計畫不適用於同步關係。

- 版本靈活複製

顯示「是」、「有備份選項」或「無」。

- 來源集群

顯示SnapMirror關係的來源叢集的 FQDN、短名稱或 IP 位址。

- 來源集群 **FQDN**

顯示SnapMirror關係的來源叢集的名稱。

- 源節點

顯示磁碟區的SnapMirror關係的來源節點名稱連結的名稱，並在物件為儲存虛擬機器或一致性群組時顯示SnapMirror關係節點計數連結。

在自訂檢視中，當您按一下節點名稱連結時，您可以查看並擴充這些一致性群組的磁碟區所屬的SnapMirror主動同步關係的儲存物件的保護。

當您單擊節點數連結時，它會將您帶到與該關係相關聯的各個節點的節點頁面。當節點數為 0 時，由於沒有與關係關聯的節點，因此不會顯示任何值。

- 目標節點

顯示磁碟區的SnapMirror關係的目標節點名稱連結的名稱，並在物件為儲存虛擬機器或一致性群組時顯示SnapMirror關係節點計數連結。

當您單擊節點數連結時，它會將您帶到與該關係相關聯的各個節點的節點頁面。當節點數為 0 時，由於沒有與關係關聯的節點，因此不會顯示任何值。

- 目標集群

顯示SnapMirror關係的目標群集的名稱。

- 目標群集 **FQDN**

顯示SnapMirror關係的目標群集的 FQDN、簡稱或 IP 位址。

- 受保護

顯示不同的關係。在此列中，您可以查看叢集和儲存虛擬機器順序的磁碟區和一致性群組關係，包括：

- SnapMirror
- 儲存虛擬機器災難復原
- SnapMirror、儲存虛擬機器災難復原
- 一致性組
- SnapMirror，一致性組。

相關資訊

- 有關 關係：**MetroCluster** 視圖的信息，請參閱["監控MetroCluster配置"](#)。
- 有關*關係：過去 1 個月轉移狀態*視圖的信息，請參閱["關係：最近 1 個月的轉移狀態視圖"](#)。
- 有關"關係：所有關係"視圖的信息，請參閱["關係：過去 1 個月的轉移率視圖"](#)。

關係：最近 1 個月的轉移狀態視圖

關係：過去 1 個月的傳輸狀態視圖可讓您分析非同步關係中的磁碟區和儲存虛擬機器在一段時間內的傳輸趨勢。此頁面還顯示傳輸是否成功或失敗。

頁面頂部的控制項可讓您執行搜尋以定位特定物件、建立和應用篩選器以縮小顯示的資料清單、新增/刪除/重新排序頁面上的列以及將頁面上的資料匯出到 .csv，.pdf，或者 .xlsx 文件。自訂頁面後，您可以將結果儲存為自訂視圖，然後安排定期產生並透過電子郵件發送此資料的報告。您可以使用*篩選器*選項僅查看選定的儲存系統，例如僅磁碟區或僅儲存虛擬機器。相同的報告顯示在儲存頁面中，並且僅針對選定的儲存實體。例如，如果您想查看磁碟區關係，您可以從 儲存 > 儲存虛擬機器 > 關係：過去 1 個月的傳輸狀態 選單或 保護 > 關係 > 關係：過去 1 個月的傳輸狀態 選單存取儲存虛擬機器的關係：過去 1 個月的狀態報告，然後使用 篩選器 僅查看磁碟區的資料。

- 來源磁碟區

顯示來源磁碟區名稱。

- 目標音量

顯示目標磁碟區名稱。

- 操作類型

顯示體積傳輸的類型。

- 操作結果

顯示卷傳輸是否成功。

- 轉機開始時間

顯示卷傳輸開始時間。

- 轉移結束時間

顯示卷傳輸結束時間。

- 轉移時長

顯示完成捲傳輸所需的時間（以小時為單位）。

- 傳輸大小

顯示已傳輸磁碟區的大小（以 MB 為單位）。

- 來源 SVM

顯示儲存虛擬機器 (SVM) 名稱。

- 來源集群

顯示來源集群名稱。

- 目標 SVM

顯示目標 SVM 名稱。

- 目標集群

顯示目標群集名稱。

相關資訊

- 有關“關係：所有關係”視圖的信息，請參閱[關係：所有關係視圖](#)。
- 有關 關係： **MetroCluster** 視圖的信息，請參閱[監控MetroCluster配置](#)。
- 有關“關係：所有關係”視圖的信息，請參閱[關係：過去 1 個月的轉移率視圖](#)。

關係：過去 1 個月的轉移率視圖

關係：過去 1 個月的傳輸率視圖使您能夠分析非同步關係中每天傳輸的資料量。此頁面還提供有關每日傳輸的詳細資訊以及完成磁碟區和儲存虛擬機器的傳輸操作所需的時間。

頁面頂部的控制項可讓您執行搜尋以定位特定物件、建立和套用篩選器以縮小顯示資料的清單、新增/刪除/重新排序頁面上的列，以及將頁面上的資料匯出至 .csv、.pdf 或 .xlsx 檔案。自訂頁面後，您可以將結果儲存為自訂視圖，然後安排定期產生並透過電子郵件發送此資料的報告。例如，如果您想查看卷宗關係，您可以訪問 [存儲 > 卷 > 關係：過去 1 個月的傳輸率](#) 菜單或訪問 [保護 > 關係 > 關係：過去 1 個月的傳輸率](#) 菜單，然後使用 [過濾器](#) 僅查看卷的數據。

- 總傳輸大小

顯示磁碟區傳輸的總大小（以千兆位元組為單位）。

- 天

顯示啟動磁碟區轉移的日期。

- 結束時間

顯示卷傳輸結束時間和日期。

相關資訊

- 有關 **關係：MetroCluster** 視圖的信息，請參閱["監控MetroCluster配置"](#)。
- 有關***關係：過去 1 個月轉移狀態***視圖的信息，請參閱["關係：最近 1 個月的轉移狀態視圖"](#)。
- 有關**"關係：所有關係"**視圖的信息，請參閱["關係：過去 1 個月的轉移率視圖"](#)

產生自訂報告

統一管理器報告

Active IQ Unified Manager（以前稱為 OnCommand Unified Manager）提供檢視、自訂、下載和排程 ONTAP 儲存系統報告的功能。報告可以提供有關儲存系統容量、健康狀況、效能、安全性和保護關係的詳細資訊。

Active IQ Unified Manager 9.6 中引入的新 Unified Manager 報表和排程功能取代了 Unified Manager 9.5 版中已淘汰的先前報告引擎。

報告提供網路的不同視圖，提供有關容量、健康、效能、安全性和保護資料的可操作情報。您可以透過顯示、隱藏和重新排列列、過濾資料、排序資料和搜尋結果來自訂視圖。您可以儲存自訂檢視以供重複使用，將其下載為報告，並將它們安排為定期報告以透過電子郵件分發。

您可以下載 Microsoft® Excel 格式的檢視並對其進行自訂。您可以使用進階 Excel 功能，例如複雜排序、分層篩選器、資料透視表和圖表。當對產生的 Excel 報表滿意時，您可以上傳 Excel 檔案以供每次排程和共用報表時使用。

除了從使用者介面產生報表之外，您還可以使用下列附加方法從 Unified Manager 中提取運行狀況、安全性和效能資料：

- 使用開放資料庫連線 (ODBC) 和 ODBC 工具直接存取資料庫以取得叢集訊息
- 執行 Unified Manager REST API 以傳回您感興趣的訊息

從此版本的 Active IQ Unified 管理器開始，對報告進行了以下增強：

- 根據配置的時間表發送報告電子郵件。即使您產生按需報告，您也會收到一封電子郵件。
- 報告的檔案名稱和報告的元資料包括產生報告的主機名稱。即使任何人更改了檔案名，您仍然可以透過此增強功能識別產生報告的主機名稱。

產生報告的存取點

您可以在 Unified Manager 中收集有關叢集的信息，以便從 UI、MySQL 資料庫查詢和 REST API 建立報告。

這些部分描述了透過 UI 進行 Unified Manager 報告和排程。

您可以透過三種方式存取 Unified Manager 提供的報表功能：

- 直接從 UI 中的庫存頁面提取資料。
- 使用開放式資料庫連線 (ODBC) 和 ODBC 工具存取所有可用物件。
- 執行 Unified Manager REST API 以傳回您想要查看的資訊。

這些部分描述了透過 UI 進行 Unified Manager 報告和排程。

可存取 **Unified Manager** 資料庫以進行自訂報告

Unified Manager 使用 MySQL 資料庫來儲存其正在監控的叢集的資料。資料被保存到 MySQL 資料庫中的各種模式。

以下資料庫的所有表格資料均可用：

資料庫	描述
netapp_model	有關ONTAP控制器上物件的資料。
netapp_model_view	有關ONTAP控制器上物件的數據，適用於報告工具消耗。
netapp_效能	集群特定的效能計數器。
奧庫姆	統一管理器應用程式資料和訊息，支援UI過濾、排序和一些衍生欄位的計算。
ocum_報告	庫存配置和容量相關資訊的數據。
ocum_report_birt	庫存配置和容量相關資料的視圖，適用於報表工具消耗。
操作	效能配置設定和閾值資訊。
規模監控器	有關 Unified Manager 應用程式健康和效能問題的數據。
vmware_model	NetApp儲存上託管的資料儲存區的 VMware 物件資料。
vmware_model_view	NetApp儲存上託管的資料儲存區的 VMware 物件資料視圖，適用於報表工具使用。
VMware效能	NetApp儲存上託管的資料儲存區的 VMware 效能計數器資料。

報告使用者（具有報告模式角色的資料庫使用者）能夠存取這些表中的資料。該使用者可以直接從 Unified Manager 資料庫以唯讀方式存取報告和其他資料庫視圖。請注意，該使用者無權存取任何包含使用者資料或叢集憑證資訊的表。

可用於報表的 **Unified Manager REST API**

您可以使用 REST API 查看 Unified Manager 擷取的運作狀況、容量、效能和安全性訊息，從而協助管理叢集。

REST API 透過 Swagger 網頁公開。您可以造訪 Swagger 網頁來顯示 Unified Manager REST API 文檔，以及手動發出 API 呼叫。在 Unified Manager Web UI 的功能表列中，按一下說明按鈕，然後選擇 **API** 文件。有關 Unified Manager REST API 的信息，請參閱["Active IQ Unified Manager REST API 入門"](#)。

您必須具有操作員、儲存管理員或應用程式管理員角色才能存取 REST API。

了解報告

報告顯示有關儲存、網路、服務品質和保護關係的詳細信息，可幫助您在問題發生之前識別並解決潛在問題。

自訂視圖時，您可以使用唯一的名稱儲存它以供將來使用。您可以根據該視圖安排報告定期運行並與他人共用。您也可以下載 Excel 中的檢視以使用進階 Excel 功能進行自訂，然後將該檔案上傳回 Unified Manager。如果您使用該視圖安排報告，它將使用您上傳的 Excel 文件來建立您可以分享的可靠報告。

您可以從「報告計畫」頁面管理所有已排程的報告。



您必須具有應用程式管理員或儲存管理員角色才能管理報告。

您可以將報告下載為逗號分隔值 (CSV)、Excel 或 PDF 檔案。

了解視圖和報表關係

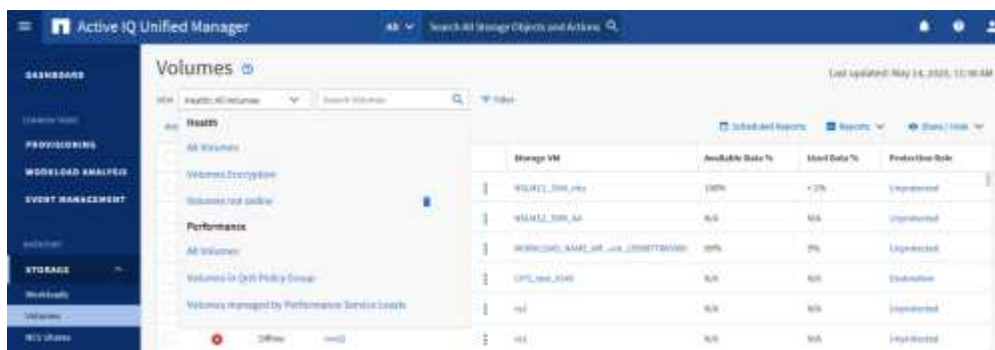
當您下載或安排視圖和庫存頁面時，它們將成為報表。

您可以自訂和儲存視圖和庫存頁面以供重複使用。幾乎您可以在 Unified Manager 中查看的所有內容都可以儲存、重複使用、自訂、排程和共用為報表。

在視圖下拉式選單中，帶有刪除圖示的項目是您或其他使用者建立的現有自訂視圖。沒有圖示的項目是 Unified Manager 提供的預設視圖。預設視圖不能被修改或刪除。



- 如果從清單中刪除自訂視圖，則也會刪除使用該視圖的所有 Excel 檔案或計畫報表。
- 如果您變更自訂視圖，則使用該視圖的報表將在下次產生報表並根據報表計畫透過電子郵件傳送時反映變更。變更視圖時，請確保您的變更與用於報表的任何相關 Excel 自訂相容。如果需要，您可以下載 Excel 文件，進行必要的更改，然後將其作為視圖的新 Excel 自訂上傳，以更新該文件。



只有具有應用程式管理員或儲存管理員角色的使用者才能看到刪除圖示、變更或刪除視圖，或變更或刪除計畫報告。

報告類型

該表提供了可作為報告使用的視圖和庫存頁面的綜合列表，您可以自訂、下載和安排這些視圖和庫存頁面。

Active IQ Unified Manager報告

類型	儲存或網路對象
容量	叢集 聚合 卷 配額樹
健康	叢集 節點 聚合 儲存虛擬機 卷 SMB/CIFS 共享 NFS 分享
表現	叢集 節點 聚合 儲存虛擬機 卷 LUN NVMe 命名空間 網路介面 (LIF) 連接埠

類型	儲存或網路對象
服務品質	傳統 QoS 策略組 自適應 QoS 策略組 效能服務等級策略群組
卷保護關係（可從卷頁取得）	所有關係 最近 1 個月的轉帳狀態 過去 1 個月的轉帳費率
安全	儲存虛擬機 叢集

報告限制

您應該注意，新的Active IQ Unified Manager報告功能有一些限制。

Unified Manager 先前版本的現有報告

您只能編輯在 Unified Manager 9.5 及更早版本中建立和匯入（作為 .rptdesign 檔案）的現有報告的計畫和收件者。如果您自訂了 Unified Manager 9.5 或更早版本提供的任何標準報告，則這些自訂報告將不會匯入新的報告工具中。

如果您需要編輯從 .rptdesign 檔案匯入的現有報告，請執行下列操作之一併刪除匯入的報告：

- 建立新視圖並從該視圖安排報表（首選）
- 將滑鼠懸停在報告上，複製 SQL，然後使用外部工具提取數據

預設視圖可以產生為報告，無需任何自訂。您可以使用新的報表解決方案來重新建立任何自訂報表。

日程與報告關係

您可以為每個已儲存的報表建立許多不同的時間表，並可任意組合收件者。但是，您不能將該計劃重複用於多個報告。

報告保護

任何具有適當權限的使用者都可以編輯或刪除報告。無法封鎖其他使用者刪除或變更已儲存的視圖或時間表。

活動報告

雖然您可以自訂事件檢視並以 CSV 格式下載產生的報告，但您無法排程重複事件報告的產生和分發。

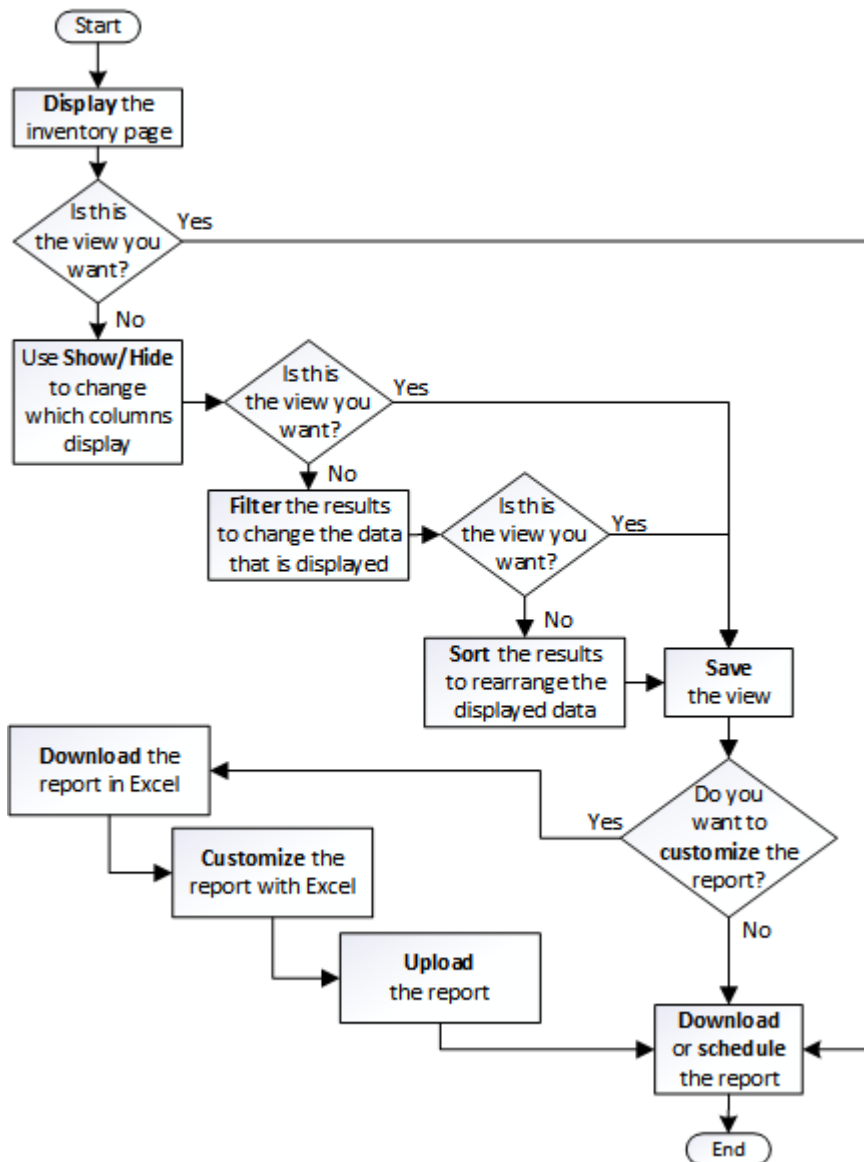
報告不能以電子郵件正文的形式傳送。相反，報告僅以 PDF、Excel 或 CSV 附件的形式傳送。

使用報告

了解如何尋找庫存頁面視圖並將其自訂為可共享的計劃報告。

報告工作流程

描述報告工作流程的決策樹。



報告快速入門

建立範例自訂報表以體驗探索檢視和排程報表。此快速啟動報告查找了您可能想要移動到雲層的捲列表，因為其中存在大量非活動（冷）資料。您將開啟「效能：所有磁碟區」視

圖，使用篩選器和列自訂視圖，將自訂視圖儲存為報告，並安排報告每週共用一次。

開始之前

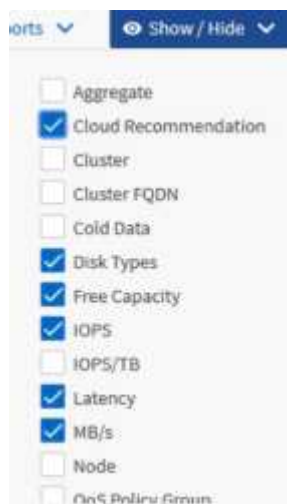
- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已配置FabricPool聚合並且在這些聚合上有磁碟區。

請依照以下步驟操作：

- 開啟預設視圖
- 透過過濾和排序資料來自訂列
- 儲存視圖
- 排程為自訂視圖產生報告

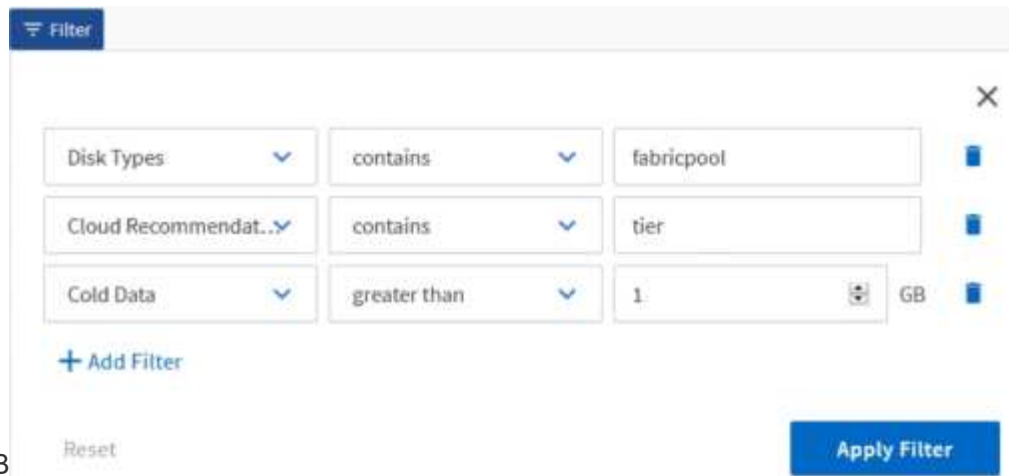
步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「效能」>「所有磁碟區」。
3. 按一下“顯示/隱藏”以確保“磁碟類型”列出現在視圖中。



新增或刪除其他欄位以建立包含對您的報表很重要的欄位的視圖。

4. 將「磁碟類型」列拖曳到「雲端推薦」列旁邊。
5. 點擊過濾器圖示以新增以下三個過濾器，然後點擊*套用過濾器*：
 - 磁碟類型包含FabricPool
 - 雲端建議包含層級
 -



冷數據大於 10 GB

請注意，每個篩選器都透過邏輯 AND 連接，以便傳回的所有磁碟區必須滿足所有條件。您最多可以新增五個濾鏡。

- 按一下「冷資料」列的頂部對結果進行排序，以便具有最多冷資料的捲出現在視圖的頂部。
- 當視圖自訂時，視圖名稱未儲存的視圖。命名檢視以反映檢視所顯示的內容，例如「Vols change tiering policy」。完成後，按一下複選標記或按 **Enter** 以新名稱儲存視圖。

Volumes - Performance / Vols change tiering policy Last updated: Feb 8, 2019, 12:26 PM

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View: Vols change tiering policy

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
rfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

- 在安排或共用之前，將報告下載為 **CSV**、**Excel** 或 **PDF** 檔案以查看輸出。

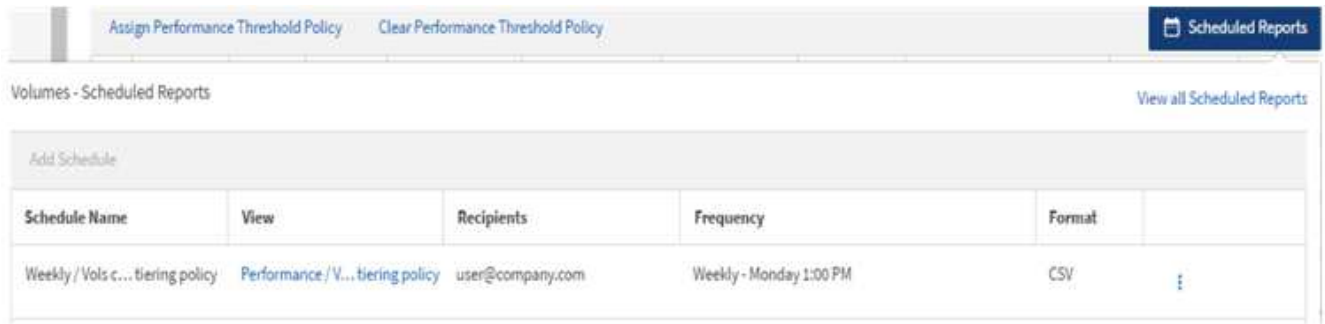
使用已安裝的應用程式（例如 Microsoft Excel（CSV 或 Excel）或 Adobe Acrobat（PDF））開啟文件，或儲存文件。



您可以透過將檢視下載為 Excel 文件，使用複雜的篩選器、排序、資料透視表或圖表進一步自訂報表。在 Excel 中開啟檔案後，使用進階功能自訂報表。滿意後，上傳 Excel 文件。執行報表時，此文件及其自訂內容將套用至視圖。

有關使用 Excel 自訂報表的更多信息，請參閱 [_Microsoft Excel 報表範例_](#)。

- 點擊庫存頁面上的“計劃報告”按鈕。與該物件（在本例中為磁碟區）相關的所有計劃報告均出現在清單中。



10. 按一下「新增計畫」為「報表計畫」頁面新增一行，以便您可以定義新報表的計畫特性。
11. 輸入報告名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

以下範例報告為 CSV 格式：

Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capa	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id
Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040
Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141

以下範例報告為 PDF 格式：

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsdst	Snapshot	28.01	121.32	150	ocum-mo	ocum-mo	aggr5_vs
Ok	nfs_vol4	Snapshot	379.64	2676.57	3072	ocum-mo	ocum-mo	aggr4

根據報告中顯示的結果，您可能需要使用ONTAP System Manager 或ONTAP CLI 將某些磁碟區的分層策略變更為“自動”或“全部”，以將更多冷資料卸載到雲層。

搜尋計劃報告

您可以按名稱、視圖名稱、物件類型或收件人搜尋計劃報告。

1. 在左側導覽窗格中，按一下「儲存管理」>「報告計畫」。
2. 使用*搜尋計劃報告*文字欄位。

要找報告...	嘗試 ...
日程表名稱	輸入報告計畫名稱的一部分。
視圖名稱	輸入報表檢視名稱的一部分。預設視圖和自訂視圖出現在視圖清單中。
接受者	輸入部分電子郵件地址。

要找報告...	嘗試 ...
文件類型	輸入“PDF”、“CSV”或“XLSX”。

- 您可以按一下列標題，按該列的升序或降序對報表進行排序，例如計劃名稱或格式。

自訂報告

您可以透過多種方式自訂視圖，以便建立包含管理ONTAP叢集所需的所有資訊的報表。

從預設庫存頁面或自訂視圖開始，然後透過新增或刪除列、更改列順序、過濾資料或按升序或降序對特定列進行排序來進行自訂。

從 Unified Manager 9.8 開始，您也可以下載 Excel 中的檢視以使用進階功能進行自訂。完成後，上傳自訂的 Excel 檔案。如果您使用該視圖安排報告，它將使用自訂的 Excel 文件來建立您可以共享的強大報告。

有關使用 Excel 自訂報表的更多信息，請參閱 [_Microsoft Excel 報表範例_](#)。



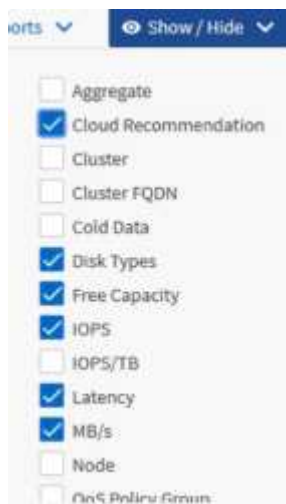
您必須具有應用程式管理員或儲存管理員角色才能管理報告。

自訂列

使用*顯示/隱藏*來選擇您想要在報表中使用的欄位。拖曳庫存頁面上的列以重新排列它們。

步驟

- 按一下“顯示/隱藏”以新增或刪除列。



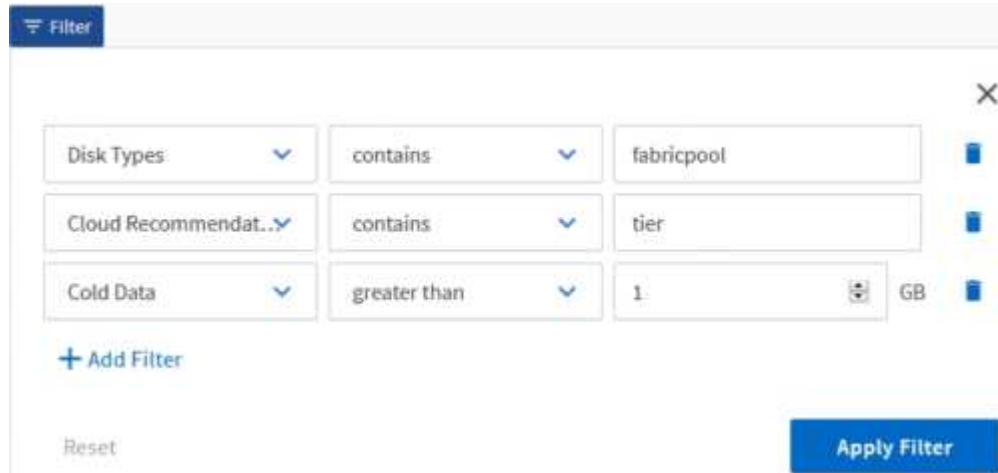
- 在庫存頁面上，拖曳列以按照報告中所需的順序重新排列它們。
- 命名未儲存的視圖以儲存您的變更。

過濾數據

過濾數據以確保結果符合您的報告要求。透過過濾，您可以僅顯示您感興趣的數據。

步驟

1. 點擊過濾器圖示新增過濾器以聚焦您想要查看的結果，然後點擊*套用過濾器*。



2. 命名未儲存的視圖以儲存您的變更。

對資料進行排序

若要對結果進行排序，請按一下某一系列並指示升序或降序。對資料進行排序可以確定報告所需資訊的優先順序。

步驟

1. 點擊列的頂部對結果進行排序，以便最重要的資訊顯示在視圖的頂部。
2. 命名未儲存的視圖以儲存您的變更。

使用搜尋來優化您的視圖

獲得所需的視圖後，您可以使用搜尋欄位進一步最佳化結果，以專注於要包含在報告中的結果。

步驟

1. 開啟您想要用作報表基礎的自訂或預設檢視。
2. 在搜尋欄位中輸入內容以優化視圖中列出的資料。您可以在任何顯示的欄位中輸入部分資料。例如，如果您想要搜尋名稱中包含「US_East」的節點，您可以最佳化完整的節點清單。

搜尋結果將保存在自訂檢視中並用於產生的計畫報告中。

3. 命名未儲存的視圖以儲存您的變更。

使用 Excel 自訂報告

儲存檢視後，您可以以 Excel 工作簿格式 (.xlsx) 下載它。開啟 Excel 檔案時，您可以使用進階 Excel 功能來自訂位報表。

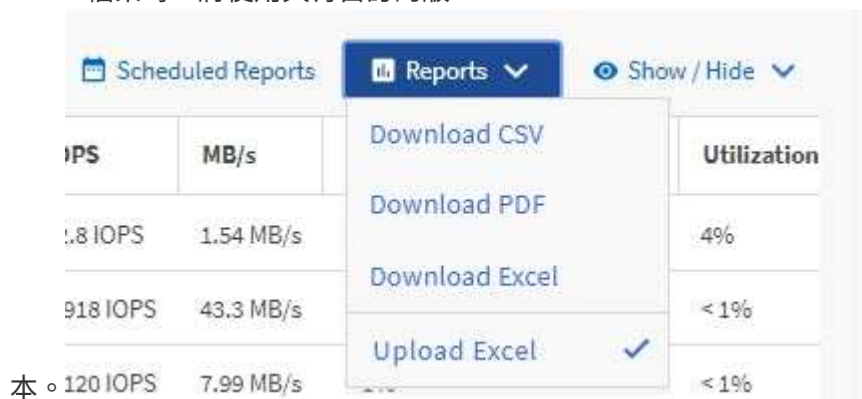
開始之前

您只能上傳副檔名為 .xlsx 的 Excel 工作簿檔案。

例如，您可以在報表中使用的一些進階 Excel 功能包括：

- 多列排序
- 複雜過濾
- 數據透視表
- 圖表

- 下載的 Excel 檔案使用視圖的預設檔名，而不是您儲存的名稱。
 - 格式為 <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - 例如，名為 `Volumes-not online` 檔案名為 `health-volumes-05-May-2020-19-18-00.xlsx` 如果在那天和那個時間保存。
- 您可以為 Excel 檔案新增工作表，但不要變更現有工作表。
 - 不要更改現有的表格、數據和資訊。相反，將資料複製到您創建的新頁面。
 - 上述規則的例外是您可以在「資料」頁面上建立公式。使用資料頁公式在新頁面上建立圖表。
 - 不要命名新表資料或資訊。
- 如果存在自訂的 Excel 文件，則 報表 > 上傳 **Excel** 選單項目旁邊會有一個複選標記。下載 Excel 檔案時，將使用具有自訂的版



步驟

1. 開啟您想要用作報表基礎的預設、自訂或已儲存的檢視。
2. 選擇*報表* > 下載 **Excel**。
3. 儲存文件。該文件已保存到您的下載資料夾。
4. 在 Excel 中開啟已儲存的檔案。請勿將檔案移至新位置，或如果您在其他位置進行工作，請在上傳檔案之前使用原始檔案名稱將檔案儲存回原始位置。
5. 使用 Excel 功能（例如複雜排序、分層篩選器、資料透視表或圖表）自訂檔案。有關更多信息，請參閱 Microsoft® Excel 文件。
6. 選擇*報表* > *上傳 Excel*並選擇您修改的檔案。最近下載的檔案是從相同檔案位置上傳的。
7. 使用*計劃報告*功能向自己發送測試報告。

下載報告

您可以下載報表並將資料以逗號分隔值 (CSV) 檔案、Microsoft Excel (.XLSX) 檔案或 PDF 檔案的形式儲存至本機或網路磁碟機。您可以使用電子表格應用程式（例如 Microsoft Excel）開啟 CSV 和 XLSX 文件，並使用閱讀器（例如 Adobe Acrobat）開啟 PDF 文件。

步驟

1. 點擊“報告”按鈕可以下載以下報告之一：

選擇	到...
下載 CSV	將報告儲存為逗號分隔值 (CSV) 檔案。
下載 PDF	將報告儲存為 .pdf 檔案。
下載 Excel	將報告儲存為 Microsoft Excel (XLSX) 檔案。

計劃報告

在您擁有想要重複使用並作為報表共用的視圖後，您可以使用 Active IQ Unified Manager 來安排它。您可以管理計劃報告，更改每個報告計劃的收件人和分發頻率。

您可以在 Unified Manager 中安排大多數檢視或庫存頁面。例外情況是事件，它們是您可以作為 CSV 檔案下載的報告，但您無法安排事件進行重新產生和共用。您也無法下載或排程儀表板、收藏夾或設定頁面。

從 Active IQ Unified Manager 9.8 開始，您可以下載 Microsoft® Excel 格式的檢視並自訂。您可以使用進階 Excel 功能，例如複雜排序、分層篩選器、資料透視表和圖表。當對產生的 Excel 報表滿意時，您可以上傳 Excel 檔案以供每次排程和共用報表時使用。

您可以安排內建視圖或自訂視圖。您可以選擇要傳送的文件類型，CSV、PDF 或 XSLX。當您第一次安排報告時，您可以下載報告並將自己指定為唯一查看該報告的收件人，因為您的收件人將會看到它。

安排報告

在您擁有想要排程定期產生和分發的檢視或 Excel 檔案後，您可以排程報表。

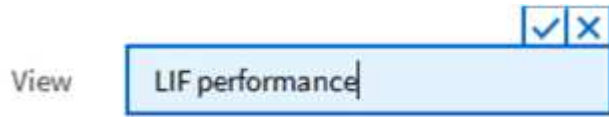
開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須在 常規 > 通知 頁面中配置 SMTP 伺服器設置，以便報告引擎可以將報告作為電子郵件附件傳送至 Unified Manager 伺服器的收件者清單。
- 必須配置電子郵件伺服器以允許附件與產生的電子郵件一起傳送。

使用下列步驟測試並排程為視圖產生的報表。選擇或自訂您想要使用的視圖。以下步驟使用網路視圖來顯示網路介面的效能，但您可以使用任何您想要的視圖。

步驟

1. 開啟你的視野。此範例使用顯示 LIF 效能的預設網路視圖。在左側導覽窗格中，按一下「網路」>「網路介面」。
2. 使用內建的 Unified Manager 功能根據需要自訂視圖。
3. 自訂視圖後，您可以在「視圖」欄位中提供一個唯一的名稱，然後按一下複選標記進行儲存。



4. 您可以使用 Microsoft® Excel 的進階功能來自訂您的報表。有關詳細信息，請參閱"使用 Excel 自訂報告"。
5. 要在安排或共享之前查看輸出：

選項	描述
如果您使用 Excel 自訂報表	查看現有的已下載的 Excel 檔案。
如果您沒有使用 Excel 自訂報表	將報告下載為 CSV 、 PDF 或 XLSX 檔案。

使用已安裝的應用程式開啟文件，例如 Microsoft Excel (CSV/XSLX) 或 Adobe Acrobat (PDF)。

6. 如果您對報告滿意，請點選「計畫報告」。
7. 在報告計劃頁面中，按一下*新增計劃*。
8. 接受預設名稱，即視圖名稱和頻率的組合，或自訂*計劃名稱*。
9. 要首次測試預定報告，只需將自己新增為*收件者*。滿意後，新增所有報告收件者的電子郵件地址。
10. 指定產生報告並傳送給收件人的頻率。您可以選擇*每日*、*每週*或*每月*。
11. 選擇格式，**PDF**、**CSV** 或 **XSLX**。



對於使用 Excel 自訂內容的報告，請始終選擇 **XSLX**。

12. 按一下複選標記 (✓) 儲存報表計劃。



該報告將立即發送以進行測試。此後，將產生報告並按照預定頻率透過電子郵件發送給列出的收件者。

安排導入 .rptdesign 報告

您可以排程在早期版本的 Unified Manager 中建立和匯入的現有報表。

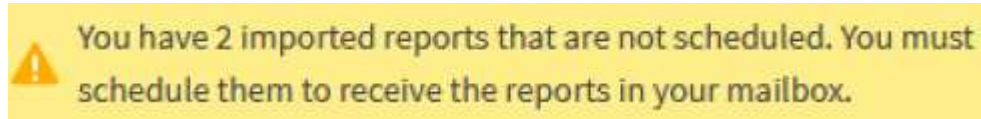
安排導入報告需要以下內容：

- 在早期的 Unified Manager 版本中匯入 BIRT 設計的 .rptdesign 檔案報告
- 適用於升級至 Unified Manager 9.6 GA 或更高版本

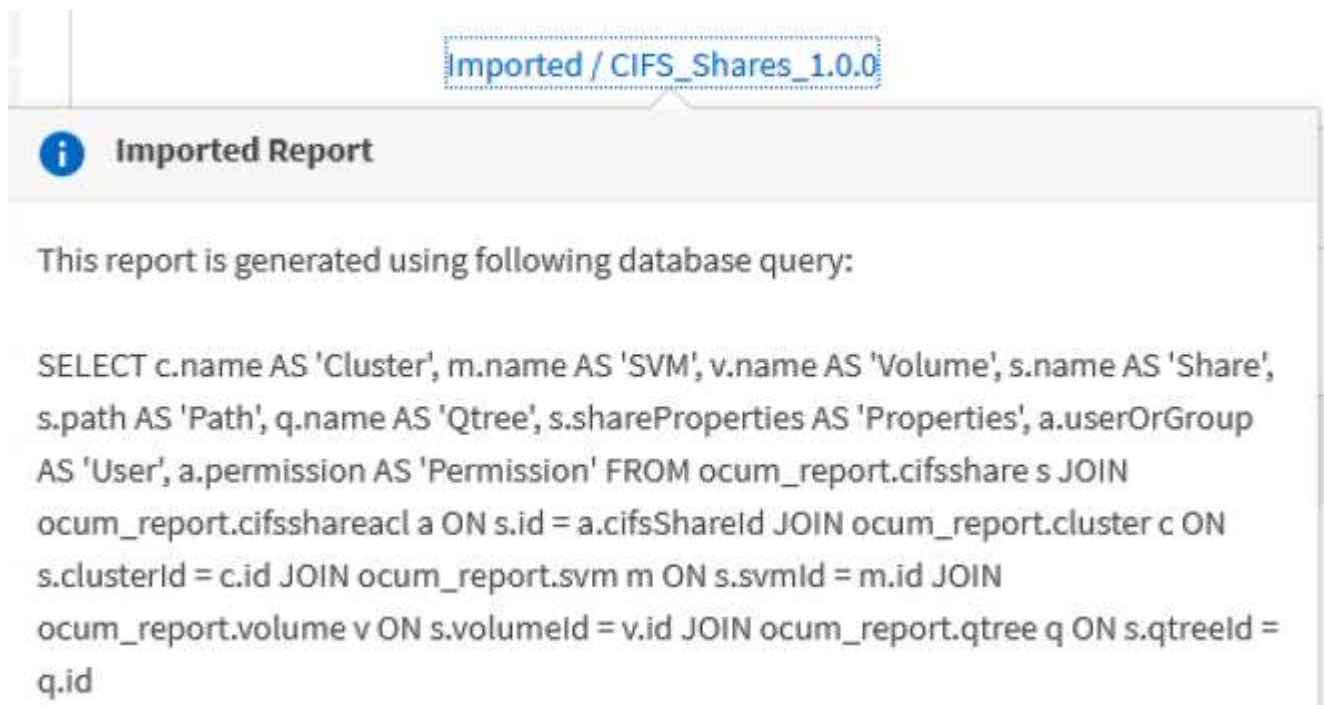
升級至 Unified Manager 9.6 GA 或更高版本後，「報表計畫」頁面會列出匯入的報告。您可以編輯這些報告的時間表以指定收件者的電子郵件地址、頻率和格式（PDF 或 CSV）。否則，這些報告無法在 Unified Manager UI 中編輯或檢視。

步驟

1. 開啟報告計劃頁面。如果您已匯入報告，則會出現一則訊息。



2. 按一下「檢視」名稱以顯示用於產生報表的 SQL 查詢。



3. 點擊更多圖標 ，點擊*編輯*，定義報告計劃詳細信息，並儲存報告。



您也可以透過「更多」圖示刪除任何不需要的報告 。

管理報告時間表

您可以從「報告計畫」頁面管理您的報告計畫。您可以查看、修改或刪除現有計劃。



開始之前

您無法從「報告計畫」頁面安排新報告。您只能從物件庫存頁面新增計劃報告。

- 您必須具有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「儲存管理」>「報告計畫」。
2. 在「報告計畫」頁面上：

如果你想...	然後...
查看現有時間表	使用捲軸和頁面控制項捲動現有報告清單。
編輯現有時間表	<ol style="list-style-type: none"> a. 點擊更多圖標  您想要使用的時間表。 b. 按一下“編輯”。 c. 做出必要的改變。 d. 按一下複選標記以儲存變更。
刪除現有計劃	<ol style="list-style-type: none"> a. 點擊更多圖標  您想要使用的時間表。 b. 按一下“刪除”。 c. 確認你的決定。

編輯計劃報告

報告安排完成後，您可以在「報告安排」頁面上編輯它們。

開始之前



- 您必須具有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「儲存管理」>「報告計畫」。

Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



如果您擁有適當的權限，您可以變更系統中的任何報告及其時間表。

- 2.

點擊更多圖標  您想要更改的時間表。

3. 按一下“編輯”。
4. 您可以變更報告計劃的*計劃名稱*、收件者*清單*、*頻率*和*格式*。
5. 完成後，按一下複選標記以儲存變更。

刪除計劃報告

安排報告後，您可以從「報告安排」頁面中刪除它們。

開始之前

- 您必須具有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「儲存管理」>「報告計畫」。


Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



如果您擁有適當的權限，您可以刪除系統中的任何報告及其時間表。

2. 點擊更多圖標  您想要刪除的時間表。
3. 按一下“刪除”。
4. 確認你的決定。

預定的報告將從清單中刪除，並且將不再按照設定的時間表產生和分發。



如果您從庫存頁面刪除自訂視圖，則使用該視圖的任何自訂 Excel 檔案或計畫報告也將被刪除。

自訂報告範例

這些範例自訂報告通常用於幫助您識別潛在問題並在問題發生之前對潛在問題做出回應。

本節的報告清單並不詳盡，並且會隨著時間的推移而增加。您可以透過提供文件回饋來建議將自訂報告新增至此部分。



您必須具有應用程式管理員或儲存管理員角色才能管理報告。

自訂叢集儲存報告

本節中的範例叢集儲存報表只是幫助您了解如何建立有關叢集容量的報表以協助您監控儲存系統資源的範例。

建立報告以按集群模型查看容量

您可以建立報告來根據儲存系統模型分析叢集的儲存容量和利用率。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立一個按叢集模型顯示容量的自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 在「檢視」功能表中，選擇「容量」>「所有群集」。
3. 選擇“顯示/隱藏”以刪除您不想在報告中顯示的任何列，例如“集群 FQDN”和“作業系統版本”。
4. 將「總原始容量」、「型號/系列」和三個聚合列拖曳到「叢集」列附近。
5. 按一下「模型/系列」列的頂部，按群集類型對結果進行排序。
6. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按叢集模型劃分的容量」。
7. 點擊庫存頁面上的“計劃報告”按鈕。
8. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要為某些叢集新增更多容量，或升級較舊的叢集模型。

建立報告以識別未分配 LUN 容量最多的集群

您可以建立報告來尋找未分配 LUN 容量最多（大於 0.5 TB）的集群，以協助確定可以在何處添加額外的工作負載。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖，顯示具有最多未指派 LUN 容量的集群，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。

2. 在「檢視」功能表中，選擇「容量」>「所有群集」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「未指派的 LUN 容量」列拖曳到「HA 對」列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 未分配的 LUN 容量大於 0.5 TB
6. 按一下「未指派的 LUN 容量」列的頂部，以未指派的 LUN 容量最大數量對結果進行排序。
7. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“Most unallocated LUN capacity”，然後按一下複選標記 (✓)。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要使用叢集未指派的 LUN 容量。

建立報表以查看具有最多可用容量的 HA 對

您可以建立報表來尋找具有最大容量的高可用性 (HA) 對，以設定新的磁碟區和 LUN。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖，該視圖顯示按最多可用容量排序的 HA 對，以設定新磁碟區和 LUN，然後規劃為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「叢集」。
2. 在「檢視」功能表中，選擇「容量」>「所有群集」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「聚合未使用容量」列拖曳到「HA 對」列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 未使用容量總計大於 0.5 TB
6. 按一下「未使用總容量」列的頂部，按未使用總容量的最大數量對結果進行排序。
7. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“最少使用的聚合容量”，然後按一下複選標記 (✓)。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要根據總容量來平衡 HA 對。

建立報表以查看運行舊版ONTAP的節點

您可以建立一個報表來顯示所有叢集節點上安裝的ONTAP軟體版本，以便您可以看到應該升級哪些節點。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立顯示執行舊版ONTAP的節點的自訂視圖，然後計畫為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「節點」。
2. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
3. 將“OS Version”列拖曳到“Node”列附近。
4. 點選“OS Version”列頂部，按ONTAP的最舊版本對結果進行排序。
5. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按ONTAP版本劃分的節點」。
6. 點擊庫存頁面上的“計劃報告”按鈕。
7. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
8. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報表中顯示的結果，您可能需要升級執行舊版ONTAP的節點。

自訂聚合容量報告

這些範例自訂報表用於協助您識別和應對與聚合儲存容量相關的潛在問題。

本節中的報告只是一個範例，旨在幫助您了解如何建立有關聚合容量的報告，以協助您監控儲存系統資源。

建立報表以查看達到滿載的聚合

您可以建立報表來尋找達到滿容量的聚合，以便可以新增更多容量或將工作負載移至其他聚合。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立一個顯示達到滿容量的聚合的自訂視圖，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 在「檢視」功能表中，選擇「容量」>「所有聚合」。

3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 完成學業所需時間少於 45 天
5. 按一下「達到滿載天數」列的頂部，以達到滿載所需的最少天數對結果進行排序。
6. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“Days to full aggregate capacity”，然後按一下複選標記 (✓)。
7. 點擊庫存頁面上的“計劃報告”按鈕。
8. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報表中顯示的結果，您可能想要增加達到滿容量的聚合儲存。此外，您可能希望將「達到滿容量所需的天數」閾值增加到預設的 7 天以上，以便接收有更多時間對空間聚合不足做出反應的事件。

建立報表以查看已滿 **80%** 或以上的聚合

您可以建立報表來突出顯示已滿 **80%** 或以上的聚合。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖，顯示已滿 80% 或以上的聚合，然後排定為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 在「檢視」功能表中，選擇「容量」>「所有聚合」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「可用資料 %」和「已使用資料 %」欄位拖曳到「聚合」列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 使用的資料百分比大於 80%
6. 按一下「已使用資料百分比」列的頂部，按容量百分比對結果進行排序。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如“聚合接近滿”，然後按一下複選標記 (✓)。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計畫」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要從某些聚合中移動一些資料。

建立報表以查看過度承諾的聚合

您可以建立報表來分析儲存容量和聚合的使用情況，並查看過度使用的聚合。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖，顯示超過過量提交閾值的聚合，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 在「檢視」功能表中，選擇「容量」>「所有聚合」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「Overcommitted Capacity %」欄位拖曳到「Aggregate」欄位附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 超額承諾容量百分比大於 100%
6. 按一下「超額承諾容量百分比」欄位的頂部，按容量百分比對結果進行排序。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如“Aggregates overcommitted”，然後按一下複選標記 (✓)。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要為聚合添加更多容量，或從某些聚合中移動一些資料。

自訂磁碟區容量報告

這些範例自訂報告用於協助您識別和回應與磁碟區容量和效能相關的潛在問題。

建立報告以識別已關閉快照自動刪除功能的接近滿容量的捲

您可以建立一個報告，其中包含在停用快照自動刪除功能的情況下接近滿容量的磁碟區清單。結果可以幫助您識別可能想要配置快照自動刪除的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

請依照下列步驟建立一個以正確順序顯示所需列的自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「容量」>「所有磁碟區」。

3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「快照自動刪除」和「剩餘天數」列拖曳到「可用資料容量」列附近。
5. 點擊過濾器圖標，添加以下兩個過濾器，然後點擊*應用過濾器*：
 - 滿期天數少於 30 天
 - 快照自動刪除已停用
6. 按一下「剩餘天數」列的頂部，以便剩餘天數最少的捲出現在清單頂部。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「Vols near capacity」。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要在磁碟區上啟用快照自動刪除或找到增加可用空間的方法。

建立報告以確定停用精簡配置的磁碟區所使用的空間

當磁碟區未進行精簡配置時，它將佔用建立磁碟區時定義的磁碟上的全部空間。識別已停用精簡配置的磁碟區有助於您決定是否要在某些磁碟區上啟用精簡配置。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

請依照下列步驟建立一個以正確順序顯示所需列的自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「容量」>「所有磁碟區」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「已使用資料百分比」和「精簡配置」欄位拖曳到「可用資料容量」欄位附近。
5. 點擊過濾器圖標，添加以下過濾器，**Thin provisioned** 為 **No**，然後點擊 **Apply Filter**。
6. 按一下「已使用資料百分比」列的頂部對結果進行排序，以便百分比最高的磁碟區出現在清單頂部。
7. 使用名稱儲存視圖以反映視圖所顯示的內容，例如「Vols no thin provisioning」。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要在某些磁碟區上啟用精簡配置。

建立報告以識別FabricPool聚合上應將資料移至雲層的捲

您可以建立一個報告，其中包含目前駐留在FabricPool聚合上、具有 Tier 雲端建議且具有大量冷資料的磁碟區清單。此報告可以幫助您決定是否應將某些磁碟區的分層策略變更為“自動”或“全部”，以將更多冷（非活動）資料卸載到雲層。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須已配置FabricPool聚合並且在這些聚合上有磁碟區。

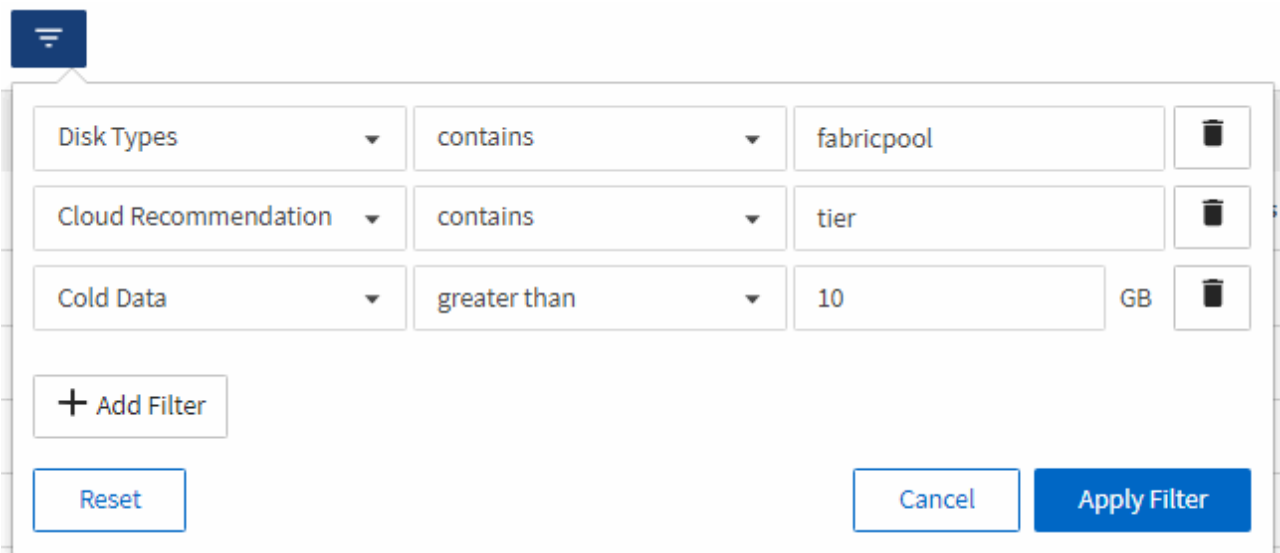
請依照下列步驟建立一個以正確順序顯示所需列的自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「效能」>「所有磁碟區」。
3. 在列選擇器中，確保“磁碟類型”列出現在視圖中。


新增或刪除其他欄位以建立對您的報表很重要的視圖。


4. 將「磁碟類型」列拖曳到「雲端推薦」列附近。
5. 點擊過濾器圖標，添加以下三個過濾器，然後點擊*應用過濾器*：
 - 磁碟類型包含FabricPool
 - 雲端建議包含層級
 - 冷數據大於 10 GB



6. 按一下「冷資料」列的頂部，以便具有最多冷資料的捲出現在視圖的頂部。
7. 使用名稱儲存檢視以反映檢視所顯示的內容，例如「Vols change tiering policy」。

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy  3

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB 	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。
10. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報表中顯示的結果，您可能需要使用系統管理員或ONTAP CLI 將某些磁碟區的分層策略變更為“自動”或“全部”，以將更多冷資料傳輸到雲層。

自訂 Qtree 容量報告

這些範例自訂報告用於協助您識別和回應與 Qtree 容量相關的潛在問題。

建立報告以查看幾乎已滿的 qtree

您可以建立報表來分析 qtree 的儲存容量和利用率，並查看幾乎已滿的 qtree。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立顯示幾乎已滿的 qtree 的自訂視圖，然後計劃為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「Qtree」。
2. 選擇“顯示/隱藏”以刪除報表中不需要的任何列。
3. 將“磁碟已使用百分比”列拖曳到“Qtrees”列附近。
4. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 磁碟使用率百分比大於 75%
5. 按一下「磁碟使用百分比」列的頂部，按容量百分比對結果進行排序。
6. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如“Qtrees nearing full”，然後按一下複選標記 (✓)。
7. 點擊庫存頁面上的“計劃報告”按鈕。

8. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要調整磁碟硬限制和軟限制（如果設定），或在 qtree 之間平衡資料。

自訂 NFS 共享報告

您可以自訂 NFS 共用報表來分析有關儲存系統上磁碟區的 NFS 匯出策略和規則的資訊。例如，您可以自訂報告以顯示具有無法存取的安裝路徑的磁碟區和具有預設匯出策略的磁碟區。

建立報告以查看具有無法存取的掛載路徑的捲

您可以建立報告來尋找具有無法存取的安裝路徑的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟為具有不可存取的安裝路徑的磁碟區建立自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「NFS 共用」。
2. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
3. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 掛載路徑活動為否
4. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“Volumes with an inaccessible mount path”，然後按一下複選標記 (✓)。
5. 點擊庫存頁面上的“計劃報告”按鈕。
6. 按一下「新增計畫」為「報表計畫」頁面新增一行，以便您可以定義新報表的計畫特性。
7. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要修正無法存取的掛載路徑。

建立報告以查看使用預設匯出策略的捲

您可以建立報告來尋找使用預設匯出策略的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟為使用預設匯出策略的磁碟區建立自訂視圖，然後計劃為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」 > 「**NFS 共用**」。
2. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
3. 將「匯出策略」列拖曳到「磁碟區」列附近。
4. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 導出策略包含預設
5. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“具有預設匯出策略的磁碟區”，然後按一下複選標記 (✓)。
6. 點擊庫存頁面上的“計劃報告”按鈕。
7. 按一下「新增計畫」為「報表計畫」頁面新增一行，以便您可以定義新報表的計畫特性。
8. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要配置自訂匯出策略。

自訂儲存虛擬機器報告

您可以建立儲存虛擬機器報告來分析磁碟區資訊並查看整體運作狀況和儲存可用性。例如，您可以建立報表來顯示達到最大磁碟區數的 SVM 並分析已停止的 SVM。

建立報表以查看達到最大磁碟區限制的儲存虛擬機

您可以建立報表來尋找達到最大容量限制的 SVM。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖，顯示達到最大磁碟區限制的儲存虛擬機，然後排定為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」 > 「儲存虛擬機器」。
2. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
3. 將「磁碟區數」和「最大允許磁碟區」欄位拖曳到「儲存虛擬機器」欄位附近。
4. 按一下「允許的最大磁碟區」列的頂部，按卷數最多對結果進行排序。
5. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如“SVM 達到最大磁碟區”，然後按一下複選標記 (✓)。
6. 點擊庫存頁面上的“計劃報告”按鈕。
7. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
8. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要平衡指派給儲存虛擬機器的捲，或者如果可能，請使用ONTAP系統管理員變更允許的最大磁碟區數。

建立報告以查看已停止的儲存虛擬機

您可以建立報表來顯示所有已停止的 SVM 的清單。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立顯示已停止的儲存虛擬機器的自訂視圖，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「儲存虛擬機器」。
2. 在「檢視」功能表中，選擇「健康」>「所有儲存虛擬機器」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「狀態」列拖曳到「儲存 VM」列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 狀態已停止
6. 使用反映視圖顯示內容的特定名稱儲存視圖，例如“Stopped SVM”，然後按一下複選標記(✓)。
7. 點擊庫存頁面上的“計劃報告”按鈕。
8. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
9. 輸入報告計畫的名稱並填寫其他報告字段，然後按一下複選標記(✓)位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要調查 SVM 停止的原因，以確定是否應該重新啟動已停止的 SVM。

自訂數量關係報告

透過卷宗關係庫存報告，您可以分析叢集中的儲存庫存詳細信息，了解磁碟區所需的保護程度，並根據故障來源、模式和計劃過濾磁碟區詳細資訊。

建立報表以按故障來源對磁碟區關係進行分組

您可以建立一個報告，根據關係處於不健康狀態的原因將磁碟區分組。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立按故障來源對磁碟區進行分組的自訂視圖，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。

2. 在「檢視」功能表中，選擇「關係」>「所有關係」。
3. 選擇“顯示/隱藏”以確保“關係健康”和“不健康原因”列出現在視圖中。

新增或刪除其他欄位以建立對您的報表很重要的視圖。

4. 將「關係健康」和「不健康原因」欄位拖曳到「狀態」欄位附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 關係健康狀況不佳
6. 按一下「不健康原因」列的頂部，按故障來源將磁碟區關係分組。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「Vol relationships by failure」。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以調查每種故障的來源和影響。

建立報告以按問題對卷宗關係進行分組

您可以建立一個按問題對磁碟區關係進行分組的報表。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立按問題對磁碟區關係進行分組的自訂視圖，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「關係」>「所有關係」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「不健康原因」欄位拖曳到「狀態」列附近。
5. 按一下「不健康原因」列的頂部，按問題將磁碟區分組。
6. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「Vol relationships by issue」。
7. 點擊庫存頁面上的“計劃報告”按鈕。
8. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以調查每種問題的來源和影響。

建立報表以查看特定時間間隔的傳輸量趨勢

您可以建立一個報表來顯示特定時間間隔內的傳輸量趨勢。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟為特定時間間隔的磁碟區建立自訂視圖，然後排程為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「關係」>「過去 1 個月的轉移狀態」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將傳輸持續時間列拖曳到「操作結果」列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 過去 7 天內的轉移結束時間
6. 按一下「傳輸持續時間」列的頂部，按時間間隔對磁碟區進行排序。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按持續時間劃分的磁碟區」。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 輸入報告計畫的名稱，將頻率設為*每週*，並完成其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以調查傳輸時間間隔。

建立報表以查看失敗或成功的磁碟區傳輸

您可以建立一個顯示磁碟區傳輸狀態的報表。您可以在此報告中查看失敗和成功的捲傳輸。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立自訂視圖來顯示哪些傳輸失敗以及哪些傳輸成功，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「關係」>「過去 1 個月的轉移狀態」。
3. 選擇“顯示/隱藏”以刪除報告中不需要的任何列。
4. 將「操作結果」列拖曳到「狀態」列附近。
5. 按一下「操作結果」列的頂部，按狀態對磁碟區進行排序。
6. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按傳輸狀態劃分的磁碟區」。
7. 點擊庫存頁面上的“計劃報告”按鈕。
8. 輸入報告計畫的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以調查轉移狀態。

建立報表以根據傳輸大小查看傳輸量

您可以建立報表來根據傳輸大小查看傳輸量。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟根據傳輸大小建立磁碟區傳輸的自訂視圖，然後排定為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」選單中，選擇「關係」>「過去 1 個月的轉移率」。
3. 按一下「總傳輸大小」列的頂部，按大小對磁碟區傳輸進行排序。
4. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按傳輸大小劃分的磁碟區」。
5. 點擊庫存頁面上的“計劃報告”按鈕。
6. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以按傳輸大小調查卷關係。

建立報表以查看按天分組的傳輸量

您可以建立報表來查看按天分組的傳輸量。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟建立按天分組的批次傳輸自訂視圖，然後安排為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」選單中，選擇「關係」>「過去 1 個月的轉移率」。
3. 按一下「天」列頂部可按天對交易量轉移進行排序。
4. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「按天傳輸量」。
5. 點擊庫存頁面上的“計劃報告”按鈕。
6. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可以按天調查交易量轉移。

自訂磁碟區效能報告

這些範例自訂報表用於協助您識別和回應與磁碟區效能相關的潛在問題。

建立報表以查看未啟用FabricPool的聚合上具有大量冷資料的捲

您可以建立報表來顯示非FabricPool聚合上具有大量冷資料的磁碟區。這可以幫助您識別應移動到FabricPool聚合的磁碟區。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟為未啟用FabricPool的聚合上具有大量冷資料的磁碟區建立自訂視圖，然後計劃為該視圖產生報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 在「檢視」功能表中，選擇「效能」>「所有磁碟區」。
3. 選擇“顯示/隱藏”以確保“磁碟類型”列出現在視圖中。

新增或刪除其他欄位以建立對您的報表很重要的視圖。

4. 將“磁碟類型”列拖曳到“冷資料”列附近。
5. 點擊過濾器圖標，添加以下過濾器，然後點擊*應用過濾器*：
 - 冷數據大於 100 GB
 - 磁碟類型包含 SSD
6. 按一下「磁碟類型」列的頂部，按磁碟類型對磁碟區進行排序，以便磁碟類型 SSD (FabricPool) 位於底部。
7. 使用反映視圖所顯示內容的特定名稱儲存視圖，例如「Cold data vols not FabricPool」。
8. 點擊庫存頁面上的“計劃報告”按鈕。
9. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報表中顯示的結果，您可以找到適合移動到FabricPool聚合的磁碟區。

Microsoft Excel 報表範例

這些 Microsoft Excel 範例報表旨在介紹使用 Excel 進階功能可用的報表選項。

Excel 的進階功能可根據您的需求建立各種各樣的報表。有關如何使用 Excel 的完整信息，請參閱產品文件。



您必須具有應用程式管理員或儲存管理員角色才能管理報告。

建立報表以顯示聚合容量表和圖表

您可以使用總計和叢集長條圖格式在 Excel 檔案中建立報表來分析容量。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。


使用下列步驟開啟「執行狀況：所有聚合」視圖，在 Excel 中下載視圖，建立可用容量圖表，上傳自訂 Excel 文件，並安排最終報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 選擇*報表* > 下載 **Excel**。



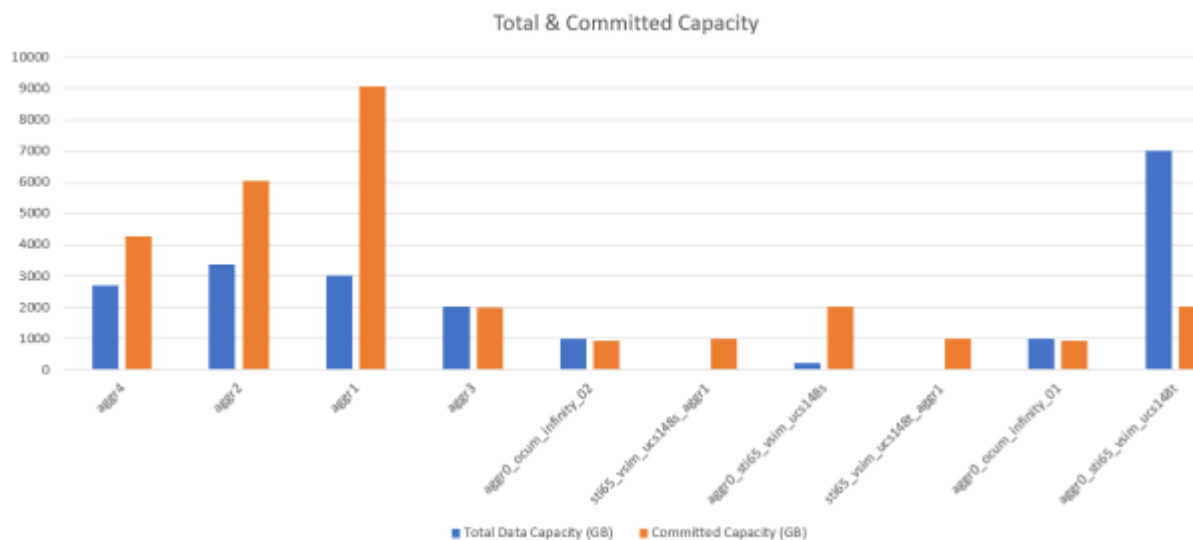
根據您的瀏覽器，您可能需要按一下「確定」來儲存檔案。

3. 如果需要，請按一下「啟用編輯」。
4. 在 Excel 中開啟下載的檔案。
5. 建立新工作表 () 之後 `data` 表並將其命名為*總資料容量*。
6. 在新的「總資料容量」表中新增以下列：
 - a. 總數據容量 (GB)
 - b. 承諾容量 (GB)
 - c. 已使用數據容量 (GB)
 - d. 可用資料容量 (GB)
7. 在每一列的第一行中，輸入以下公式，確保它引用資料表 (資料!)，並引用捕獲資料的正確列和行說明符 (總資料容量從 E 列、第 2 行到第 20 行提取資料)。
 - a. =SUM (數據!E\$2:數據!E\$20)
 - b. =SUM (數據!F\$2:數據!F\$50)
 - c. =SUM (數據!G\$2:數據!G\$50)
 - d. =SUM(數據!H\$2:數據!H\$50)

此公式根據當前資料對每一列進行總計。

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. 在資料表上，選擇*總資料容量 (GB) *和*承諾容量 (GB) *列。
2. 從*插入*選單中選擇*建議圖表*，然後選擇*簇狀長條圖*。
3. 右鍵單擊圖表並選擇*移動圖表*將圖表移動到 `Total Data Capacity` 床單。
4. 使用選擇圖表時可用的「設計」和「格式」選單，您可以自訂圖表的外觀。
5. 滿意後，儲存包含變更的檔案。請勿更改檔案名稱或位置。



6. 在 Unified Manager 中，選擇 報表 > 上傳 **Excel**。



確保您處於下載 Excel 檔案的相同視圖中。

7. 選擇您已修改的 Excel 檔案。
8. 按一下“開啟”。
9. 點選“提交”。

報表 > 上傳 **Excel** 選單項目旁邊會出現一個複選標記。

Scheduled Reports		Reports	Show / Hide
IOPS	MB/s		Utilization
1.8 IOPS	1.54 MB/s	Download CSV	4%
918 IOPS	43.3 MB/s	Download PDF	< 1%
120 IOPS	7.99 MB/s	Download Excel	< 1%
		Upload Excel ✓	

- 按一下“計劃報告”。
- 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。



為報告選擇 **XLSX** 格式。

- 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要研究如何最好地利用整個網路的可用容量。

建立報表以顯示總計與可用容量圖表

您可以建立報告，以 Excel 圖表格式分析儲存總量和已提交容量。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用以下步驟開啟「運行狀況：所有聚合」視圖，在 Excel 中下載該視圖，建立總容量和承諾容量圖表，上傳自訂 Excel 文件，並安排最終報告。

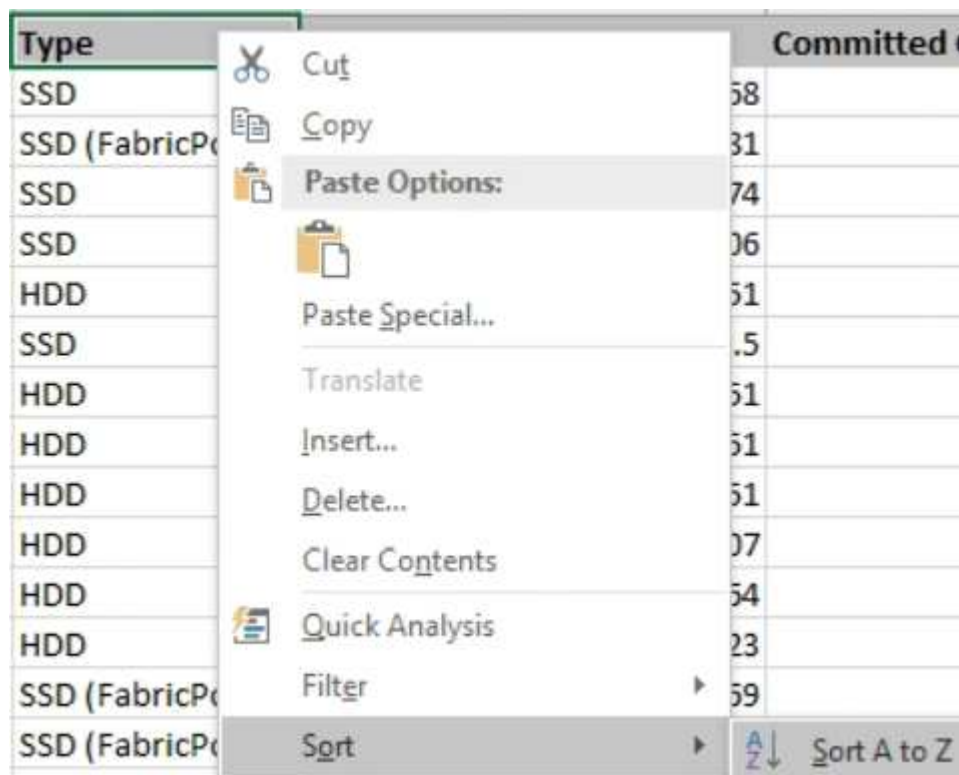
步驟

- 在左側導覽窗格中，按一下「儲存」>「聚合」。
- 選擇*報表* > 下載 **Excel**。



根據您的瀏覽器，您可能需要按一下「確定」來儲存檔案。

3. 在 Excel 中開啟下載的檔案。
4. 如果需要，請按一下「啟用編輯」。
5. 在資料表上，右鍵單擊類型列並選擇*排序* > 按 **A** 到 **Z** 排序。



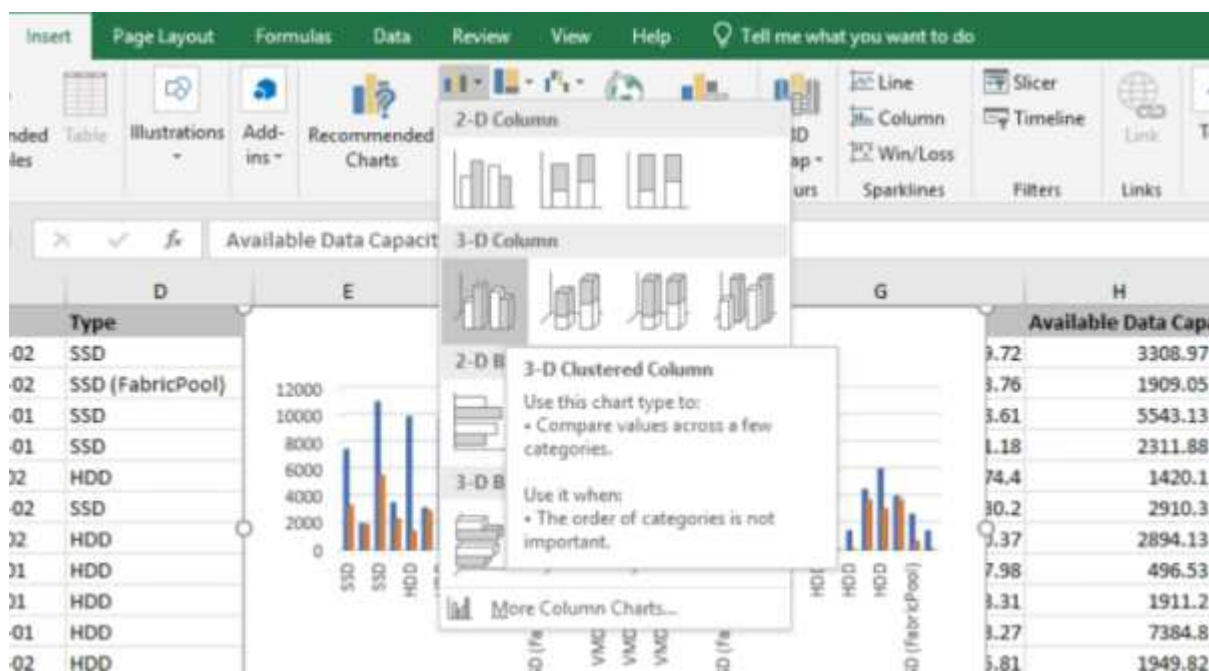
這將按存儲類型排列您的數據，例如：

- 硬碟
- 雜交種
- 固態硬碟
- SSD (FabricPool)

6. 選擇 `Type, Total Data Capacity,` 和 `Available Data Capacity` 列。

7. 在「插入」功能表上，選擇「3-D column」圖表。

該圖表出現在數據表上。



8. 右鍵單擊圖表並選擇「移動圖表」。

9. 選擇「新工作表」並將工作表命名為「總儲存圖表」。

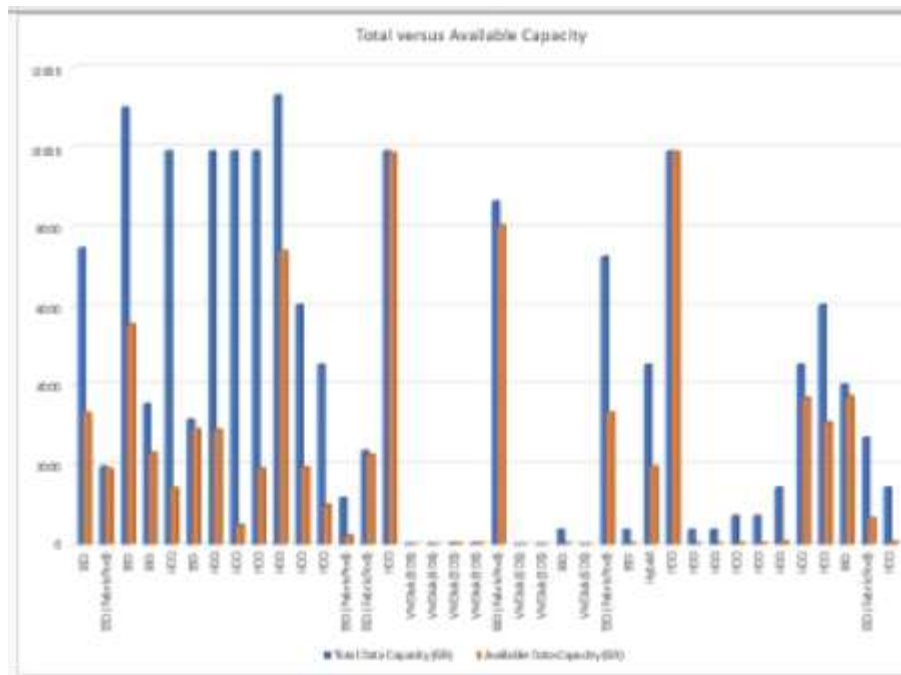


確保新表出現在資訊和資料表之後。

10. 將圖表標題命名為「總容量與可用容量」。

11. 使用選擇圖表時可用的「設計」和「格式」選單，您可以自訂圖表的外觀。

12. 滿意後，儲存包含變更的檔案。請勿更改檔案名稱或位置。



13. 在 Unified Manager 中，選擇 報表 > 上傳 **Excel**。



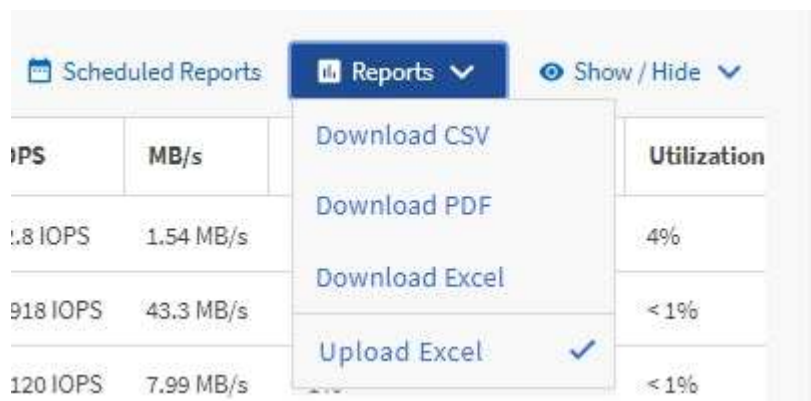
確保您處於下載 Excel 檔案的相同視圖中。

14. 選擇您已修改的 Excel 檔案。

15. 按一下“開啟”。

16. 點選“提交”。

報表 > 上傳 **Excel** 選單項目旁邊會出現一個複選標記。



17. 按一下“計劃報告”。

18. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。



為報告選擇 **XLSX** 格式。

19. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報表中顯示的結果，您可能需要平衡聚合上的負載。

建立報表以查看可用磁碟區容量圖表

您可以建立報表來分析 Excel 圖表中的可用磁碟區容量。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟開啟「執行狀況：所有磁碟區」視圖，在 Excel 中下載視圖，建立可用容量圖表，上傳自訂 Excel 文件，並安排最終報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「磁碟區」。
2. 選擇*報表* > 下載 **Excel**。



根據您的瀏覽器，您可能需要按一下「確定」來儲存檔案。

3. 如果需要，請按一下「啟用編輯」。
4. 在 Excel 中開啟下載的檔案。
5. 在 data` 在工作表中，選擇要使用的數據 `Volume` 和 `Available Data%` 列。
6. 在「插入」功能表上，選擇 3-D piechart.

此圖表顯示哪些磁碟區具有最大的可用空間。該圖表出現在數據表上。

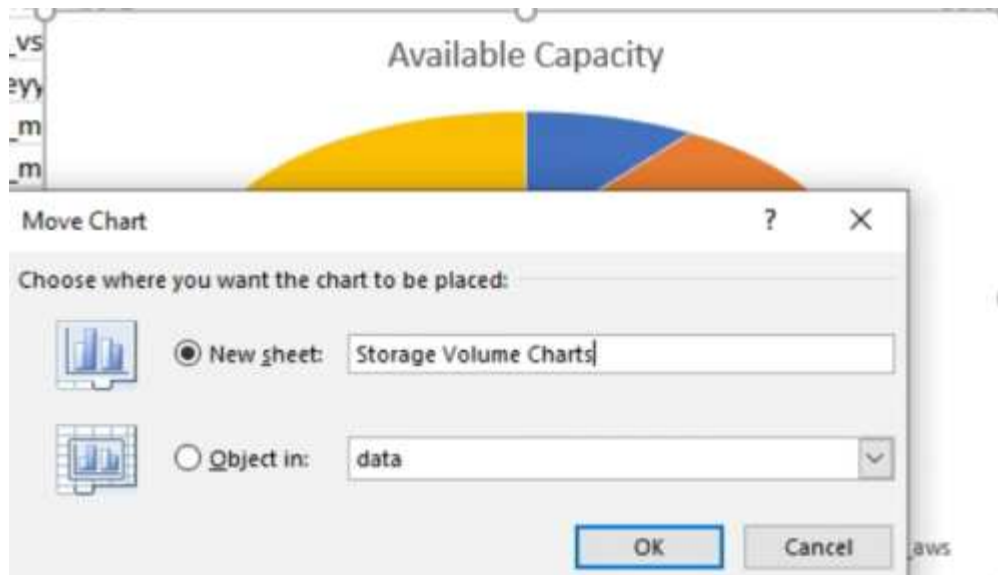


根據您的網路配置，選擇整列或太多資料行可能會導致圓餅圖無法讀取。此範例使用三維餅圖，但您可以使用任何圖表類型。使用最能顯示您想要捕捉的數據的圖表。

7. 將圖表標題命名為「可用容量」。
8. 右鍵單擊圖表並選擇*移動圖表*。
9. 選擇「新工作表」並將工作表命名為「儲存量圖表」。



確保新表出現在資訊和資料表之後。

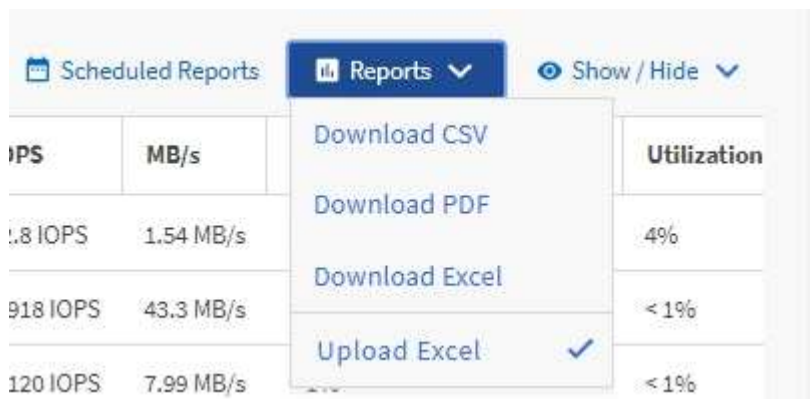


10. 使用選擇圖表時可用的「設計」和「格式」選單，您可以自訂圖表的外觀。
11. 滿意後，儲存包含變更的檔案。
12. 在 Unified Manager 中，選擇 報表 > 上傳 **Excel**。


 確保您處於下載 Excel 檔案的相同視圖中。

13. 選擇您已修改的 Excel 檔案。
14. 按一下“開啟”。
15. 點選“提交”。

報表 > 上傳 **Excel** 選單項目旁邊會出現一個複選標記。



16. 按一下“計劃報告”。
17. 按一下「新增計畫」為「報告計畫」頁面新增一行，以便您可以定義新報告的計畫特徵。
18. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。

 為報告選擇 **XLSX** 格式。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能需要平衡磁碟區上的負載。

建立報表以查看具有最多可用 IOPS 的聚合

此報告顯示哪些聚合具有每種聚合類型最多的可用 IOPS，您可以在其上配置新的工作負載。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。

使用下列步驟開啟「執行狀況：所有磁碟區」視圖，在 Excel 中下載視圖，建立可用容量圖表，上傳自訂 Excel 文件，並安排最終報表。

步驟

1. 在左側導覽窗格中，按一下「儲存」>「聚合」。
2. 從「檢視」下拉式選單中選擇「效能：所有聚合」。
3. 選擇「顯示/隱藏」以顯示 `Available IOPS` 列並隱藏 `Cluster FQDN, Inactive Data Reporting,` 和 `Threshold Policy` 列。
4. 拖放 `Available IOPS` 和 `Free Capacity` 旁邊的列 `Type` 柱子。
5. 命名並儲存自訂視圖 Available IOPS Per Aggr.
6. 選擇*報表* > 下載 **Excel**。



根據您的瀏覽器，您可能需要按一下「確定」來儲存檔案。

7. 如果需要，請按一下「啟用編輯」。
8. 在 Excel 中開啟下載的檔案。
9. 在資料表上，按一下表左上角的小三角形以選擇整個表。
10. 在「資料」功能區中，從「排序」中選擇 Sort & Filter area.
11. 設定以下排序級別：
 - a. 將*排序依據*指定為 Available IOPS (IOPS)，*排序依據*為 Cell Values, 並且*訂單*為 `Largest to Smallest`.

- b. 按一下“新增等級”。
- c. 將*排序依據*指定為 Type，*排序依據*為 Cell Values，`並且*訂單*為 `Z to A。
- d. 按一下“新增等級”。
- e. 將*排序依據*指定為 Free Capacity (GB)，排序依據 Cell Values，`並且*訂單*為 `Largest to Smallest。
- f. 按一下“確定”。

12. 儲存並關閉 Excel 文件。

13. 在 Unified Manager 中，選擇 報表 > 上傳 **Excel**。



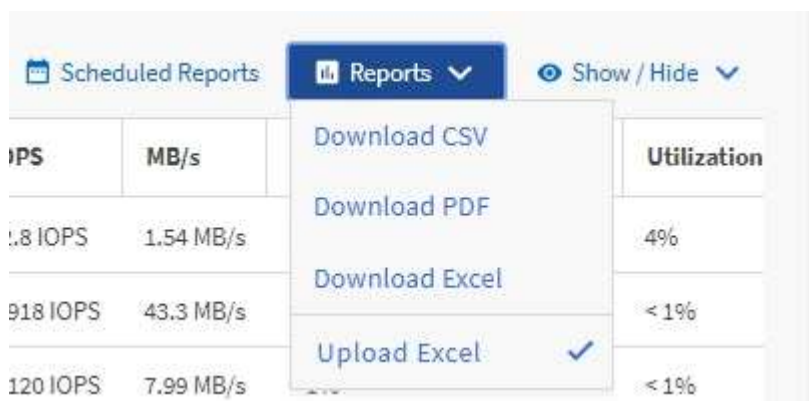
確保您處於下載 Excel 檔案的相同視圖中。

14. 選擇您修改過的 Excel 文件，在本例中 performance-aggregates-<date>.xlsx。

15. 按一下“開啟”。

16. 點選“提交”。

報表 > 上傳 **Excel** 選單項目旁邊會出現一個複選標記。



17. 按一下“計劃報告”。

18. 按一下「新增計劃」以新增一行至「報表計畫」頁面，以便您可以定義新報告的計畫特徵。

19. 輸入報告計劃的名稱並填寫其他報告字段，然後按一下複選標記 (✓) 位於行尾。



為報告選擇 **XLSX** 格式。

該報告將立即發送以進行測試。此後，將產生報告並透過電子郵件發送給使用指定頻率列出的收件者。

根據報告中顯示的結果，您可能想要在具有最大可用 IOPS 的聚合上配置新的工作負載。

使用 REST API 管理存儲

開始使用Active IQ Unified Manager REST API

Active IQ Unified Manager提供了一組 API，透過 RESTful Web 服務介面管理支援儲存系統上的儲存資源，以實現任何第三方整合。

在這些主題中，您將找到有關 Unified Manager API、解決特定問題的範例工作流程以及一些範例程式碼的資訊。利用這些訊息，您可以建立NetApp Manageability 軟體解決方案的 RESTful 用戶端來管理NetApp系統。API 是基於表述性狀態轉移 (REST) 架構風格。支援所有四種 REST 操作：建立、讀取、更新和刪除（也稱為 CRUD）。

看["Active IQ Unified Manager"](#)有關Active IQ Unified Manager REST API 優勢的更多資源和詳細資訊。

此內容的受眾

此處的主題適用於建立透過 REST API 與Active IQ Unified Manager軟體互動的應用程式的開發人員。

儲存管理員和架構師可以參考這些資訊來基本了解如何使用 Unified Manager REST API 建立用戶端應用程式來管理和監控NetApp儲存系統。

如果您想使用儲存提供者、ONTAP叢集和管理管理 API 來管理存儲，則應該使用此資訊。



您必須具有以下角色之一：操作員、儲存管理員或應用程式管理員。您必須知道要在其上執行 REST API 的 Unified Manager 伺服器的 IP 位址或完全限定網域名稱。

Active IQ Unified Manager API 存取權和類別

Active IQ Unified Manager API 可讓您管理和配置環境中的儲存物件。您也可以存取 Unified Manager Web UI 來執行其中一些功能。

建立 URL 以直接存取 REST API

您可以透過程式語言（例如 Python、C#、C++、JavaScript 等）直接存取 REST API。輸入主機名稱或 IP 位址以及用於存取 REST API 的 URL，格式如下

`https://<主機名稱>/api`



預設連接埠為 443。您可以根據環境的需求配置連接埠。

存取線上 API 文件頁面

您可以存取隨產品打包的 API 文件_參考內容頁面，展示 API 文檔，也可以手動啟動 API 呼叫（例如在介面上，Swagger）。您可以透過點擊「功能表列」>「說明按鈕」>「API 文件」來存取此文檔

或者，輸入主機名稱或 IP 位址以及 URL 以存取 REST API 頁面，格式如下

<https://<主機名稱>/docs/api/>

類別

API 呼叫根據區域或類別按功能進行組織。若要找到特定的 API，請按一下適用的 API 類別。

Unified Manager 提供的 REST API 可協助您執行管理、監控和設定功能。API 分為以下類別。

- 資料中心

此類別包含幫助您使用工具（例如工作流程自動化和 Ansible）進行資料中心儲存管理和分析的 API。此類別下的 REST API 提供有關資料中心中的叢集、節點、聚合、磁碟區、LUN、檔案共用、命名空間和其他元素的資訊。

- 管理伺服器

management-server 類別下的 API 包含 `jobs`、`system`、和 `events` 蜜蜂。作業是計畫非同步執行的與管理 Unified Manager 上的儲存物件或工作負載相關的操作。這 `events` API 傳回資料中心中的事件，並且 `system` API 傳回 Unified Manager 實例詳細資料。

- 儲存提供者

此類別包含管理和設定檔共用、LUN、效能服務等級和儲存效率策略所需的所有設定 API。API 還可讓您設定存取端點、Active Directory，以及在儲存工作負載上指派效能服務等級和儲存效率原則。

- 行政

此類別包含用於執行管理任務的 API，例如維護備份設定、查看 Unified Manager 資料來源的信任庫憑證以及將 ONTAP 叢集作為 Unified Manager 的資料來源進行管理。

- 網關

Unified Manager 可讓您透過網關類別下的 API 呼叫 ONTAP REST API 並管理資料中心中的儲存物件。

- 安全

此類別包含用於管理 Unified Manager 使用者的 API。

Active IQ Unified Manager 中提供的 REST 服務

在開始使用 Active IQ Unified Manager API 之前，您應該先了解所提供的 REST 服務和操作。

用於設定 API 伺服器的設定和管理 API 支援讀取（GET）或寫入（POST、PATCH、DELETE）操作。以下是 API 支援的 GET、PATCH、POST 和 DELETE 作業的一些範例：

- GET 範例：`GET /datacenter/cluster/clusters` 檢索資料中心中的群集詳細資訊。傳回的最大記錄數 `GET` 操作為 1000。



API 可讓您根據支援的屬性對記錄進行過濾、排序和排列。

- POST 範例：`POST /datacenter/svm/svms` 建立自訂儲存虛擬機器 (SVM)。
- PATCH 範例：`PATCH /datacenter/svm/svms/{key}` 使用其唯一鍵修改 SVM 的屬性。
- 刪除範例：`DELETE /storage-provider/access-endpoints/{key}` 使用其唯一金鑰從 LUN、SVM 或檔案共用中刪除存取端點。

可以使用 API 執行的 REST 操作取決於操作員、儲存管理員或應用程式管理員使用者的角色。

使用者角色	支援的 REST 方法
操作員	對資料的唯讀存取。具有此角色的使用者可以執行所有 GET 請求。
儲存管理員	讀取所有資料的權限。具有此角色的使用者可以執行所有 GET 請求。 此外，他們還具有寫入存取權（執行 PATCH、POST 和 DELETE 請求）來執行特定活動，例如管理、儲存服務物件和儲存管理選項。
應用程式管理員	對所有資料的讀寫存取。具有此角色的使用者可以對所有功能執行 GET、PATCH、POST 和 DELETE 請求。

有關所有 REST 操作的更多信息，請參閱_線上 API 文件_。

Active IQ Unified Manager 中的 API 版本

Active IQ Unified Manager 中的 REST API URI 指定了版本號。例如，`/v2/datacenter/svm/svms` 版本號 `v2` 在 `/v2/datacenter/svm/svms` 表示特定版本中使用的 API 版本。版本號碼透過發回客戶端可以處理的回應來最大限度地減少 API 變更對客戶端軟體的影響。

此版本號的數位部分隨著版本的發布而遞增。帶有版本號的 URI 提供了一致的接口，以保持未來版本的向後相容性。例如，您也可以找到沒有版本的相同 API `/datacenter/svm/svms` 表示沒有版本的基本 API。基礎 API 始終是最新版本的 API。



在您的 Swagger 介面右上角，您可以選擇要使用的 API 版本。預設選擇最高版本。建議您使用 Unified Manager 實例中可用的特定 API 的最高版本（就增量整數而言）。

對於所有請求，您必須明確要求要使用的 API 版本。當指定版本號時，服務不會傳回您的應用程式未設計處理的回應元素。在 REST 請求中，您應該包含版本參數。早期版本的 API 在幾次發布後最終會被棄用。在此版本中，`v1` 該 API 的版本已被棄用。

ONTAP 中的儲存資源

ONTAP 中的儲存資源大致可分為_實體儲存資源_和_邏輯儲存資源_。若要使用 Active IQ Unified Manager 中提供的 API 有效管理 ONTAP 系統，您必須了解儲存資源模型以及各種

儲存資源之間的關係。

- 實體儲存資源

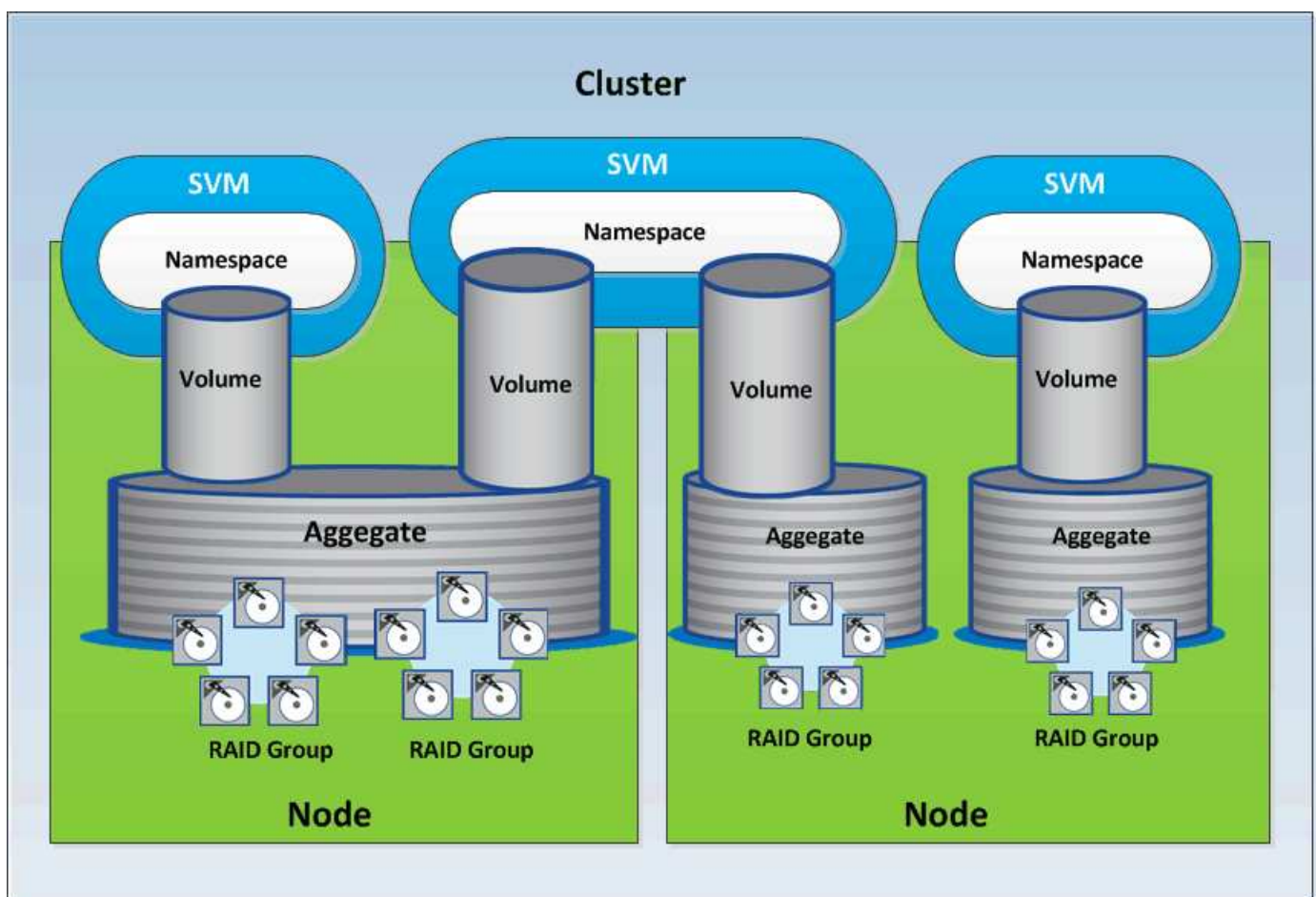
指ONTAP提供的實體儲存物件。實體儲存資源包括磁碟、叢集、儲存控制器、節點和聚合。

- 邏輯儲存資源

指ONTAP提供的不與實體資源綁定的儲存資源。這些資源與儲存虛擬機器（SVM，以前稱為 Vserver）相關聯，並且它們獨立於任何特定的實體儲存資源（例如磁碟、陣列 LUN 或聚合）而存在。

邏輯儲存資源包括所有類型和 qtree 的捲，以及可以與這些資源一起使用的功能和配置，例如 Snapshot 副本、重複資料刪除、壓縮和配額。

下圖顯示了雙節點叢集中的儲存資源：



Active IQ Unified Manager中的 REST API 存取權和身分驗證

可以使用任何能夠透過基本 HTTP 驗證機制發出 HTTP 要求的 REST 用戶端或程式設計平台存取Active IQ Unified Manager REST API。

範例請求和回應：

- 要求

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

• 回覆

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
```

```

        "minor": 0
    },
    "model": "FAS8040",
    "uptime": 13924095,
    "serial_number": "701424000157"
},
{
    "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
    "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
    "name": "fas8040-206-21-02",
    "_links": {
        "self": {
            "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
        }
    },
    "location": null,
    "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
    },
    "model": "FAS8040",
    "uptime": 14012386,
    "serial_number": "701424000564"
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
    }
}
}
},

```

- `IP address/hostname` 是 API 伺服器的 IP 位址或完全限定網域名稱 (FQDN)。
- 埠 443

443 是預設 HTTPS 連接埠。如果需要，您可以自訂 HTTPS 連接埠。

若要從 Web 瀏覽器發出 HTTP 請求，您必須使用 REST API 瀏覽器外掛程式。您也可以使用 cURL 和 Perl 等腳本平台存取 REST API。

驗證

Unified Manager 支援 API 的基本 HTTP 驗證方案。為了確保資訊流（請求和回應）的安全，REST API 只能透過 HTTPS 存取。API 伺服器向所有用戶端提供自簽名 SSL 證書，用於伺服器驗證。此證書可以用自訂證書（或 CA 證書）替換。

您必須設定使用者對 API 伺服器的存取權限才能呼叫 REST API。使用者可以是本機使用者（儲存在本機資料庫中的使用者設定檔）或 LDAP 使用者（如果您已將 API 伺服器設定為透過 LDAP 進行驗證）。您可以透過登入 Unified Manager 管理控制台使用者介面來管理使用者存取。

Active IQ Unified Manager 中使用的 HTTP 狀態碼

在執行 API 或解決問題時，您應該注意 Active IQ Unified Manager API 使用的各種 HTTP 狀態碼和錯誤碼。

下表列出了與認證相關的錯誤代碼：

HTTP 狀態碼	狀態代碼標題	描述
200	好的	同步 API 呼叫成功執行後傳回。
201	創建	透過同步呼叫建立新資源，例如 Active Directory 的配置。
202	公認	成功執行設定功能（例如建立 LUN 和檔案共用）的非同步呼叫後返回。
400	無效請求	表示輸入驗證失敗。使用者必須更正輸入，例如請求正文中的有效金鑰。
401	未經授權的請求	您無權查看資源/未經授權。
403	禁止請求	禁止存取您嘗試存取的資源。
404	未找到資源	未找到您嘗試存取的資源。
405	方法不允許	方法不允許。
429	請求過多	當用戶在特定時間內發送過多請求時返回。

HTTP 狀態碼	狀態代碼標題	描述
500	內部伺服器錯誤	內部伺服器錯誤。無法從伺服器取得回應。此內部伺服器錯誤可能是永久性的，也可能不是。例如，如果你運行 `GET` 或者 `GET ALL` 操作並收到此錯誤，建議您重複此操作至少五次。如果是永久性錯誤，則傳回的狀態代碼繼續為 500。如果操作成功，則回傳的狀態碼為 200。

使用Active IQ Unified Manager API 的建議

使用Active IQ Unified Manager中的 API 時，您應該遵循某些建議的做法。

- 為了有效執行，所有回應內容類型必須採用以下格式：

```
application/json
```

- API版本號與產品版本號無關。您應該使用適用於 Unified Manager 實例的最新版本的 API。有關 Unified Manager API 版本的更多信息，請參閱「Active IQ Unified Manager中的 REST API 版本控制」部分。
- 使用 Unified Manager API 更新陣列值時，必須更新整個值字串。您不能將值附加到數組。您只能替換現有陣列。
- 您可以對所有查詢參數使用篩選運算符，例如垂直線 (|) 和通配符 (*)，但雙精確度值除外，例如指標 API 中的 IOPS 和效能。
- 避免使用篩選運算子通配符 (*) 和管道符 (|) 的組合來查詢物件。它可能會檢索到不正確數量的物件。
- 使用值進行過濾時，請確保值不包含任何 `?` 特點。這是為了減輕 SQL 注入的風險。
- 請注意 `GET` 任何 API 的 (all) 請求最多傳回 1000 筆記錄。即使您透過設定 `max_records` 參數設定為高於 1000 的值，則僅傳回 1000 筆記錄。
- 為了執行管理功能，建議您使用 Unified Manager UI。

故障排除日誌

系統日誌可讓您分析故障原因並解決執行 API 時可能出現的問題。

從下列位置檢向日誌以解決與 API 呼叫相關的問題。

日誌位置	使用
/var/log/ocie/access_log.log	包含所有API呼叫詳情，例如呼叫API的使用者的使用者名稱、開始時間、執行時間、狀態、URL等。 您可以使用此日誌檔案檢查常用的 API，或排除任何 GUI 工作流程的故障。您還可以根據執行時間使用它來擴展分析。
/var/log/ocum/ocumserver.log	包含所有 API 執行日誌。 您可以使用此日誌檔案來排除故障和偵錯 API 呼叫。
/var/log/ocie/server.log	包含所有 Wildfly 伺服器部署和啟動/停止服務相關記錄。 您可以使用此日誌檔案來尋找 Wildfly 伺服器啟動、停止或部署期間發生的任何問題的根本原因。
/var/log/ocie/au.log	包含採集單元相關日誌。 當您在ONTAP中建立、修改或删除任何物件但這些物件不會反映在Active IQ Unified Manager REST API 中時，您可以使用此記錄檔。

Job物件異步進程

Active IQ Unified Manager提供 `jobs` API 會擷取有關在執行其他 API 時執行的作業的資訊。您必須知道如何使用作業對象進行非同步處理。

某些 API 呼叫（尤其是用於新增或修改資源的呼叫）可能比其他呼叫需要更長的時間才能完成。Unified Manager 非同步處理這些長時間運行的要求。

使用 **Job** 物件描述的非同步請求

進行非同步運行的 API 呼叫後，HTTP 回應代碼 202 表示請求已成功驗證並接受，但尚未完成。該請求將作為後台任務處理，並在客戶端收到初始 HTTP 回應後繼續執行。回應中包含錨定該請求的 Job 物件及其唯一識別碼。

查詢與 **API** 請求關聯的 **Job** 對象

HTTP 回應中傳回的 Job 物件包含多個屬性。您可以查詢 state 屬性來決定請求是否已成功完成。Job物件可以處於以下狀態之一：

- NORMAL
- WARNING
- PARTIAL_FAILURES
- ERROR

輪詢 Job 物件來偵測任務的最終狀態（成功或失敗）時，可以使用兩種技術：

- 標準輪詢請求：立即返回目前作業狀態。
- 長輪詢請求：當作業狀態轉移到 NORMAL, ERROR, 或者 PARTIAL_FAILURES.

非同步請求中的步驟

您可以使用下列進階程序來完成非同步 API 呼叫：

1. 發出異步 API 呼叫。
2. 收到 HTTP 回應 202，表示成功接受請求。
3. 從回應主體中提取 Job 物件的識別碼。
4. 在循環中，等待 Job 物件達到終止狀態 NORMAL, ERROR, 或者 PARTIAL_FAILURES.
5. 驗證作業的最終狀態並擷取作業結果。

你好 API 伺服器

Hello API server 是一個範例程序，示範如何使用簡單的 REST 用戶端呼叫Active IQ Unified Manager中的 REST API。範例程式以 JSON 格式向您提供有關 API 伺服器的基本詳細資訊（伺服器僅支援 `application/json` 格式）。

使用的 URI 是：`https://<hostname>/api/datacenter/svm/svms.` 此範例程式碼採用以下輸入參數：

- API 伺服器 IP 位址或 FQDN
- 可選：連接埠號碼（預設值：443）
- 使用者名稱
- 密碼
- 回應格式(application/json)

若要呼叫 REST API，您也可以使用其他腳本（例如 Jersey 和 RESTEasy）為Active IQ Unified Manager編寫 Java REST 用戶端。您應該了解有關範例程式碼的以下注意事項：

- 使用與Active IQ Unified Manager 的HTTPS 連線來呼叫指定的 REST URI
- 忽略Active IQ Unified Manager提供的憑證
- 握手期間跳過主機名稱驗證
- 用途 `javax.net.ssl.HttpURLConnection` 用於 URI 連接
- 使用第三方函式庫(org.apache.commons.codec.binary.Base64) 用於建立 HTTP 基本驗證中使用的 Base64 編碼字串

若要編譯和執行範例程式碼，必須使用 Java 編譯器 1.8 或更高版本。

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
```

```

import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsURLConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +

```

```

response_format);
    String authString = getAuthorizationString();
    connection.setRequestProperty("Authorization", "Basic " +
authString);
    if (connection.getResponseCode() != 200) {
        System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
        System.exit(1);
    }
    BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
    String response;
    System.out.println("Response:");
    while ((response = br.readLine()) != null) {
        System.out.println(response);
    }
    connection.disconnect();
} catch (Exception e) {
    e.printStackTrace();
}
}

/* Print the usage of this sample code */ private static void
printUsage() {
    System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
    System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
    System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
    System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
    System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
    System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
}

/* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
    String[] args) {
    server = args[0];
    user = args[1];
    password = args[2];
    if (server.contains(":")) {

```

```

        String[] parts = server.split(":");
        server = parts[0];
        port = parts[1];
    }
}

/*
 * * Create a trust manager which accepts all certificates and * use
this trust
 * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
 * SSL Context and skip * server hostname verification during SSL
handshake. * *
 * Note: Trusting all certificates or skipping hostname verification *
is not
 * required for API Services to work. These are done here to * keep
this sample
 * REST Client code as simple as possible.
 */ private static HttpsURLConnection
getAllTrustingHttpsURLConnection() {           HttpsURLConnection conn =
null;           try {           /* Creating a trust manager that does not
validate certificate chains */           TrustManager[]
trustAllCertificatesManager = new           TrustManager[]{new
X509TrustManager() {
    public X509Certificate[] getAcceptedIssuers(){return null;}
    public void checkClientTrusted(X509Certificate[]
certs, String authType){}
    public void checkServerTrusted(X509Certificate[]
certs, String authType){}           }};           /* Initialize the
SSLContext with the all-trusting trust manager */
    SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));           URL url = new URL(server_url);           conn =
(HttpsURLConnection) url.openConnection();           /* Do not perform an
actual hostname verification during SSL Handshake.           Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {           public
boolean verify(String host, SSLSession session) {
return true;           }           });           } catch (Exception e)
{           e.printStackTrace();           }           return conn;           }

/*
 * * This forms the Base64 encoded string using the username and
password *

```

```
    * provided by the user. This is required for HTTP Basic
    Authentication.
    */ private static String getAuthorizationString() {
        String userPassword = user + ":" + password;
        byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
        String authString = new String(authEncodedBytes);
        return authString;
    }
}
```

Unified Manager REST API

本節根據類別列出了Active IQ Unified Manager的 REST API。

您可以從 Unified Manager 實例查看線上文件頁面，其中包含每個 REST API 呼叫的詳細資訊。本文檔不重複線上文件的細節。本文檔中列出或描述的每個 API 呼叫僅包含您在文件頁面上找到該呼叫所需的資訊。找到特定的 API 呼叫後，您可以查看該呼叫的完整詳細信息，包括輸入參數、輸出格式、HTTP 狀態代碼和請求處理類型。

工作流程中的每個 API 呼叫都包含以下信息，以幫助在文件頁面上找到該呼叫：

- 類別

API 呼叫在文件頁面上按功能相關區域或類別進行組織。若要找到特定的 API 呼叫，請向下捲動到頁面底部，然後按一下適用的 API 類別。

- HTTP 動詞（呼叫）

HTTP 動詞標識對資源執行的動作。每個 API 呼叫都透過單一 HTTP 動詞執行。

- 小路

路徑決定了操作在執行呼叫時所使用的特定資源。路徑字串會附加到核心 URL 中，以形成標識資源的完整 URL。

使用 API 管理資料中心內的儲存對象

REST API 下的 `datacenter` 類別可讓您管理資料中心中的儲存對象，例如叢集、節點、聚合、儲存虛擬機器、磁碟區、LUN、檔案共用和命名空間。這些 API 可用於查詢物件的配置，其中一些 API 可讓您執行新增、刪除或修改這些物件的操作。

大多數 API 都是 GET 調用，提供跨叢集聚合、過濾、排序和分頁支援。執行這些 API 時，它們會從資料庫傳回資料。因此，新建立的物件需要在下一個獲取週期中被發現並出現在回應中。

如果要查詢特定物件的詳細信息，則需要輸入該物件的唯一 ID 來查看其詳細資訊。例如，有關存儲對象的指標和分析信息，請參閱["查看性能指標"](#)。

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



您的 Swagger API 介面上提供了 CURL 命令、範例、請求和對 API 的回應。您可以按照 Swagger 上指示的特定參數過濾和排序結果。這些 API 可讓您過濾特定儲存物件（例如叢集、磁碟區或儲存 VM）的結果。

資料中心儲存物件的 API

HTTP 動詞	小路	描述
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	您可以使用此方法查看整個資料中心的 ONTAP 叢集的詳細資訊。API 傳回訊息，例如叢集的 IPv4 或 IPv6 位址、有關節點的資訊（例如節點健康狀況、效能容量和高可用性 (HA) 對），並指示叢集是否為全 SAN 陣列。
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	傳回資料中心叢集上安裝的許可證的詳細資訊。您可以根據所需條件篩選結果。傳回許可證密鑰、叢集密鑰、到期日期和許可證範圍等資訊。您可以輸入許可證密鑰來檢索特定許可證的詳細資訊。
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	您可以透過此方法查看資料中心內節點的詳細資訊。您可以查看有關叢集、節點健康狀況、效能容量和節點的高可用性 (HA) 對的資訊。
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	您可以透過此方式查看資料中心內 CIFS 共享的詳細資訊。除了叢集、SVM 和磁碟區詳細資訊之外，還會傳回有關存取控制清單 (ACL) 的資訊。
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	您可以使用此方法查看受支援的 NFS 服務的匯出策略的詳細資訊。 您可以查詢叢集或儲存虛擬機器的導出策略，並重複使用匯出策略金鑰來配置 NFS 檔案共用。有關在工作負載上指派和重複使用匯出策略的更多信息，請參閱「配置 CIFS 和 NFS 檔案共用」。

HTTP 動詞	小路	描述
GET	<pre>/datacenter/storage/aggregates</pre> <pre>/datacenter/storage/aggregates/{key}</pre>	您可以使用此方法查看資料中心中的聚合集合或特定聚合，以便在其上配置工作負載或進行監控。返回叢集和節點詳細資訊、使用的效能容量、可用和已使用空間以及儲存效率等資訊。
GET	<pre>/datacenter/storage/luns</pre> <pre>/datacenter/storage/luns/{key}</pre>	可以透過此方法查看整個資料中心的LUN集合。您可以查看有關LUN的信息，例如叢集和SVM詳細資訊、QoS策略和igroup。
GET	<pre>/datacenter/storage/qos/policies</pre> <pre>/datacenter/storage/qos/policies/{key}</pre>	您可以使用此方法查看適用於資料中心內儲存物件的所有QoS策略的詳細資訊。傳回叢集和SVM詳細資訊、固定或自適應策略詳細資訊以及適用於該策略的物件數量等資訊。
GET	<pre>/datacenter/storage/qtrees</pre> <pre>/datacenter/storage/qtrees/{key}</pre>	您可以使用此方法查看資料中心內所有FlexVol磁碟區或FlexGroup磁碟區的qtree詳細資訊。傳回叢集和SVM詳細資料、FlexVol volume和匯出策略等資訊。
GET	<pre>/datacenter/storage/volumes</pre> <pre>/datacenter/storage/volumes/{key}</pre>	<p>您可以使用此方法查看資料中心中的磁碟區集合。傳回有關磁碟區的信息，例如SVM和叢集詳細資料、QoS和匯出策略，以及磁碟區的類型是讀寫、資料保護或負載共用。</p> <p>對於FlexVol和FlexClone磁碟區，您可以查看有關相應聚合的資訊。對於FlexGroup卷，查詢傳回組成聚合的清單。</p>

HTTP 動詞	小路	描述
GET POST DELETE PATCH	/datacenter/protocols/san/ igroups /datacenter/protocols/san/ igroups/{key}	<p>您可以指派授權存取特定 LUN 目標的啟動器群組 (igroup)。如果存在現有的 igroup，您可以指派它。您也可以建立 igroup 並將其指派給 LUN。</p> <p>您可以分別使用這些方法來查詢、建立、刪除和修改 igroup。</p> <p>注意事項：</p> <ul style="list-style-type: none"> • `POST`：建立 igroup 時，您可以指定要指派存取權限的儲存虛擬機器。 • `DELETE`：您需要提供 igroup 鍵作為輸入參數來刪除特定的 igroup。如果您已經為 LUN 指派了 igroup，則無法刪除該 igroup。 • `PATCH`：您需要提供 igroup 鍵作為輸入參數來修改特定的 igroup。您還必須輸入要更新的屬性及其值。
GET POST DELETE PATCH	/datacenter/svm/svms /datacenter/svm/svms/{key}	<p>您可以使用這些方法來檢視、建立、刪除和修改儲存虛擬機器（儲存 VM）。</p> <ul style="list-style-type: none"> • `POST`：您必須輸入要建立的儲存虛擬機器物件作為輸入參數。您可以建立自訂儲存虛擬機，然後為其指派所需的屬性。 • `DELETE`：您需要提供儲存虛擬機器金鑰來刪除特定的儲存虛擬機器。 • `PATCH`：您需要提供儲存虛擬機器金鑰來修改特定的儲存虛擬機器。您還需要輸入要更新的屬性及其值。



注意事項：

如果您在環境中啟用了基於 SLO 的工作負載配置，則在建立儲存虛擬機器時，請確保它支援配置 LUN 及其文件共用所需的所有協議，例如 CIFS 或 SMB、NFS、FCP 和 iSCSI。如果儲存虛擬機器不支援所需的服務，則配置工作流程可能會失敗。建議在儲存虛擬機器上也啟用對應類型工作負載的服務。

如果您已在環境中啟用基於 SLO 的工作負載配置，則無法刪除已配置儲存工作負載的儲存虛擬機器。當您刪除

已設定 CIFS 或 SMB 伺服器的儲存虛擬機器時，此 API 也會刪除 CIFS 或 SMB 伺服器以及本機 Active Directory 設定。但是，CIFS 或 SMB 伺服器名稱仍會保留在 Active Directory 設定中，您必須將其從 Active Directory 伺服器中手動刪除。

資料中心網路元素的 API

資料中心類別中的以下 API 會擷取有關您環境中的連接埠和網路介面的信息，特別是 FC 連接埠、FC 介面、乙太網路連接埠和 IP 介面。

HTTP 動詞	小路	描述
GET	<pre>/datacenter/network/ethernet/ports</pre> <pre>/datacenter/network/ethernet/ports/{key}</pre>	檢索有關資料中心環境中所有乙太網路連接埠的資訊。使用連接埠鍵作為輸入參數，您可以查看該特定連接埠的資訊。檢索訊息，例如叢集詳細資訊、廣播域、連接埠詳細資訊（例如狀態、速度和類型）以及連接埠是否啟用。
GET	<pre>/datacenter/network/fc/interfaces</pre> <pre>/datacenter/network/fc/interfaces/{key}</pre>	您可以使用此方法查看資料中心環境中 FC 介面的詳細資訊。使用介面鍵作為輸入參數，您可以查看該特定介面的資訊。檢索叢集詳細資訊、主節點詳細資訊和主連接埠詳細資訊等資訊。
GET	<pre>/datacenter/network/fc/ports</pre> <pre>/datacenter/network/fc/ports/{key}</pre>	檢索有關資料中心環境中節點中使用的所有 FC 連接埠的資訊。使用連接埠鍵作為輸入參數，您可以查看該特定連接埠的資訊。檢索叢集詳細資訊、連接埠描述、支援的協定和連接埠狀態等資訊。
GET	<pre>/datacenter/network/ip/interfaces</pre> <pre>/datacenter/network/ip/interfaces/{key}</pre>	您可以使用此方法查看資料中心環境中 IP 介面的詳細資訊。使用介面鍵作為輸入參數，您可以查看該特定介面的資訊。檢索叢集詳細資料、IP 空間詳細資料、主節點詳細資料、是否啟用故障轉移等資訊。

透過代理存取存取ONTAP API

網關 API 為您提供了使用Active IQ Unified Manager憑證執行ONTAP REST API 和管理儲存物件的優勢。當從 Unified Manager Web UI 啟用 API 閘道功能時，這些 API 可用。

Unified Manager REST API 僅支援在 Unified Manager 資料來源（即ONTAP叢集）上執行一組選定的操作。您可以透過ONTAP API 使用其他功能。網關 API 允許 Unified Manager 成為一個直通接口，用於傳輸在其管理的ONTAP叢集上執行的所有 API 請求，而無需單獨登入每個資料中心叢集。它作為單一管理點，在由 Unified Manager 實例管理的ONTAP叢集中執行 API。API 閘道功能可讓 Unified Manager 成為單一控制平面，您可以從中管理多個ONTAP集群，而無需單獨登入它們。網關 API 可讓您保持登入 Unified Manager 並透過執行ONTAP REST API 操作來管理ONTAP叢集。



所有使用者都可以使用 GET 操作執行查詢。應用程式管理員可以執行所有 ONTAP REST 操作。

網關充當代理，透過維護與 ONTAP API 相同的格式的標頭和正文請求來傳輸 API 請求。您可以使用 Unified Manager 憑證並執行特定操作來存取和管理 ONTAP 叢集，而無需傳遞單獨的叢集憑證。它繼續管理叢集身份驗證和叢集管理，但將 API 請求重定向到直接在特定叢集上運行。API 傳回的回應與直接從 ONTAP 執行的對應 ONTAP REST API 傳回的回應相同。

HTTP 動詞	路徑 (URL)	描述
GET	/gateways	<p>此 GET 方法會擷取由 Unified Manager 管理的支援 ONTAP REST 呼叫的所有叢集的清單。您可以驗證叢集詳細資訊並選擇根據叢集 UUID 或通用唯一識別碼 (UUID) 執行其他方法。</p> <p> 網關 API 僅檢索 ONTAP 9.5 或更高版本支援並透過 HTTPS 新增至 Unified Manager 的叢集。</p>
GET POST DELETE PATCH OPTIONS (Swagger 上不可用) HEAD (Swagger 上不可用)	<p>/gateways/{uuid}/{path}</p> <p> {uuid} 的值必須替換為執行 REST 操作的叢集 UUID。此外，請確保 UUID 屬於 ONTAP 9.5 或更高版本支援的集群，並透過 HTTPS 新增至 Unified Manager。 {path} 必須替換為 ONTAP REST URL。您必須刪除 '/api/' 來自 URL。</p>	<p>這是一個單點代理 API，支援所有 ONTAP REST API 的 POST、DELETE、PATCH 操作和 GET。只要受 ONTAP 支持，任何 API 均不受任何限制。隧道或代理功能無法被停用。</p> <p>這 `OPTIONS` 方法傳回 ONTAP REST API 支援的所有操作。例如，如果 ONTAP API 僅支援 `GET` 操作，運行 `OPTIONS` 使用此網關 API 傳回的方法 `GET` 作為回應。Swagger 上不支援此方法，但可以在其他 API 工具上執行。</p> <p>這 `OPTIONS` 方法確定資源是否可用。此操作可用於查看 HTTP 回應頭中有關資源的元資料。Swagger 上不支援此方法，但可以在其他 API 工具上執行。</p>

了解 API 網關隧道

網關 API 可讓您透過 Unified Manager 管理 ONTAP 物件。Unified Manager 管理叢集和身份驗證詳細信息，並將請求重新導向到 ONTAP REST 端點。網關 API 將標頭和回應主體中的 URL 和超媒體轉換為應用程式狀態引擎 (HATEOAS) 連結以及 API 閘道基本 URL。網關 API 可作為代理基本 URL，您可以將 ONTAP REST URL 附加到該 URL 並執行所需的 ONTAP REST 端點。



為了使ONTAP API 能夠透過 API 閘道成功運行，該 API 必須得到其所運行的ONTAP叢集版本的支援。執行ONTAP叢集上不支援的 API 不會傳回任何結果。

在此範例中，網關 API (代理基本 URL) 為： /gateways/{uuid}/

採用的ONTAP API 是： /storage/volumes。您需要新增ONTAP API REST URL 作為路徑參數的值。



新增路徑時，請確保已刪除"/`" symbol at the beginning of the URL. For the API `/storage/volumes, 添加 `storage/volumes.

附加的 URL 是： /gateways/{uuid}/storage/volumes

在運行 GET 操作，產生的URL如下：

```
`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes
```

這 `/api` 附加 URL 中的ONTAP REST URL 標籤被刪除，而網關 API 的標籤被保留。

範例 cURL 指令

```
curl -X GET "https://<hostname>/api/gateways/lcd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

API 傳回該叢集中的儲存磁碟區清單。回應格式與您從ONTAP執行相同 API 時收到的格式相同。傳回的狀態代碼是ONTAP REST 狀態代碼。

設定 API 範圍

所有 API 都在叢集範圍內設定了上下文。基於儲存虛擬機器操作的API也是以叢集為範圍的，即API操作是在被管理的叢集內的特定儲存虛擬機器上執行的。當你運行 `/gateways/{uuid}/{path}` API，請確保輸入執行該操作的叢集的叢集 UUID (Unified Manager 資料來源 UUID)。若要將上下文設定為該叢集內的特定儲存虛擬機，請輸入儲存虛擬機金鑰作為 X-Dot-SVM-UUID 參數或輸入儲存虛擬機名稱作為 X-Dot-SVM-Name 參數。此參數會作為過濾器新增至字串標頭中，並且操作在該叢集內的該儲存虛擬機器範圍內運作。

範例 cURL 指令

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

有關使用ONTAP REST API 的更多信息，請參閱<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP REST API 自動化"]

使用 API 執行管理任務

您可以使用 `administration` 類別來修改備份設定、驗證備份檔案資訊和叢集證書，以及將 ONTAP 叢集作為 Active IQ Unified Manager 資料來源進行管理。



您必須具有應用程式管理員角色才能執行這些操作。您也可以使用 Unified Manager Web UI 設定這些設定。

HTTP 動詞	小路	描述
GET PATCH	<code>/admin/backup-settings</code>	<p>您可以使用 `GET` 方法查看 Unified Manager 中預設配置的備份計畫的設定。您可以驗證以下內容：</p> <ul style="list-style-type: none">• 計畫是否啟用或停用• 計畫備份的頻率（每日或每週）• 備份時間• 應用程式中應保留的最大備份檔案數量 <p>備份時間為伺服器時區。</p> <p>預設情況下，資料庫備份設定在 Unified Manager 上可用，您無法建立備份計畫。但是，您可以使用 `PATCH` 方法來修改預設值。</p>
GET	<code>/admin/backup-file-info</code>	<p>每次修改 Unified Manager 的備份計畫時都會產生備份轉儲檔案。您可以使用此方法來驗證備份檔案是否根據修改後的備份設定生成，以及檔案上的資訊是否與修改後的設定相符。</p>
GET	<code>/admin/datasource-certificate</code>	<p>您可以使用此方法從信任庫中查看資料來源（叢集）憑證。在將 ONTAP 叢集新增為 Unified Manager 資料來源之前，需要先驗證憑證。</p>

HTTP 動詞	小路	描述
GET	/admin/datasources/clusters	您可以使用 `GET` 方法來檢索由 Unified Manager 管理的資料來源 (ONTAP 叢集) 的詳細資訊。
POST	/admin/datasources/clusters/{key}	您也可以將新叢集新增至 Unified Manager 作為資料來源。要新增集群，您必須知道其主機名稱、使用者名稱和密碼。 若要修改和刪除由 Unified Manager 作為資料來源管理的叢集，請使用 ONTAP 叢集金鑰。
PATCH		
DELETE		

使用 API 管理用戶

您可以使用 `security` 類別來控制使用者對 Active IQ Unified Manager 中選取叢集物件的存取。您可以新增本機使用者或資料庫使用者。您也可以新增屬於身份驗證伺服器的遠端使用者或群組。根據您指派給使用者的角色的權限，他們可以管理儲存物件或查看 Unified Manager 中的資料。



您必須具有應用程式管理員角色才能執行這些操作。您也可以使用 Unified Manager Web UI 設定這些設定。

下的 API `security` 類別使用使用者參數（即使用者名稱），而不是鍵參數作為使用者實體的唯一識別碼。

HTTP 動詞	小路	描述
GET	/security/users	您可以使用這些方法來取得使用者的詳細資訊或向 Unified Manager 新增使用者。 您可以根據使用者類型為使用者新增特定角色。新增使用者時，必須提供本機使用者、維護使用者和資料庫使用者的密碼。
POST	/security/users	
GET	/security/users/{name}	GET 方法可讓您檢索使用者的所有詳細信息，例如姓名、電子郵件地址、角色、授權類型。PATCH 方法可讓您更新詳細資訊。DELETE 方法可讓您刪除使用者。
PATCH		
DELETE		

使用 API 查看效能指標

Active IQ Unified Manager 為您提供了一組 API `/datacenter` 類別，使您能夠查看資料中心中的叢集和儲存物件的效能資料。這些 API 會擷取不同儲存物件的效能數據，例如叢集、

節點、LUN、磁碟區、聚合、儲存虛擬機器、FC 介面、FC 連接埠、乙太網路連接埠和 IP 介面。

這 `/metrics` 和 `/analytics` API 提供了效能指標的不同視圖，使用這些視圖，您可以深入了解資料中心中以下儲存物件的不同層級的詳細資訊：

- 叢集
- 節點
- 儲存虛擬機
- 聚合體
- 卷
- LUN
- FC 介面
- FC 連接埠
- 乙太網路埠
- IP 介面

下表對 `/metrics` 和 `/analytics` 與檢索到的效能資料細節有關的 API。

指標	分析
單一物件的效能詳細資訊。例如， <code>/datacenter/cluster/clusters/{key}/metrics</code> API 要求輸入叢集鍵作為路徑參數來檢索該特定叢集的指標。	資料中心內同一類型的多個物件的效能詳細資訊。例如， <code>/datacenter/cluster/clusters/analytics</code> API 檢索資料中心中所有群集的集體指標。
根據檢索的時間間隔參數對儲存物件的效能指標進行採樣。	某一類型儲存物件在一定時期內（72 小時以上）的效能高階聚合值。
檢索物件的基本詳細信息，例如節點或叢集的詳細資訊。	未檢索到具體細節。
檢索單一物件的累積計數器，例如最小值、最大值、第 95 個百分位數和一段時間內的平均效能值，例如讀取、寫入、總計和其他計數器。	對於同一類型的所有對象，將顯示單一聚合值。

指標	分析
<p>時間範圍和樣本資料基於以下時間表：資料的時間範圍。例如 1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m。如果範圍超過 3 天（72 小時），您將獲得 1 小時樣本，否則您將獲得 5 分鐘樣本。每個時間範圍的周期如下：</p> <ul style="list-style-type: none"> • 1 小時：最近 5 分鐘內採樣的一小時內的指標。 • 12h：最近 12 小時內每 5 分鐘採樣一次的指標。 • 1d：最近一天 5 分鐘內採樣的指標。 • 2d：最近 2 天的 5 分鐘採樣指標。 • 3d：最近 3 天的 5 分鐘採樣指標。 • 15d：最近 15 天的 1 小時內採樣的指標。 • 1w：最近一週內 1 小時內採樣的指標。 • 1m：最近一個月內 1 小時內採樣的指標。 • 2m：最近 2 個月內 1 小時內採樣的指標。 • 3m：最近 3 個月內 1 小時內採樣的指標。 • 6m：最近 6 個月內 1 小時內採樣的指標。 <p>可用值：1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m</p> <p>預設值：1h</p>	<p>超過72小時。計算此樣本的持續時間以 ISO-8601 標準格式表示。</p>

指標 **API** 的輸出範例

例如，`/datacenter/cluster/nodes/{key}/metrics` API 檢索節點的以下詳細資訊（以及其他資訊）：



摘要值中的 95 分位數表示該期間收集的 95% 樣本的計數器值小於指定的 95 分位數。

```
{
  "iops": {
    "local": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  }
}
```

```

    },
    "latency": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "performance_capacity": {
      "available_iops_percent": 0,
      "free_percent": 0,
      "system_workload_percent": 0,
      "used_percent": 0,
      "user_workload_percent": 0
    },
    "throughput": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "timestamp": "2018-01-01T12:00:00-04:00",
    "utilization_percent": 0
  }
],
"start_time": "2018-01-01T12:00:00-04:00",
"summary": {
  "iops": {
    "local_iops": {
      "other": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      },
      "read": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      },
      "total": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      }
    },
  },
}

```



```
"write": {  
  "95th_percentile": 28,  
  "avg": 28,  
  "max": 28,  
  "min": 5  
}  
,
```

分析 **API** 的輸出範例

例如， `/datacenter/cluster/nodes/analytics` API 會擷取所有節點的下列值（以及其他值）：

```

{
  "iops": 1.7471,
  "latency": 60.0933,
  "throughput": 5548.4678,
  "utilization_percent": 4.8569,
  "period": 72,
  "performance_capacity": {
    "used_percent": 5.475,
    "available_iops_percent": 168350
  },
  "node": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "name": "ocum-infinity-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
      }
    }
  },
  "cluster": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
    "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
    "name": "ocum-infinity",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/nodes/analytics"
    }
  }
},
},

```

可用 API 列表

下表描述了 `/metrics` 和 `/analytics` 詳細的 API。



這些 API 傳回的 IOPS 和效能指標都是 double 值，例如 100.53。不支援使用管道符 (|) 和通配符 (*) 過濾這些浮點值。

HTTP 動詞	小路	描述
GET	/datacenter/cluster/clusters/{key}/metrics	檢索由群集鍵的輸入參數指定的群集的性能資料（樣本和摘要）。傳回群集鍵和 UUID、時間範圍、IOPS、吞吐量、樣本數等資訊。
GET	/datacenter/cluster/clusters/analytics	檢索資料中心內所有群集的高階效能指標。您可以根據所需條件篩選結果。傳回諸如聚合 IOPS、吞吐量和收集週期（以小時為單位）等值。
GET	/datacenter/cluster/nodes/{key}/metrics	檢索節點鍵的輸入參數指定的節點的效能資料（樣本和摘要）。傳回節點 UUID、時間範圍、IOPS 摘要、吞吐量、延遲和效能、收集的樣本數和利用率百分比等資訊。
GET	/datacenter/cluster/nodes/analytics	檢索資料中心中所有節點的高階效能指標。您可以根據所需條件篩選結果。返回節點和集群鍵等資訊以及聚合 IOPS、吞吐量和收集週期（以小時為單位）等值。
GET	/datacenter/storage/aggregates/{key}/metrics	檢索聚合鍵的輸入參數指定的聚合的效能資料（樣本和摘要）。傳回的資訊包括時間範圍、IOPS 摘要、延遲、吞吐量和效能容量、每個計數器收集的樣本數以及利用率百分比。
GET	/datacenter/storage/aggregates/analytics	檢索資料中心內所有聚合的高階效能指標。您可以根據所需條件篩選結果。傳回諸如聚合和群集鍵之類的資訊以及諸如聚合 IOPS、吞吐量和收集週期（以小時為單位）之類的值。
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	檢索 LUN 或卷鍵的輸入參數指定的 LUN 或檔案共用（磁碟區）的效能資料（樣本和摘要）。傳回讀取、寫入和總 IOPS、延遲和吞吐量的最小值、最大值和平均值的摘要以及每個計數器收集的樣本數等資訊。

HTTP 動詞	小路	描述
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	檢索資料中心內所有 LUN 或磁碟區的高階效能指標。您可以根據所需條件篩選結果。傳回儲存 VM 和叢集鍵等資訊以及聚合 IOPS、吞吐量 and 收集週期（以小時為單位）等值。
GET	/datacenter/svm/svms/{key}/metrics	檢索儲存 VM 鍵的輸入參數指定的儲存 VM 的效能資料（樣本和摘要）。根據每個支援的協定匯總 IOPS，例如 nvmf, fcp, iscsi, 和 nfs、吞吐量、延遲和收集的樣本數量。
GET	/datacenter/svm/svms/analytics	檢索資料中心內所有儲存虛擬機器的進階效能指標。您可以根據所需條件篩選結果。傳回儲存 VM UUID、聚合 IOPS、延遲、吞吐量和收集週期（以小時為單位）等資訊。
GET	/datacenter/network/ethernet/ports/{key}/metrics	檢索由連接埠鍵的輸入參數指定的特定乙太網路連接埠的效能指標。當提供支援範圍的間隔（時間範圍）時，API 將傳回累積的計數器，例如該時間段內的最小值、最大值和平均效能值。
GET	/datacenter/network/ethernet/ports/analytics	檢索資料中心環境中所有乙太網路連接埠的進階效能指標。傳回叢集和節點金鑰和 UUID、吞吐量、收集週期和連接埠的使用率百分比等資訊。您可以根據可用參數（例如連接埠鍵、使用率百分比、叢集和節點名稱以及 UUID 等）過濾結果。
GET	/datacenter/network/fc/interfaces/{key}/metrics	檢索由介面鍵的輸入參數指定的特定網路 FC 介面的效能指標。當提供支援範圍的間隔（時間範圍）時，API 將傳回累積的計數器，例如該時間段內的最小值、最大值和平均效能值。

HTTP 動詞	小路	描述
GET	/datacenter/network/fc/interfaces/analytics	檢索資料中心環境中所有乙太網路連接埠的進階效能指標。傳回叢集和 FC 介面金鑰和 UUID、吞吐量、IOPS、延遲和儲存 VM 等資訊。您可以根據可用參數過濾結果，例如叢集和 FC 介面名稱和 UUID、儲存 VM、吞吐量等。
GET	/datacenter/network/fc/ports/{key}/metrics	檢索由連接埠鍵的輸入參數指定的特定 FC 連接埠的效能指標。當提供支援範圍的間隔（時間範圍）時，API 將傳回累積的計數器，例如該時間段內的最小值、最大值和平均效能值。
GET	/datacenter/network/fc/ports/analytics	檢索資料中心環境中所有 FC 連接埠的進階效能指標。傳回叢集和節點金鑰和 UUID、吞吐量、收集週期和連接埠的使用率百分比等資訊。您可以根據可用參數（例如連接埠鍵、使用率百分比、叢集和節點名稱以及 UUID 等）過濾結果。
GET	/datacenter/network/ip/interfaces/{key}/metrics	檢索介面鍵的輸入參數指定的網路 IP 介面的效能指標。當從支援的範圍中提供一個間隔（時間範圍）時，API 將傳回訊息，例如樣本數、累積計數器、吞吐量以及接收和傳輸的資料包數。
GET	/datacenter/network/ip/interfaces/analytics	檢索資料中心環境中所有網路 IP 介面的進階效能指標。傳回叢集和 IP 介面金鑰和 UUID、吞吐量、IOPS 和延遲等資訊。您可以根據可用參數過濾結果，例如叢集和 IP 介面名稱和 UUID、IOPS、延遲、吞吐量等。

查看作業和系統詳細信息

您可以使用 `jobs` API 下的 `management-server` 類別查看非同步操作的執行詳情。這 `system` API 下的 `management-server` 類別可讓您查看 Active IQ Unified Manager 環境中的實例詳細資訊。

查看職位

在 Active IQ Unified Manager 中，新增和修改資源等操作由同步和非同步 API 呼叫執行。為非同步執行而安排的呼叫可以透過為該呼叫建立的 Job 物件進行追蹤。每個 Job 物件都有一個唯一的鍵用於識別。每個 Job 物件都

會傳回 Job 物件 URI，以便您存取和追蹤作業的進度。您可以使用此 API 來檢索每次執行的詳細資訊。

透過使用此 API，您可以查詢資料中心的所有作業對象，包括歷史資料。查詢所有作業，預設傳回透過 Web UI 和 API 介面觸發的最近 20 個作業的詳細資訊。使用內建過濾器查看特定的作業。您也可以使用 Job 鍵查詢特定作業的詳細資訊並對資源執行下一組操作。

類別	HTTP 動詞	小路	描述
管理伺服器	得到	/management-server/jobs	傳回所有作業的作業詳細資料。沒有任何排序順序，最後提交的 Job 物件將會傳回在上面。
管理伺服器	得到	/management-server/jobs/{key} 輸入 Job 物件的 job 鍵來查看該 job 的具體詳情。	傳回特定 Job 物件的詳細資訊。

查看系統詳細信息

透過使用 `/management-server/system` API，您可以查詢 Unified Manager 環境的特定於實例的詳細資訊。API 傳回有關產品和服務的信息，例如系統上安裝的 Unified Manager 版本、UUID、供應商名稱、主機作業系統以及在 Unified Manager 實例上執行的服務的名稱、描述和狀態。

類別	HTTP 動詞	小路	描述
管理伺服器	得到	/management-server/system	執行此 API 不需要輸入參數。預設傳回目前 Unified Manager 實例的系統詳細資料。

使用 API 管理事件和警報

這 `events`，`alerts`，和 `scripts` API 下的 `management-server` 類別可讓您管理 Active IQ Unified Manager 環境中的事件、警報以及與警報相關的腳本。

查看和修改事件

Unified Manager 接收在 ONTAP 上為由 Unified Manager 監控和管理的叢集產生的事件。透過使用這些 API，您可以查看為您的叢集產生的事件，並解決和更新它們。

透過運行 `GET` 方法 `/management-server/events` API，可以查詢您資料中心內的事件，包括歷史資料。使用內建篩選器（例如名稱、影響等級、影響區域、嚴重性、狀態、資源名稱和資源類型）來查看特定事件。資源類型和區域參數傳回有關發生事件的儲存物件的信息，影響區域傳回有關引發事件的問題的信息，例如可用性、容量、配置、安全性、保護和效能。

透過執行此 API 的 `PATCH` 操作，您可以啟用事件的解決工作流程。您可以將事件指派給自己或其他使用者並確認收到該事件。在資源上執行步驟以解決觸發事件的問題時，您可以使用此 API 將事件標記為已解決。

有關事件的更多信息，請參閱["管理活動"](#)。

類別	HTTP 動詞	小路	描述
管理伺服器	得到	/management-server/events /management-server/events/{key}	當您執行 Get ALL 方法時，回應主體包含資料中心中所有事件的事件詳細資訊。當您透過特定鍵檢索事件詳細資訊時，您可以查看特定事件的詳細資訊並對資源執行下一組操作。回應主體包含該事件的詳細資訊。
管理伺服器	修補	management-server/events/{key}	執行此 API 來指派事件或將狀態變更為已確認或已解決。您也可以使用此方法將事件指派給您自己或其他使用者。這是一個同步操作。

管理警報

事件是自動且連續產生的。僅當事件滿足特定過濾條件時，Unified Manager 才會產生警報。您可以選擇應產生警報的事件。透過使用 `management-server/alerts` API，您可以設定警報，以便在發生特定事件或某些嚴重程度類型的事件時自動發送通知。

有關警報的更多信息，請參閱["管理警報"](#)。

類別	HTTP 動詞	小路	描述
管理伺服器	得到	/management-server/alerts /management-server/alerts/{key}	使用警報鍵查詢環境中所有現有警報或特定警報。您可以查看有關您的環境中產生的警報的信息，例如警報描述、操作、發送通知的電子郵件 ID、事件和嚴重性。
管理伺服器	郵政	/management-server/alerts	此方法使您能夠為特定事件新增警報。您必須新增警報名稱、警報適用的實體或邏輯資源或事件、警報是否啟用以及是否發出 SNMP 陷阱。您可以添加要生成警報的其他詳細信息，例如操作、通知電子郵件 ID、腳本詳細信息（如果您要添加警報腳本）等等。

類別	HTTP 動詞	小路	描述
管理伺服器	修補並刪除	management-server/events/{key}	您可以使用這些方法來修改和刪除特定的警報。您可以修改不同的屬性，例如描述、名稱以及啟用和停用警報。當不再需要警報時，您可以刪除該警報。



在選擇用於新增警報的資源時，請注意，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。

管理腳本

透過使用 `/management-server/scripts`` API，您也可以將警報與觸發警報時執行的腳本關聯起來。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。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。

有關腳本的更多信息，請參閱“[管理腳本](#)”。

類別	HTTP 動詞	小路	描述
管理伺服器	得到	/management-server/scripts	使用此 API 查詢您環境中所有現有的腳本。使用標準過濾和排序操作來僅查看特定腳本。
管理伺服器	郵政	/management-server/scripts	使用此 API 為腳本新增描述並上傳與警報相關的腳本檔案。

使用 API 管理工作負載

這裡描述的 API 涵蓋了儲存管理的各種功能，例如查看儲存工作負載、建立 LUN 和檔案共用、管理效能服務等級和儲存效率策略以及在儲存工作負載上指派策略。

使用 API 查看儲存工作負載

此處列出的 API 可讓您查看資料中心內所有 ONTAP 叢集的儲存工作負載的綜合清單。API 還提供了 Active IQ Unified Manager 環境中配置的儲存工作負載數量及其容量和效能 (IOPS) 統計資料的摘要視圖。

查看儲存工作負載

您可以使用以下方法查看您資料中心內所有叢集的所有儲存工作負載。有關根據特定列過濾回應的信息，請參閱 Unified Manager 實例中提供的 API 參考文件。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/workloads

查看儲存工作負載摘要

您可以使用以下方法來評估每個效能服務等級所管理的已使用容量、可用容量、已使用 IOPS、可用 IOPS 和儲存工作負載數量。顯示的儲存工作負載可以是任何 LUN、NFS 檔案共用或 CIFS 共用。API 提供了儲存工作負載概覽、Unified Manager 配置的儲存工作負載概覽、資料中心概覽、以及資料中心的總空間、已使用空間和可用空間以及 IOPS 概覽（根據指派的效能服務等級）。回應此 API 所收到的資訊用於填入 Unified Manager UI 中的儀表板。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/workloads-summary

使用 API 管理存取端點

您需要建立存取端點或邏輯介面 (LIF)，這是設定儲存虛擬機器 (SVM)、LUN 和檔案共用所必需的。您可以檢視、建立、修改和刪除 Active IQ Unified Manager 環境中的 SVM、LUN 或檔案共用的存取端點。

查看存取端點

您可以使用下列方法檢視 Unified Manager 環境中的存取端點清單。若要查詢特定 SVM、LUN 或檔案共用的存取端點列表，您需要輸入 SVM、LUN 或檔案共用的唯一識別碼。您也可以輸入唯一的存取端點金鑰來擷取特定存取端點的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

新增存取端點

您可以建立自訂存取端點並為其指派所需的屬性。您必須輸入要建立的存取端點的詳細資訊作為輸入參數。您可以使用此 API、系統管理員或 ONTAP CLI 在每個節點上建立存取端點。支援使用 IPv4 和 IPv6 位址建立存取端點。



您必須為每個節點的 SVM 配置最少數量的存取端點，才能成功設定 LUN 和檔案共用。您應該為每個節點配置至少兩個 SVM 存取端點，一個支援 CIFS 和/或 NFS 協議，另一個支援 iSCSI 或 FCP 協定。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/access-endpoints

刪除存取端點

您可以使用以下方法刪除特定的存取端點。您需要提供存取端點金鑰作為輸入參數來刪除特定的存取端點。

類別	HTTP 動詞	小路
儲存提供者	刪除	/storage-provider/access-endpoints/{key}

修改訪問端點

您可以使用下列方法修改存取端點並更新其屬性。您需要提供存取端點金鑰來修改特定的存取端點。您還需要輸入要更新的屬性及其值。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/access-endpoints/{key}

使用 API 管理 Active Directory 映射

您可以使用此處列出的 API 來管理 SVM 上的 Active Directory 映射，這些映射是在 SVM 上配置 CIFS 共用所需的。需要設定 Active Directory 映射才能將 SVM 與 ONTAP 對應。

查看 Active Directory 映射

您可以使用下列方法查看 SVM 的 Active Directory 對應的設定詳細資訊。若要查看 SVM 上的 Active Directory 映射，您需要輸入 SVM 金鑰。要查詢特定映射的詳細信息，您必須輸入映射鍵。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

新增 Active Directory 映射

您可以使用下列方法在 SVM 上建立 Active Directory 對應。您必須輸入映射詳細資訊作為輸入參數。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/active-directories-mappings

使用 API 管理文件共享

您可以使用 `/storage-provider/file-shares` 用於檢視、新增、修改和刪除資料中心環境中的 CIFS 和 NFS 檔案共用磁碟區的 API。

在設定檔共用磁碟區之前，請確保已建立 SVM 並使用支援的協定進行設定。如果您在設定時指派效能服務等級 (PSL) 或儲存效率原則 (SEP)，則應在建立檔案共用之前建立 PSL 或 SEP。

查看檔案共享

您可以使用下列方法檢視 Unified Manager 環境中可用的檔案共用磁碟區。當您在 Active IQ Unified Manager 上將 ONTAP 叢集新增為資料來源時，這些叢集的儲存工作負載會自動新增至您的 Unified Manager 實例中。此 API 會擷取自動和手動新增至 Unified Manager 實例的檔案共用。您可以使用文件共享金鑰運行此 API 來查看特定文件共享的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares /storage-provider/file-shares/{key}

新增檔案共享

您可以使用以下方法在 SVM 中新增 CIFS 和 NFS 檔案共用。您必須輸入要建立的文件共享的詳細資訊作為輸入參數。您不能使用此 API 來新增 FlexGroup 磁碟區。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/file-shares



根據是否提供存取控制清單 (ACL) 參數或匯出策略參數，建立 CIFS 共用或 NFS 檔案共用。如果您不提供 ACL 參數的值，則不會建立 CIFS 共享，並且預設建立 NFS 共享，以提供所有人的存取權限。

建立資料保護磁碟區：當您向 SVM 新增檔案共用時，預設會掛載的磁碟區類型是 `rw` (讀寫)。若要建立資料保護 (DP) 卷，請指定 `dp` 作為 `type` 範圍。

刪除檔案共享

您可以使用以下方法刪除特定的檔案共用。您需要輸入檔案共用金鑰作為輸入參數來刪除特定的檔案共用。

類別	HTTP 動詞	小路
儲存提供者	刪除	/storage-provider/file-shares/{key}

修改檔案共享

您可以使用以下方法修改檔案共用並更新其屬性。

您需要提供文件共享金鑰來修改特定的文件共享。此外，您還需要輸入要更新的屬性及其值。



請注意，一次呼叫此 API 只能更新一個屬性。對於多次更新，您需要多次執行此 API。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/file-shares/{key}

使用 API 管理 LUN

您可以使用 `/storage-provider/luns` API 用於檢視、新增、修改和刪除資料中心環境中的 LUN。

在配置 LUN 之前，請確保已建立 SVM 並使用支援的協定進行設定。如果您在設定時指派效能服務等級 (PSL) 或儲存效率原則 (SEP)，則應在建立 LUN 之前建立 PSL 或 SEP。

查看 LUN

您可以使用下列方法檢視 Unified Manager 環境中的 LUN。當您在 Active IQ Unified Manager 上將 ONTAP 叢集新增為資料來源時，這些叢集的儲存工作負載會自動新增至您的 Unified Manager 實例中。此 API 會擷取自動和手動新增至 Unified Manager 實例的所有 LUN。您可以透過使用 LUN 鍵執行此 API 來查看特定 LUN 的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns /storage-provider/luns/{key}

添加 LUN

您可以使用以下方法將 LUN 新增至您的 SVM。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/luns



在您的 cURL 請求中，如果您在輸入中為可選參數 `volume_name_tag` 提供了一個值，那麼在建立 LUN 期間命名磁碟區時將使用該值。此標籤可以輕鬆搜尋磁碟區。如果您在請求中提供音量鍵，則會跳過標記。

刪除 LUN

您可以使用以下方法刪除特定的 LUN。您需要提供 LUN 密鑰來刪除特定的 LUN。



如果您在 ONTAP 中建立了一個磁碟區，然後透過 Unified Manager 在該磁碟區上設定了 LUN，則當您使用此 API 刪除所有 LUN 時，該磁碟區也會從 ONTAP 叢集中刪除。

類別	HTTP 動詞	小路
儲存提供者	刪除	<code>/storage-provider/luns/{key}</code>

修改 LUN

您可以使用以下方法修改 LUN 並更新其屬性。您需要提供 LUN 密鑰來修改特定的 LUN。您還需要輸入要更新的 LUN 屬性及其值。若要使用此 API 更新 LUN 陣列，您應該查看「使用 API 的建議」中的建議。



每次呼叫此 API 時只能更新一個屬性。對於多次更新，您需要多次執行此 API。

類別	HTTP 動詞	小路
儲存提供者	修補	<code>/storage-provider/luns/{key}</code>

使用 API 管理效能服務級別

您可以使用 Active IQ Unified Manager 上的儲存提供者 API 檢視、建立、修改和刪除效能服務等級。

查看效能服務級別

您可以使用下列方法查看效能服務級別，並將其指派給儲存工作負載。API 列出了所有系統定義和使用者建立的效能服務級別，並檢索所有效能服務等級的屬性。如果要查詢特定的效能服務級別，則需要輸入該效能服務等級的唯一 ID 來擷取其詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	<code>/storage-provider/performance-service-levels</code> <code>/storage-provider/performance-service-levels/{key}</code>

新增效能服務級別

如果系統定義的效能服務等級不符合儲存工作負載所需的服務等級目標 (SLO)，您可以使用下列方法建立自訂效能服務等級並指派給儲存工作負載。輸入您想要建立的效能服務等級的詳細資訊。對於 IOPS 屬性，請確保輸入有效範圍的值。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/performance-service-levels

刪除效能服務級別

您可以使用以下方法刪除特定的效能服務等級。如果效能服務等級已指派給工作負載，或者它是唯一可用的效能服務級別，則您無法刪除該效能服務等級。您需要提供效能服務等級的唯一 ID 作為輸入參數來刪除特定的效能服務等級。

類別	HTTP 動詞	小路
儲存提供者	刪除	/storage-provider/performance-service-levels/{key}

修改效能服務級別

您可以使用下列方法修改效能服務等級並更新其屬性。您無法修改系統定義或指派給工作負載的效能服務等級。您需要提供唯一的 ID 來修改特定的效能服務等級。您還必須輸入要更新的 IOPS 屬性以及有效值。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/performance-service-levels/{key}

根據效能服務等級查看聚合功能

您可以使用下列方法查詢基於效能服務等級的聚合能力。此 API 傳回資料中心中可用的聚合列表，並指示這些聚合中可以支援的效能服務等級方面的功能。在磁碟區上配置工作負載時，您可以查看聚合支援特定效能服務等級的能力，並根據該能力配置工作負載。只有當您使用 API 調配工作負載時，才可以指定聚合。此功能在 Unified Manager Web UI 上不可用。

類別	HTTP 動詞	小路
儲存提供者	得到	<pre>/storage-provider/aggregate-capabilities</pre> <pre>/storage-provider/aggregate-capabilities/{key}</pre>

使用 API 管理儲存效率策略

您可以使用儲存提供者 API 檢視、建立、修改和刪除儲存效率策略。

請注意以下幾點：



- 在 Unified Manager 上建立工作負載時，指派儲存效率策略並不是強制性的。
- 在為工作負載指派策略後，您無法取消指派該策略。
- 如果工作負載在 ONTAP 磁碟區上指定了某些儲存設定（例如重複資料刪除和壓縮），則這些設定可能會被您在 Unified Manager 上新增儲存工作負載時所套用的儲存效率原則中指定的設定所覆寫。

查看儲存效率策略

您可以使用以下方法在將儲存效率策略指派給儲存工作負載之前查看儲存效率策略。此 API 列出所有系統定義和使用者建立的儲存效率策略，並檢索所有儲存效率策略的屬性。如果您想查詢特定的儲存效率策略，您需要輸入該策略的唯一 ID 來檢索其詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	<pre>/storage-provider/storage-efficiency-policies</pre> <pre>/storage-provider/storage-efficiency-policies/{key}</pre>

新增儲存效率策略

如果系統定義的策略不符合您的儲存工作負載的配置要求，您可以使用下列方法建立自訂儲存效率策略，並將其指派給您的儲存工作負載。輸入要建立的儲存效率策略的詳細資訊作為輸入參數。

類別	HTTP 動詞	小路
儲存提供者	郵政	<pre>/storage-provider/storage-efficiency-policies</pre>

刪除儲存效率策略

您可以使用以下方法刪除特定的儲存效率策略。如果儲存效率策略已指派給工作負載，或者它是唯一可用的儲存效率策略，則您無法刪除該策略。您需要提供儲存效率策略的唯一 ID 作為輸入參數來刪除特定的儲存效率策略。

類別	HTTP 動詞	小路
儲存提供者	刪除	/storage-provider/storage-efficiency-policies/{key}

修改儲存效率策略

您可以使用下列方法修改儲存效率策略並更新其屬性。您無法修改系統定義或指派給工作負載的儲存效率策略。您需要提供儲存效率策略的唯一 ID 來修改特定的儲存效率策略。此外，您還需要提供想要更新的屬性及其值。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/storage-efficiency-policies/{key}

儲存管理的常見 API 工作流程

常見的工作流程為客戶端應用程式開發人員提供了客戶端應用程式如何呼叫 Active IQ Unified Manager API 來執行常見儲存管理功能的範例。本節包含一些範例工作流程。

工作流程描述了一些常用的儲存管理用例以及供您使用的範例程式碼。每個任務都使用由一個或多個 API 呼叫組成的工作流程來描述。

了解工作流程中使用的 API 呼叫

您可以從 Unified Manager 實例查看線上文件頁面，其中包含每個 REST API 呼叫的詳細資訊。本文檔不重複線上文件的細節。本文檔中的工作流程範例中使用的每個 API 呼叫僅包含在文件頁面上找到該呼叫所需的資訊。找到特定的 API 呼叫後，您可以查看該呼叫的完整詳細信息，包括輸入參數、輸出格式、HTTP 狀態代碼和請求處理類型。

工作流程中的每個 API 呼叫都包含以下信息，以幫助在文件頁面上找到該呼叫：

- 類別：API 呼叫在文件頁面上按功能相關區域或類別組織。若要尋找特定的 API 呼叫，請捲動到頁面底部，然後點擊相應的 API 類別。
- HTTP 動詞（呼叫）：HTTP 動詞標識對資源執行的操作。每個 API 呼叫都透過單一 HTTP 動詞執行。
- 路徑：路徑決定了執行呼叫時操作所應用的特定資源。路徑字串會附加到核心 URL 中，以形成標識資源的完整 URL。

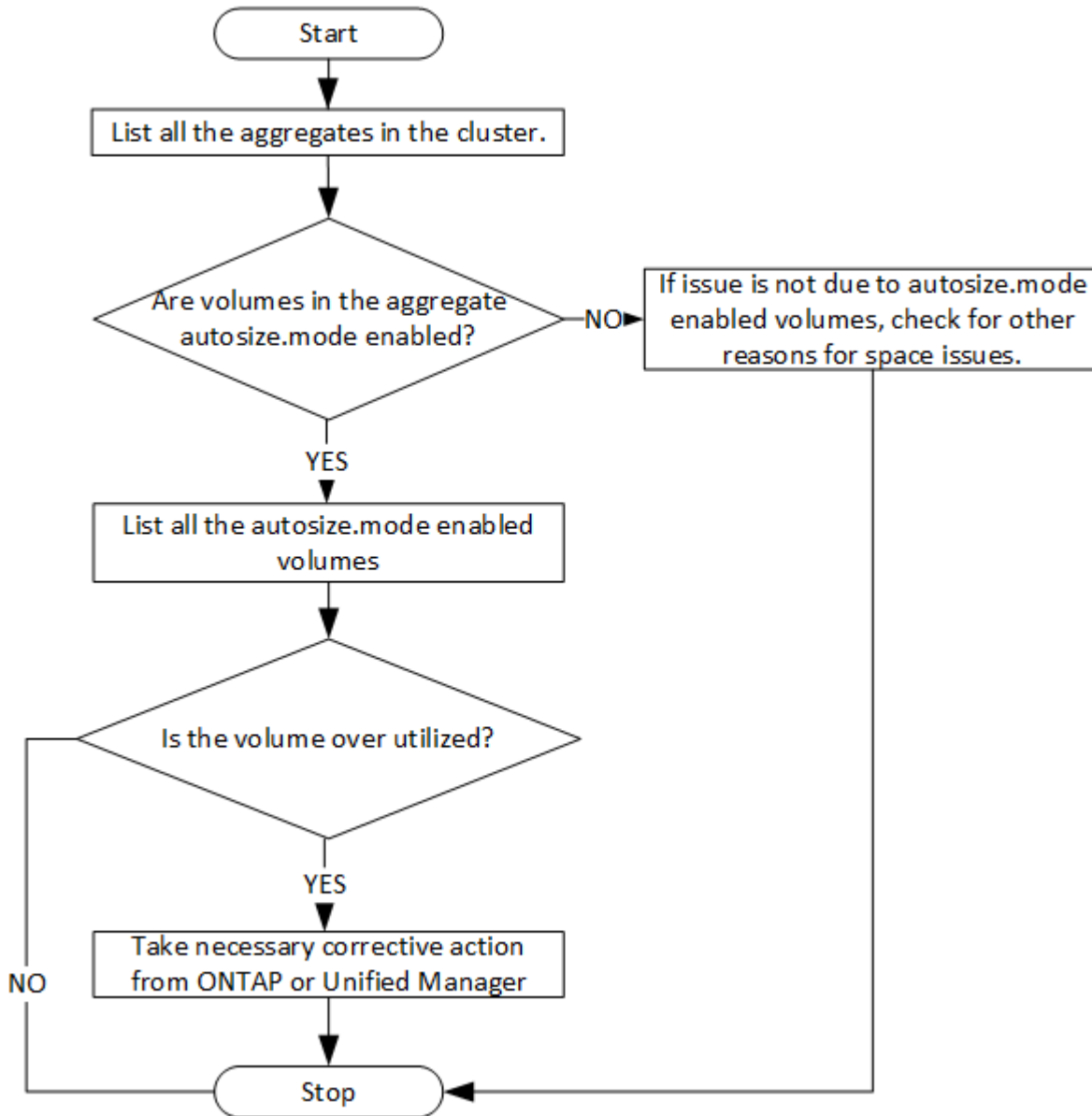
使用 API 確定聚合中的空間問題

您可以使用 Active IQ Unified Manager 中的資料中心 API 來監控磁碟區中空間的可用性和使用率。您可以確定磁碟區中的空間問題並識別過度利用或利用不足的儲存資源。

聚合的資料中心 API 會擷取有關可用空間和已使用空間以及節省空間效率設定的相關資訊。您也可以根據指定的屬性篩選檢索到的資訊。

確定聚合中是否缺少空間的一種方法是驗證您的環境中是否存在啟用了自動調整大小模式的磁碟區。然後，您應該確定哪些磁碟區被過度利用並執行任何糾正措施。

以下流程圖說明了檢索啟用自動調整大小模式的磁碟區資訊的過程：



此流程假定叢集已在ONTAP中建立並新增至 Unified Manager。

1. 取得叢集金鑰，除非您知道其值：

類別	HTTP 動詞	小路
資料中心	得到	/datacenter/cluster/clusters

2. 使用叢集鍵作為過濾參數，查詢該叢集上的聚合。

類別	HTTP 動詞	小路
資料中心	得到	/datacenter/storage/aggregates

3. 根據響應，分析聚合的空間使用情況並確定哪些聚合存在空間問題。對於每個存在空間問題的聚合，從相同的 JSON 輸出中取得聚合鍵。
4. 使用每個聚合鍵，過濾所有具有 autosize.mode 參數值的捲 grow。

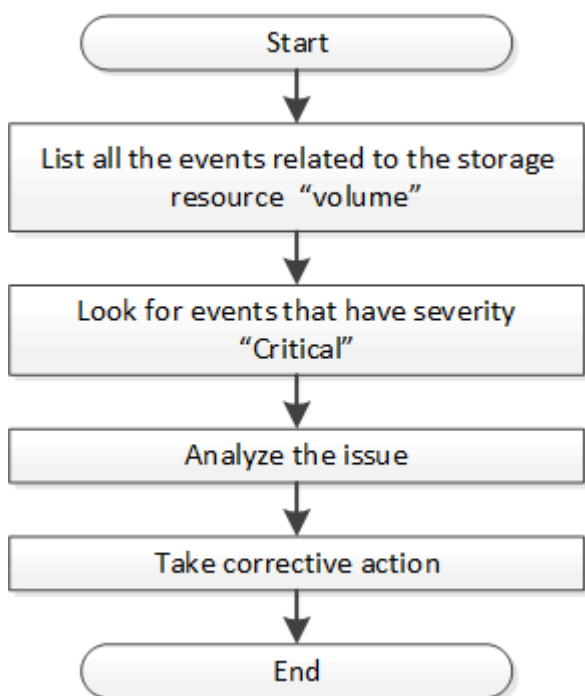
類別	HTTP 動詞	小路
資料中心	得到	/datacenter/storage/volumes

5. 分析哪些卷宗被過度利用。
6. 執行任何必要的糾正措施（例如跨聚合移動卷）以解決磁碟區中的空間問題。您可以從 ONTAP 或 Unified Manager Web UI 執行這些操作。

使用事件 API 確定儲存物件中的問題

當資料中心中的儲存物件超過閾值時，您會收到有關該事件的通知。使用此通知，您可以分析問題並採取糾正措施，方法是使用 `events` 蜜蜂。

此工作流程以磁碟區作為資源物件的範例。您可以使用 `events` API 用於檢索與磁碟區相關的事件列表，分析該卷的關鍵問題，然後採取糾正措施來糾正問題。



在採取補救措施之前，請按照以下步驟確定卷中的問題。

步驟

1. 分析資料中心磁碟區的關鍵Active IQ Unified Manager事件通知。
2. 使用 /management-server/events API 中的以下參數查詢卷的所有事件：

```
"resource_type": "volume"  
"severity": "critical"
```

類別	HTTP 動詞	小路
管理伺服器	得到	/管理伺服器/事件

3. 查看輸出並分析特定磁碟區中的問題。
4. 使用 Unified Manager REST API 或 Web UI 執行必要的操作來解決問題。

使用網關 API 對ONTAP磁碟區進行故障排除

網關 API 充當網關，呼叫ONTAP API 來查詢有關ONTAP儲存物件的資訊並採取補救措施來解決報告的問題。

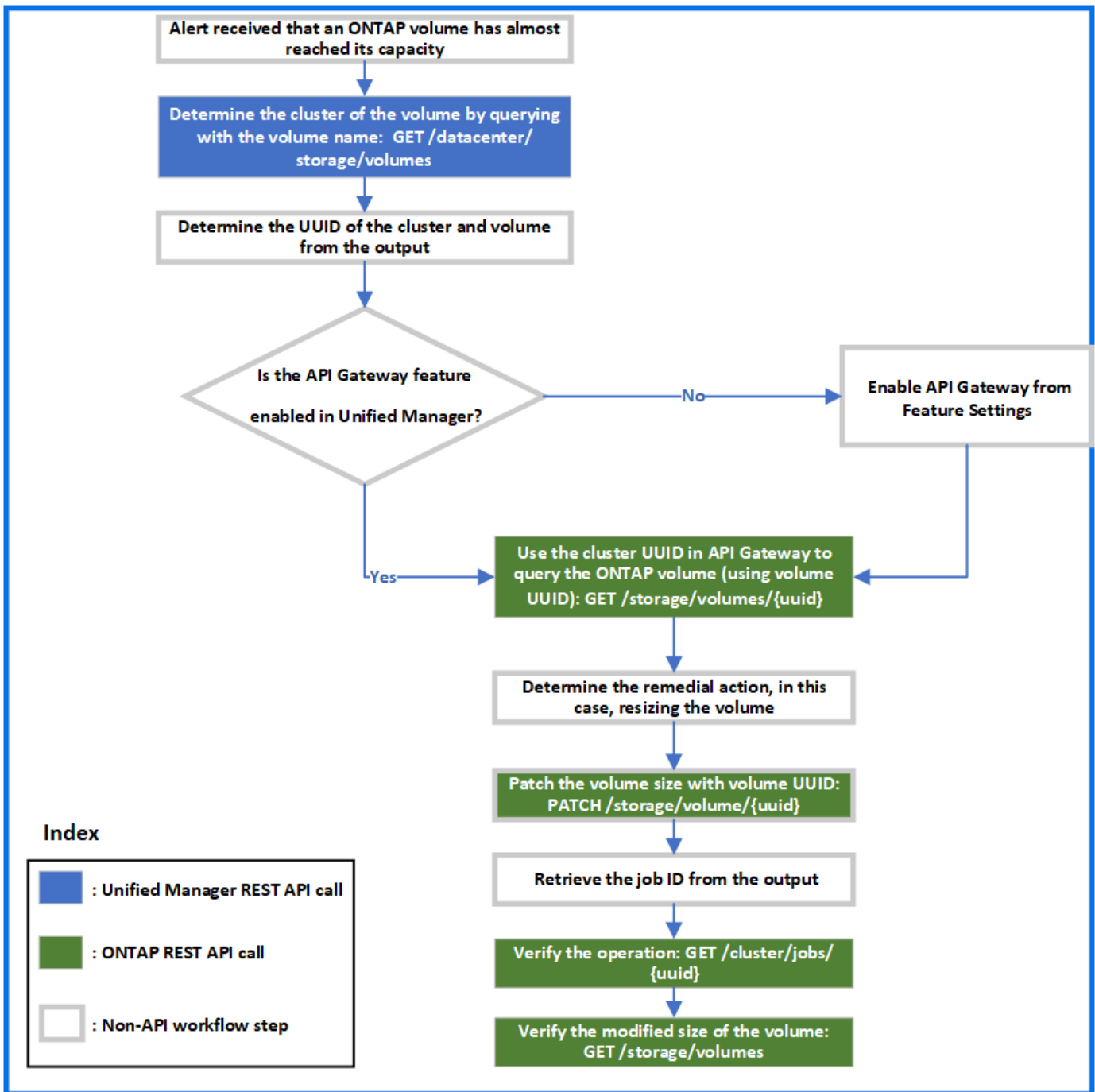
此工作流程採用一個範例用例，其中當ONTAP磁碟區幾乎達到其容量時會引發一個事件。此工作流程也示範如何透過呼叫Active IQ Unified Manager和ONTAP REST API 的組合來解決此問題。

在運行工作流程步驟之前，請確保以下事項：



- 您了解網關 API 及其使用方法。有關信息，請參閱["透過代理程式存取ONTAP API"](#)。
- 您了解ONTAP REST API 的用法。有關使用ONTAP REST API 的信息，請參閱<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP自動化文檔"]。
- 您是應用程式管理員。
- 您要在其上執行 REST API 操作的叢集受ONTAP 9.5 或更高版本支持，並且該叢集透過HTTPS 新增至 Unified Manager。

下圖說明了解決ONTAP磁碟區容量使用問題的工作流程中的每個步驟。



此工作流程涵蓋 Unified Manager 和 ONTAP REST API 的呼叫點。

1. 記下通知磁碟區容量利用率的事件中的磁碟區名稱。
2. 透過使用磁碟區名稱作為名稱參數中的值，透過執行以下 Unified Manager API 來查詢磁碟區。

類別	HTTP 動詞	小路
資料中心	得到	/datacenter/storage/volumes

3. 從輸出中檢索叢集 UUID 和磁碟區 UUID。

- 在 Unified Manager Web UI 上，導覽至 常規 > 功能設定 > **API 閘道** 以驗證 API 閘道功能是否已啟用。除非啟用，否則網關類別下的 API 不可供您呼叫。如果該功能已停用，請啟用它。
- 使用叢集 UUID 運行 ONTAP API `/storage/volumes/{uuid}` 透過 API 網關。當磁碟區 UUID 作為 API 參數傳遞時，查詢將傳回磁碟區詳細資料。

若要透過 API 閘道執行 ONTAP API，Unified Manager 憑證會在內部傳遞以進行驗證，且您不需要為單一叢集存取權執行額外的驗證步驟。

類別	HTTP 動詞	小路
統一管理器：網關 ONTAP：存儲	得到	網關 API： <code>/gateways/{uuid}/{path}</code> ONTAP API： <code>/storage/volumes/{uuid}</code>



在 `/gateways/{uuid}/{path}` 中，`{uuid}` 的值必須替換為執行 REST 作業的叢集 UUID。`{path}` 必須替換為 ONTAP REST URL `/storage/volumes/{uuid}`。

附加的 URL 是：`/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

執行 GET 操作時，產生的 URL 為：

```
GET https://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}
```

範例 **cURL** 指令

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

- 根據輸出，確定大小、用途和要採取的補救措施。在此工作流程中，採取的補救措施是調整磁碟區大小。
- 使用叢集 UUID 並透過 API 閘道執行以下 ONTAP API 來調整磁碟區大小。有關網關和 ONTAP API 的輸入參數的信息，請參閱步驟 5。

類別	HTTP 動詞	小路
統一管理器：網關 ONTAP：存儲	修補	網關 API： <code>/gateways/{uuid}/{path}</code> ONTAP API： <code>/storage/volumes/{uuid}</code>



除了群集 UUID 和磁碟區 UUID 之外，您還必須輸入用於調整磁碟區大小的大小參數值。確保以位元組為單位輸入值。例如，如果要將磁碟區的大小從 100 GB 增加到 120 GB，請在查詢結尾輸入參數大小的值：`-d {"size": 128849018880}"`

範例 cURL 指令

```
curl -X PATCH "https://<hostname>/api/gateways/lcd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

JSON 輸出傳回作業 UUID。

- 使用作業 UUID 驗證作業是否成功運作。使用叢集 UUID 和作業 UUID 透過 API 閘道執行下列 ONTAP API。有關網關和 ONTAP API 的輸入參數的信息，請參閱步驟 5。

類別	HTTP 動詞	小路
統一管理器：網關 ONTAP：叢集	得到	網關 API： /gateways/{uuid}/{path} ONTAP API： /cluster/jobs/{uuid}

傳回的 HTTP 程式碼與 ONTAP REST API HTTP 狀態碼相同。

- 執行以下 ONTAP API 來查詢已調整大小的磁碟區的詳細資訊。有關網關和 ONTAP API 的輸入參數的信息，請參閱步驟 5。

類別	HTTP 動詞	小路
統一管理器：網關 ONTAP：存儲	得到	網關 API： /gateways/{uuid}/{path} ONTAP API： /storage/volumes/{uuid}

輸出顯示磁碟區大小增加到了 120 GB。

用於工作負載管理的 API 工作流程

使用 Active IQ Unified Manager，您可以設定和修改儲存工作負載（LUN、NFS 檔案共用和 CIFS 共用）。配置包括多個步驟，從建立儲存虛擬機器 (SVM) 到在儲存工作負載上套用效能服務等級和儲存效率策略。修改工作負載包括修改特定參數和啟用附加功能的步驟。

描述了以下工作流程：

- 在 Unified Manager 上設定儲存虛擬機器 (SVM) 的工作流程。



在 Unified Manager 上設定 LUN 或檔案共用之前，需要執行此工作流程。

- 設定檔共享。
- 配置 LUN。
- 修改 LUN 和檔案共用（使用更新儲存工作負載的效能服務等級參數的範例）。
- 修改 NFS 檔案共用以支援 CIFS 協議
- 修改工作負載以將 QoS 升級到 AQoS



對於每個設定工作流程（LUN 和檔案共用），請確保您必須已完成驗證叢集上的 SVM 的工作流程。

在工作流程中使用每個 API 之前，您還必須閱讀建議和限制。API 的相關詳細資訊可在相關概念和參考中列出的各個部分中找到。

使用 API 驗證叢集上的 SVM

在設定檔共用或 LUN 之前，您必須驗證叢集上是否建立了儲存虛擬機器 (SVM)。



此工作流程假定 ONTAP 叢集已新增至 Unified Manager，並且已取得叢集金鑰。叢集應具有配置 LUN 和檔案共用所需的許可證。

1. 驗證叢集是否已建立 SVM。

類別	HTTP 動詞	小路
資料中心	得到	/datacenter/svm/svms /datacenter/svm/svms/{key }

範例 cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 如果未傳回 SVM 金鑰，則建立 SVM。若要建立 SVM，您需要在其上配置 SVM 的叢集金鑰。您還需要指定 SVM 名稱。請依照以下步驟操作。

類別	HTTP 動詞	小路
資料中心	得到	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

獲取集群密鑰。

範例 cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. 從輸出中取得叢集鍵，然後將其用作建立 SVM 的輸入。



建立 SVM 時，請確保它支援配置 LUN 及其上檔案共用所需的所有協議，例如 CIFS、NFS、FCP 和 iSCSI。如果 SVM 不支援所需的服務，則配置工作流程可能會失敗。建議在 SVM 上也啟用對應類型工作負載的服務。

類別	HTTP 動詞	小路
資料中心	郵政	/datacenter/svm/svms

範例 cURL

輸入 SVM 物件詳細資訊作為輸入參數。


```

curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": { },
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcg\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"

```

JSON 輸出顯示一個作業物件鍵，您可以使用它來驗證您建立的 SVM。

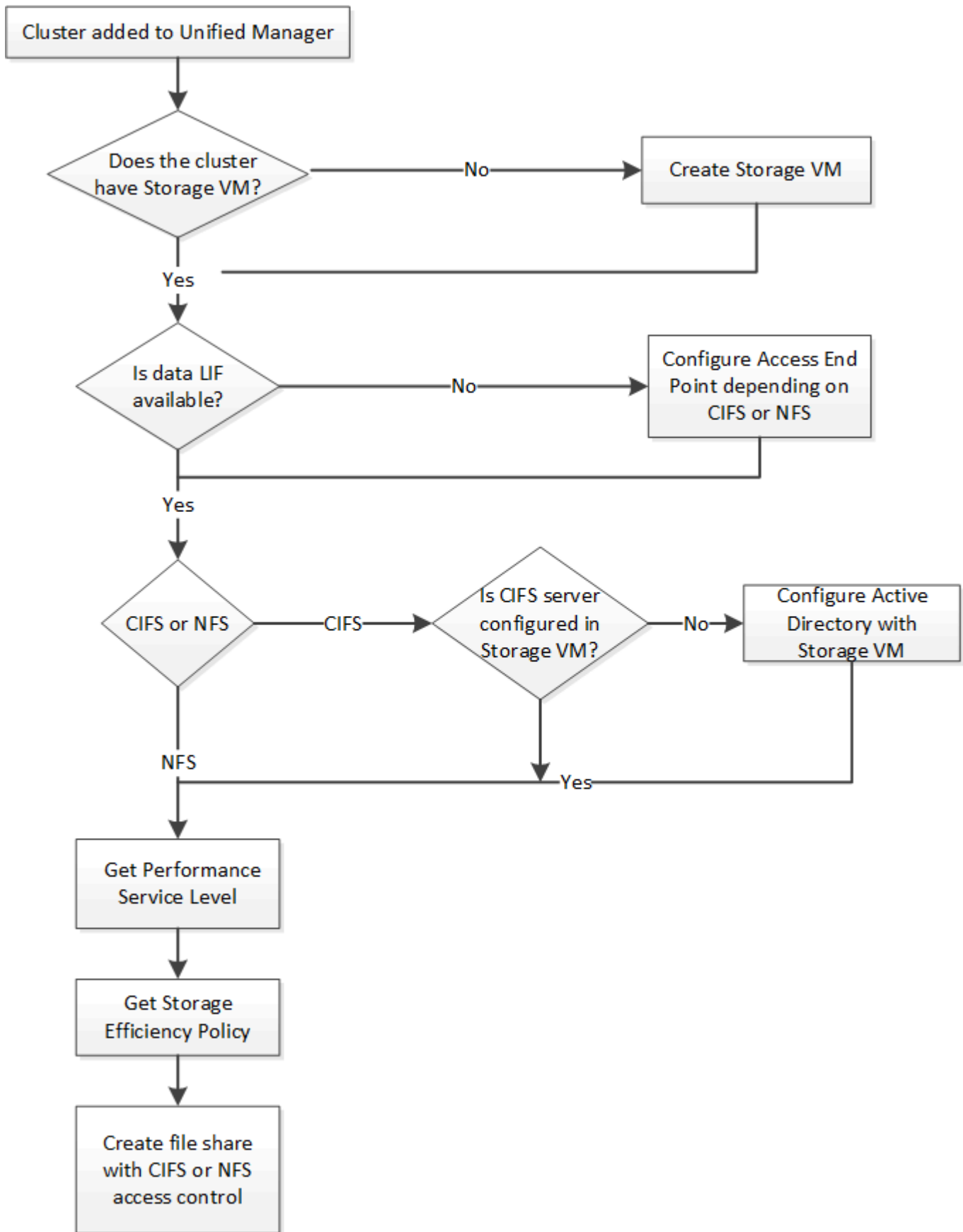
4. 使用作業物件鍵進行查詢來驗證 SVM 建立。如果 SVM 建立成功，則在回應中傳回 SVM 金鑰。

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

使用 API 預配 CIFS 和 NFS 檔案共用

您可以使用 Active IQ Unified Manager 提供的設定 API 在儲存虛擬機器 (SVM) 上設定 CIFS 共用和 NFS 檔案共用。此組態工作流程詳細說明了在建立文件共用之前檢索 SVM、效能服務等級和儲存效率策略的金鑰的步驟。

下圖說明了文件共用配置工作流程中的每個步驟。它包括配置 CIFS 共享和 NFS 檔案共享。



確保以下事項：



- ONTAP叢集已新增至 Unified Manager，並且已取得叢集金鑰。
- 已在叢集上建立 SVM。
- SVM 支援 CIFS 和 NFS 服務。如果 SVM 不支援所需的服務，則設定檔共用可能會失敗。
- FCP 連接埠已上線，可供連接埠設定。

1. 確定要建立 CIFS 共享的 SVM 上是否有可用的資料 LIF 或存取端點。取得 SVM 上可用存取端點的清單：

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

範例 cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 如果您的存取端點在清單中，則取得存取端點金鑰，否則建立存取端點。



確保建立已啟用 CIFS 協定的存取端點。除非您建立了啟用了 CIFS 協定的存取端點，否則配置 CIFS 共用將會失敗。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/access-endpoints

範例 cURL

您必須輸入要建立的存取端點的詳細資訊作為輸入參數。

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

JSON 輸出顯示一個作業物件鍵，您可以使用它來驗證您建立的存取端點。

3. 驗證存取端點：

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

4. 確定是否必須建立 CIFS 共用或 NFS 檔案共用。若要建立 CIFS 共享，請依照下列子步驟操作：

a. 確定您的 SVM 上是否配置了 CIFS 伺服器，即確定 SVM 上是否建立了 Active Directory 對應。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/active-directories-mappings

b. 如果建立了 Active Directory 映射，則取得金鑰，否則在 SVM 上建立 Active Directory 映射。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/active-directories-mappings

範例 cURL

您必須輸入建立 Active Directory 對應的詳細資訊作為輸入參數。

```
curl -X POST "https://<hostname>/api/storage-provider/active-  
directories-mappings" -H "accept: application/json" -H "Content-Type:  
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"  
{ \"_links\": {},  
\"dns\": \"10.000.000.000\",  
\"domain\": \"example.com\",  
\"password\": \"string\",  
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-  
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },  
\"username\": \"string\"}
```

+

這是一個同步調用，您可以在輸出中驗證 Active Directory 映射的建立。如果發生錯誤，則會顯示錯誤訊息，以便您排除故障並重新執行請求。

- 取得要在其上建立 CIFS 共用或 NFS 檔案共用的 SVM 的 SVM 金鑰，如 `_驗證叢集上的 SVM_工作流程` 主題中所述。
- 透過執行以下 API 並從回應中檢索金鑰來取得效能服務等級的金鑰。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/performance-service-levels



您可以透過設定 `system_defined`輸入參數`true`。從輸出中取得要在檔案共用上套用的效能服務等級的金鑰。

- 或者，透過執行以下 API 並從回應中檢索金鑰，取得要在文件共用上套用的儲存效率策略的儲存效率策略金鑰。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/storage-efficiency-policies

- 建立文件共享。您可以透過指定存取控制清單和匯出策略來建立同時支援 CIFS 和 NFS 的檔案共用。如果您想要建立文件共用以僅支援磁碟區上的一種協議，則下列子步驟將提供資訊。建立 NFS 共用後，您還可以更新 NFS 檔案共用以包含存取控制清單。有關信息，請參閱“修改儲存工作負載”主題。
 - 若要僅建立 CIFS 共享，請收集有關存取控制清單 (ACL) 的資訊。若要建立 CIFS 共享，請為下列輸入參數提供有效值。對於您指派的每個使用者群組，在設定 CIFS/SMB 共用時都會建立一個 ACL。根據您為 ACL 和 Active Directory 對應輸入的值，在建立 CIFS 共用時決定其存取控制和對應。

帶有範例值的 cURL 指令

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
  },
}
```

- b. 若要僅建立 NFS 檔案共享，請收集有關匯出策略的資訊。若要建立 NFS 檔案共享，請為以下輸入參數提供有效值。根據您的值，匯出策略在建立時會附加到 NFS 檔案共用。



在配置 NFS 共用時，您可以透過提供所有必要的值來建立匯出策略，或提供匯出策略金鑰並重複使用現有的匯出策略。如果要重複使用儲存虛擬機器的導出策略，則需要新增匯出策略金鑰。除非您知道金鑰，否則您可以使用 `/datacenter/protocols/nfs/export-policies`API`。若要建立新策略，您必須輸入如以下範例所示的規則。對於輸入的規則，API 嘗試透過匹配主機、儲存虛擬機器和規則來搜尋現有的匯出策略。如果存在現有的匯出策略，則使用該策略。否則，將建立新的出口政策。

帶有範例值的 cURL 指令

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

配置存取控制清單和匯出策略後，為 CIFS 和 NFS 檔案共用的強制輸入參數提供有效值：



儲存效率策略是建立文件共享的可選參數。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/file-shares

JSON 輸出顯示一個作業物件鍵，您可以使用它來驗證您建立的檔案共用。◦ 使用查詢作業中傳回的作業物件鍵來驗證檔案共用的建立：

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

在回應的末尾，您會看到建立的文件共享的金鑰。

```

    ],
    "job_results": [
      {
        "name": "fileshareKey",
        "value": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
      }
    ],
    "_links": {
      "self": {
        "href": "/api/management-server/jobs/06a6148bf9e862df:-2611856e:16e8d47e722:-7f87"
      }
    }
  }
}

```

1. 透過使用傳回的金鑰運行以下 API 來驗證文件共享的建立：

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares/{key}

JSON 輸出範例

您可以看到 `storage-provider/file-shares` 內部呼叫每個函數所需的所有 API 並建立物件。例如，它調用 `storage-provider/performance-service-levels/` 用於指派文件共用上的效能服務等級的 API。

```

{
  "key": "7d5a59b3-953a-11e8-8857-

```

```

00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
      }
    }
  },
  "svm": {
    "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
    "name": "RRT_ritu_vs1",
    "_links": {
      "self": {
        "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
      }
    }
  },
  "assigned_performance_service_level": {
    "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
      "self": {
        "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
      }
    }
  },
  "recommended_performance_service_level": {
    "key": null,
    "name": "Idle",
    "peak_iops": null,
    "expected_iops": null,
    "_links": {}
  }
}

```



```

},
"space": {
  "size": 104857600
},
"assigned_storage_efficiency_policy": {
  "key": null,
  "name": "Unassigned",
  "_links": {}
},
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 1,
        "protocols": [
          "nfs3",
          "nfs4"
        ],
        "ro_rule": [
          "sys"
        ],
        "rw_rule": [
          "sys"
        ],
        "superuser": [
          "none"
        ]
      }
    ],
    {
      "anonymous_user": "65534",

```

```

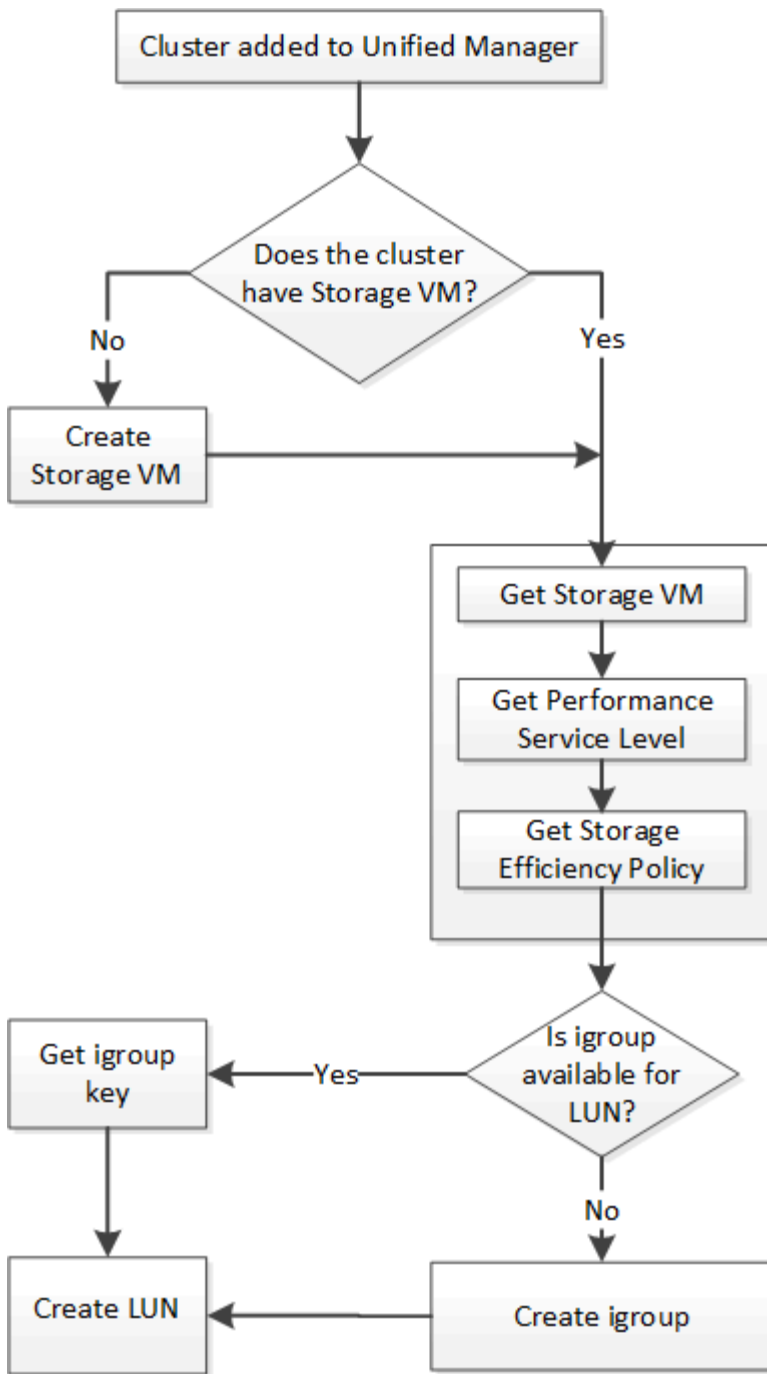
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
},
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

使用 API 預配 LUN

您可以使用 Active IQ Unified Manager 提供的設定 API 在儲存虛擬機器 (SVM) 上設定 LUN。此組態工作流程詳細說明了在建立 LUN 之前檢索 SVM、效能服務等級和儲存效率策略的金鑰的步驟。

下圖說明了 LUN 設定工作流程中的步驟。



此工作流程假定ONTAP叢集已新增至 Unified Manager，並且已取得叢集金鑰。該工作流程還假設在叢集上已建立 SVM。

1. 取得要在其上建立 LUN 的 SVM 的 SVM 金鑰，如_驗證叢集上的 SVM_ 工作流程主題中所述。
2. 透過執行以下 API 並從回應中檢索金鑰來取得效能服務等級的金鑰。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/performance-service-levels



您可以透過設定 `system_defined`輸入參數`true`。從輸出中取得要在 LUN 上套用的效能服務等級的金鑰。

3. 或者，透過執行以下 API 並從回應中擷取金鑰，取得要在 LUN 上套用的儲存效率策略的儲存效率策略金鑰。

類別	HTTP 動詞	小路
儲存提供者	得到	<code>/storage-provider/storage-efficiency-policies</code>

4. 決定是否已建立啟動程式群組 (igroup) 來授予對要建立的 LUN 目標的存取權限。

類別	HTTP 動詞	小路
資料中心	得到	<code>/datacenter/protocols/san/igroups</code> <code>/datacenter/protocols/san/igroups/{key}</code>

您必須輸入參數值來指示 igroup 有權存取的 SVM。此外，如果您想查詢特定的 igroup，請輸入 igroup 名稱（鍵）作為輸入參數。

5. 在輸出中，如果您可以找到要授予存取權限的 igroup，請取得金鑰。否則創建 igroup。

類別	HTTP 動詞	小路
資料中心	郵政	<code>/datacenter/protocols/san/igroups</code>

您必須輸入要建立的 igroup 的詳細資訊作為輸入參數。這是一個同步調用，您可以在輸出中驗證 igroup 的建立。如果發生錯誤，則會顯示一則訊息，以便您排除故障並重新執行 API。

6. 建立 LUN。

類別	HTTP 動詞	小路
儲存提供者	郵政	<code>/storage-provider/luns</code>

若要建立 LUN，請確保已將檢索到的值新增為強制輸入參數。



儲存效率策略是建立 LUN 的可選參數。

範例 cURL

您必須輸入要建立的 LUN 的所有詳細資訊作為輸入參數。

JSON 輸出顯示一個作業物件鍵，您可以使用它來驗證您建立的 LUN。

7. 使用查詢作業中傳回的作業物件鍵來驗證 LUN 的建立：

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

在回應的末尾，您會看到建立的 LUN 的金鑰。

8. 透過使用傳回的金鑰執行以下 API 來驗證 LUN 的建立：

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns/{key}

JSON 輸出範例

您可以看到 `/storage-provider/luns` 內部呼叫每個函數所需的所有 API 並建立物件。例如，它調用 `/storage-provider/performance-service-levels/` 用於在 LUN 上指派效能服務等級的 API。

== LUN 建立或對應失敗的故障排除步驟

完成此工作流程後，您可能仍會看到 LUN 建立失敗。即使成功建立了 LUN，由於建立 LUN 的節點上 SAN LIF 或存取端點不可用，LUN 與 igroup 的對應也可能會失敗。如果發生故障，您將看到以下訊息：

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server_name>. Use the access-endpoints API to create a LIF for the LUN.
```

請依照以下故障排除步驟來解決此故障。

1. 在您嘗試建立 LUN 的 SVM 上建立支援 iSCSI/FCP 協定的存取端點。

類別	HTTP 動詞	小路
儲存提供者	郵政	/storage-provider/access-endpoints

範例 cURL

您必須輸入要建立的存取端點的詳細資訊作為輸入參數。



確保在輸入參數中已新增指示 LUN 主節點的位址和指示主節點的伙伴節點的 `ha_address`。當您執行此操作時，它會在主節點和夥伴節點上建立存取端點。

2. 使用 JSON 輸出中傳回的作業物件鍵查詢作業，以驗證它是否已成功運行以在 SVM 上新增存取端點，以及是否已在 SVM 上啟用 iSCSI/FCP 服務。

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

JSON 輸出範例

在輸出的最後，您可以看到建立的存取端點的金鑰。在下面的輸出中，「name」：「accessEndpointKey」值表示在 LUN 的主節點上建立的存取端點，其金鑰為 9c964258-14ef-11ea-95e2-00a098e32c28。「name」：「accessEndpointHAKey」值表示在主節點的夥伴節點上建立的存取端點，其金鑰為 9d347006-14ef-11ea-8760-00a098e3215f。

3. 修改 LUN 以更新 igroup 映射。有關工作流程修改的更多信息，請參閱“修改儲存工作負載”。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/lun/{key}

在輸入中，指定要用來更新 LUN 對應的 igroup 鍵以及 LUN 鍵。

範例 cURL

JSON 輸出顯示一個 Job 物件鍵，您可以使用它來驗證映射是否成功。

4. 透過查詢 LUN 鍵來驗證 LUN 對應。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns/{key}

JSON 輸出範例

在輸出中，您可以看到 LUN 已成功對應到最初設定的 igroup（鍵 d19ec2fa-fec7-11e8-b23d-00a098e32c28）。

使用 API 修改儲存工作負載

修改儲存工作負載包括更新缺少參數的 LUN 或檔案共用，或變更現有參數。

此工作流程以更新 LUN 和檔案共享的效能服務等級為例。



工作流程假定 LUN 或檔案共用已配置效能服務等級。

修改檔案共享

修改檔案共用時，您可以更新以下參數：

- 容量或大小。
- 線上或離線設定。
- 儲存效率策略。
- 性能服務水準。
- 存取控制清單 (ACL) 設定。
- 導出策略設定。您也可以刪除匯出策略參數並還原檔案共用上的預設（空）匯出策略規則。



在單一 API 運行期間，您只能更新一個參數。

此過程描述了向文件共享添加效能服務等級。您可以使用相同的程序來更新任何其他文件共用屬性。

1. 取得要更新的檔案共享的 CIFS 共用或 NFS 檔案共用金鑰。此 API 查詢資料中心上的所有檔案共用。如果您已經知道檔案共用金鑰，請跳過此步驟。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares

2. 使用您取得的文件共享金鑰執行以下 API 來查看文件共享的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares/{key}

在輸出中查看文件共享的詳細資訊。

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. 取得您想要在此文件共用上指派的效能服務等級的金鑰。目前尚未為其分配任何策略。

類別	HTTP 動詞	小路
性能服務水平	得到	/storage-provider/performance-service-levels



您可以透過設定 `system_defined`輸入參數`true`。從輸出中取得要套用於檔案共用的效能服務等級的金鑰。

4. 在文件共享上套用效能服務等級。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/file-shares/{key}

在輸入中，您必須僅指定要更新的參數以及檔案共用金鑰。在這種情況下，它是效能服務水準的關鍵。

範例 cURL

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

JSON 輸出顯示一個 Job 對象，您可以使用它來驗證主節點和合作夥伴節點上的存取端點是否已成功建立。

5. 使用輸出中顯示的作業對象鍵驗證效能服務等級是否已新增至文件共用。

類別	HTTP 動詞	小路
管理伺服器	得到	/management-server/jobs/{key}

如果透過作業物件的 ID 進行查詢，您可以看到檔案共用是否已成功更新。如果發生故障，請排除故障並再次執行 API。成功建立後，查詢文件共用以查看修改的物件：

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares/{key}

在輸出中查看文件共享的詳細資訊。


```

"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}

```

更新 LUN

更新 LUN 時，您可以修改以下參數：

- 容量或尺寸
- 在線或離線設置
- 儲存效率策略
- 性能服務水平
- LUN 映射



在單一 API 運行期間，您只能更新一個參數。

此程序描述了向 LUN 新增效能服務等級。您可以使用相同的程序來更新任何其他 LUN 屬性。

1. 取得要更新的 LUN 的 LUN 密鑰。此 API 傳回資料中心內所有 LUNS 的詳細資訊。如果您已經知道 LUN 金鑰，請跳過此步驟。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns

2. 使用您取得的 LUN 金鑰執行以下 API 來查看 LUN 的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns/{key}

在輸出中查看 LUN 的詳細資訊。您可以看到沒有為該 LUN 指派效能服務等級。

JSON 輸出範例

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. 取得要指派給 LUN 的效能服務等級的金鑰。

類別	HTTP 動詞	小路
性能服務水平	得到	/storage-provider/performance-service-levels



您可以透過設定 `system_defined`輸入參數`true`。從輸出中取得要在 LUN 上套用的效能服務等級的金鑰。

4. 在 LUN 上套用效能服務等級。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/lun/{key}

在輸入中，您必須只指定要更新的參數以及 LUN 鍵。在這種情況下，它是效能服務水準的關鍵。

範例 cURL

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

JSON 輸出顯示一個作業物件鍵，您可以使用它來驗證已更新的 LUN。

5. 使用您取得的 LUN 金鑰執行以下 API 來查看 LUN 的詳細資訊。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/luns/{key}

在輸出中查看 LUN 的詳細資訊。您可以看到效能服務等級已指派給此 LUN。

JSON 輸出範例

```

"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}

```

使用 API 修改 NFS 檔案共用以支援 CIFS

您可以修改 NFS 檔案共用以支援 CIFS 協定。在建立檔案共用期間，可以為相同檔案共用指定存取控制清單 (ACL) 參數和匯出策略規則。但是，如果您想要在建立 NFS 檔案共用的相同磁碟區上啟用 CIFS，則可以更新該檔案共用上的 ACL 參數以支援 CIFS。

開始之前

1. 必須僅使用匯出策略詳細資訊來建立 NFS 檔案共用。有關信息，請參閱 [_管理文件共享_](#) 和 [_修改存儲工作負載_](#)。
2. 您必須擁有文件共用金鑰才能執行此操作。有關查看文件共享詳細資訊和使用作業 ID 檢索文件共享密鑰的信息，請參閱 [_配置 CIFS 和 NFS 文件共享_](#)。

這適用於您透過僅新增匯出策略規則而不是 ACL 參數建立的 NFS 檔案共用。您修改 NFS 檔案共用以包含 ACL 參數。

步驟

1. 在 NFS 檔案共享上，執行 `PATCH` 使用允許 CIFS 存取的 ACL 詳細資訊進行操作。

類別	HTTP 動詞	小路
儲存提供者	修補	/storage-provider/file-shares

範例 cURL

根據您指派給使用者群組的存取權限（如以下範例所示），將建立 ACL 並將其指派給檔案共用。

```

{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}

```

JSON 輸出範例

此操作傳回執行更新的作業的作業 ID。

2. 透過查詢相同文件共用的文件共用詳細資訊來驗證參數是否已正確新增。

類別	HTTP 動詞	小路
儲存提供者	得到	/storage-provider/file-shares/{key}

JSON 輸出範例

```

"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ]
      }
    ],
  }
}

```

```

        "index": 1,
        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},

```

```
  "_links": {
    "self": {
      "href": "/api/storage-provider/file-shares/7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
    }
  }
}
```

您可以看到與匯出策略一起指派給相同文件共用的 ACL。

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

專利

NetApp擁有的專利的最新清單可在以下位置找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

開源

有關本產品中使用的第三方版權和許可的資訊。

["Active IQ Unified Manager 9.16 通知"](#)

版權資訊

Copyright © 2025 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。